Terms of Service or General Terms and Conditions for Pera Services ("GTC")

If a valid agreement exists between you ("Customer") and Pera People Science B.V. ("Pera") related to the subject matter hereof, those terms take precedence over these terms unless otherwise agreed by the Parties in relation to a specific Order Form.

These GTC may be updated from time to time as explained herein. Refer to these GTC regularly to ensure compliance. These GTC can be found at the URL below:
https://www.getpera.com/pera-terms-of-service.pdf

Acceptance. Please read these GTC carefully before using www.getpera.com (the "Website") or the products or services offered by Pera (the "Services"). These GTC take effect when you click an "I Accept" button or checkbox presented with these GTC or when you use any of the Services or Website, whichever occurs first. If you are agreeing to these GTC on behalf of Customer, you represent to Pera that you have legal authority to bind Customer.

Modifications to this Agreement. Pera may modify these GTC at any time by posting a revised version at the URL given above or otherwise providing notice to Customer. By continuing to use the Services after the effective date of any modifications to these GTC, Customer agrees to be bound by the modified terms.

Revised September 1 September 2022
****

1. DEFINITIONS
    1. In these terms and conditions, the following terms, beginning with a capital letter, whether singular or plural, will have the following meaning:

Additional Services:	Any additional services separately rendered by Pera in connection to the Service, and which need to be agreed upon through a separate agreement;
Affiliate:	Means any person, firm, trust, partnership, corporation, company or other entity or combination thereof, which directly or indirectly, Controls Customer, is Controlled by Customer, or is under common Control with Customer. "Control," for purposes of this definition, means direct or indirect ownership of more than fifty percent (50%) of the voting interests of Customer;
Authorized User:	Means any individual to whom Customer grants access authorization to use the Cloud Service that is an employee, agent, contractor, or representative of a. Customer b. Customer's Affiliates, and/or c. Customer's and Customer's Affiliates' Business Partners.
Business Partner:	Means a legal entity that requires use of a Cloud Service in connection with Customer's and its Affiliates' internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.
Cloud Materials:	Mean any materials provided or developed by Pera (independently or with Customer's cooperation) during performance under the Agreement, including in the delivery of any support or Consulting Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information, or the Cloud Service.
Cloud Service:	Means any distinct, subscription-based, hosted, supported, and operated on- demand solution provided by Pera under an Order Form.

Confidential Information:	All information relating to a Party's business affairs, including and without limitation any technical, financial, operational, administrative, marketing, economic and other information document or data of any kind including Customer Content disclosed by one Party to the other or by a third party, whether recorded or transmitted orally, in writing, electronically or otherwise that is either identified or marked as "confidential" or "proprietary" at the time of such disclosure or which under the circumstances surrounding the disclosure can reasonably be presumed to be confidential or secretive and that relates to either Party's past, present and future plans, businesses, activities, products, software, technologies, services, customers and suppliers or relates to Affiliates;
Consulting Services:	Means professional services, such as implementation, configuration, custom development and training, performed by Pera' employees or subcontractors as described in any Order Form, and which are governed by the Supplement for Consulting Services or similar agreement.
Content:	Results, Customer Content, User Content and Pera Content;
Customer:	A natural or legal person who has therewith entered into an Agreement with Pera regarding the Service;
Customer Content:	All information, data, or material in the form of images, videos, text and audio-visual material or any other content submitted by Customer;
Customer Data:	Means any content, materials, data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include Pera' Confidential Information.
Documentation:	Means Pera' then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.
Environment:	The environment, which is accessible through a dedicated URL is managed by Customer, by which Customer is able to access the Results and User Content;
Intellectual Property Rights/IPR:	All intellectual property rights and associated rights, including copyrights, trademark rights, patent rights, design rights, trade name rights, database rights, and neighboring rights, as well as rights to knowhow;
Order Form:	Means the medium by which Customer purchases a Cloud Service, including, as applicable, an ordering document that references the GTC.
Parties:	Pera and Customer together, or separately referred to as "Party";
Platform/Solution:	The software-as-a-service platform, developed by Pera and/or its licensor(s) based on proprietary technology in the area of language analytics, psychology, artificial intelligence and machine learning with specific applications for HR, staffing and performance. Customer can access the Results visible through the Environment;
Results:	The results of the digital interview process as completed by User in the Platform;
Pera:	Means Pera People Science B.V., a private company organised under the laws of the Netherlands, with an office at: Parallelweg 27 's Hertogenbosch North Brabant 5223 AL The Netherlands In this matter legally represented by Rina Joosten-Rabou;

Pera Content:	All information, data or material in the form of images, videos, text and audio-visual material or any other content not Customer Content, User Content or Results made available by Pera and/or its licensor(s) through the Service whether or not on a customized basis;
Pera Policies:	Means the operational guidelines and policies applied by Pera to provide and support the Cloud Service as incorporated in an Order Form.
Service:	All services that Pera provides to Customer, including the access and use of the Platform and the Environment;
Subscription Term:	Means the term of a Cloud Service subscription identified in the applicable Order Form, including all renewals.
Supplement:	Means as applicable, the supplemental terms and conditions that apply to the Cloud Service and that are incorporated in an Order Form.
Terms / Agreement:	These service terms and their exhibits, addendums and any proposal or any other document by which Customer orders the Service, pertaining to the use of the Service and Additional Services;
Usage Metric:	Means the standard of measurement for determining the permitted use and calculating the fees due for a Cloud Service as set forth in an Order Form.
User Content:	All information, data or material or any other content, including but not limited to personal data, submitted by a User through the Platform.

2. USAGE RIGHTS AND RESTRICTIONS
    1. Grant of Rights. Pera grants to Customer a non-exclusive, non-transferable, and world-wide right to use the Cloud Service (including its implementation and configuration), Cloud Materials (as applicable) and Documentation solely for Customer's and its Affiliates' internal business operations. Permitted uses and restrictions of the Cloud Service also apply to Cloud Materials and Documentation.
    2. Authorized Users. Customer may permit Authorized Users to use the Cloud Service. Usage is limited to the Usage Metrics and volumes stated in the Order Form. Access credentials for the Cloud Service may not be used by more than one individual but may be transferred from one individual to another if the original user is no longer permitted to use the Cloud Service. Customer is responsible for breaches of the Agreement caused by Authorized Users.
    3. Acceptable Use Policy. With respect to the Cloud Service, Customer will not:
        a. disassemble, decompile, reverse-engineer, copy, translate or make derivative works,
        b. transmit any content or data that is unlawful or infringes any intellectual property rights, or
        c. circumvent or endanger its operation or security.
    4. Verification of Use. Customer will monitor its own use of the Cloud Service and report any use in excess of the Usage Metrics and volume. Pera may monitor use to verify compliance with Usage Metrics, volume, and the Agreement.
    5. Suspension of Cloud Service. Pera may suspend or limit use of the Cloud Service if continued use may result in material harm to the Cloud Service or its users. Pera will promptly notify Customer of the suspension or limitation. Pera will limit a suspension or limitation in time and scope as reasonably possible under the circumstances.
    6. Third Party Web Services. The Cloud Service may include integrations with web services made available by third parties (other than Pera's Affiliates) that are accessed through the Cloud Service and subject to terms and conditions with those third parties. These third-party web services are not part of the Cloud Service, and the Agreement does not apply to them.
3. PERA RESPONSIBILITIES
    1. Provisioning. Pera provides access to the Cloud Service as described in the Agreement.
    2. Support. Pera provides support for the Cloud Service as referenced in the Order Form.
    3. Security. Pera will implement and maintain appropriate technical and organizational measures to protect the personal data processed by Pera as part of the Cloud Service as described in the Data Processing Agreement attached hereto as Exhibit A ("DPA") for Cloud Services incorporated into the Order Form in compliance with applicable data protection law.
    4. Modifications.

a. The Cloud Service and Pera Policies may be modified by Pera. Pera will inform Customer of modifications by email, the support portal, release notes, Documentation, or the Cloud Service. The information will be delivered by email if the modification is not solely an enhancement. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement and Documentation.
b. If Customer establishes that a modification is not solely an enhancement and materially reduces the Cloud Service, Customer may terminate its subscriptions to the affected Cloud Service by providing written notice to Pera within thirty days after receipt of Pera' informational notice.

5. Analyses. Pera or Pera's Affiliates may create analyses utilizing, in part, Customer Data and information derived from Customer's use of the Cloud Service and Consulting Services, as set forth below ("Analyses"). Analyses will anonymize and aggregate information and will be treated as Cloud Materials. Unless otherwise agreed, personal data contained in Customer Data is only used to provide the Cloud Service and Consulting Services. Analyses may be used for the following purposes:
    a. product improvement (in particular, product features and functionality, workflows and user interfaces) and development of new Pera products and services,
    b. improving resource allocation and support,
    c. internal demand planning,
    d. training and developing machine learning algorithms,
    e. improving product performance,
    f. verification of security and data integrity
    g. identification of industry trends and developments, creation of indices and anonymous benchmarking

4. CUSTOMER AND PERSONAL DATA
    1. Customer Data. Customer is responsible for the Customer Data and entering it into the Cloud Service. Customer grants to Pera (including Pera' Affiliates and subcontractors) a nonexclusive right to process Customer Data solely to provide and support the Cloud Service.
    2. Personal Data. Customer will collect and maintain all personal data contained in the Customer Data in compliance with applicable data privacy and protection laws.
    3. Security. Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service. Customer will not conduct or authorize penetration tests of the Cloud Service without advance approval from Pera.
    4. Access to Customer Data.
        a. During the Subscription Term, Customer can access its Customer Data at any time. Customer may export and retrieve its Customer Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Pera and Customer will find a reasonable method to allow Customer access to Customer Data.
        b. Before the Subscription Term expires, if available, Customer may use Pera' self-service export tools (as available) to perform a final export of Customer Data from the Cloud Service. Alternatively, Customer may request data export through support ticket.
        c. At the end of the Agreement, Pera will delete or anonymize the Customer Data remaining on servers hosting the Cloud Service unless applicable law requires retention. Retained data is subject to the confidentiality provisions of the Agreement.
        d. In the event of third-party legal proceedings relating to the Customer Data, Pera will cooperate with Customer and comply with applicable law (both at Customer's expense) with respect to handling of the Customer Data.

5. FEES AND TAXES
    1. Fees and Payment. Customer will pay fees as stated in the Order Form. After prior written notice, Pera may suspend Customer's use of the Cloud Service until payment is made. Customer cannot withhold, reduce or set-off fees owed nor reduce Usage Metrics during the Subscription Term. All Order Forms are non-cancellable and fees non-refundable.
    2. Taxes. Fees and other charges imposed under an Order Form will not include taxes, all of which will be for Customer's account. Customer is responsible for all taxes, other than Pera' income and payroll taxes. Customer must provide to Pera any direct pay permits or valid tax-exempt certificates prior to signing an Order Form. If Pera is required to pay taxes (other than its income and payroll taxes), Customer will reimburse Pera for those amounts and indemnify Pera for any taxes and related costs paid or payable by Pera attributable to those taxes.

6. TERM AND TERMINATION
    1. Term. The Subscription Term is as stated in the Order Form.
    2. Termination. A party may terminate the Agreement:
        a. upon thirty days written notice of the other party's material breach unless the breach is cured during that thirty day period,

b. as permitted under Sections 3.4(b), 7.3(b), 7.4(c), or 8.1(c) (with termination effective thirty days after receipt of notice in each of these cases), or
c. immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 11 or 12.6.

3. Refund and Payments. Pera will not refund the prepaid fees upon termination unless there is a breach of contract (as described in Clause 7.4).
    a. a
4. Effect of Expiration or Termination. Upon the effective date of expiration or termination of the Agreement:
    a. Customer's right to use the Cloud Service and all Pera Confidential Information will end,
    b. Confidential Information of the disclosing party will be returned or destroyed as required by the Agreement, and
    c. termination or expiration of the Agreement does not affect other agreements between the parties.
5. Survival. Sections 1, 5, 6.3, 6.4, 6.5, 8, 9, 10, 11, and 12 will survive the expiration or termination of the Agreement.

7. WARRANTIES
    1. Compliance with Law. Each party warrants its current and continuing compliance with all laws and regulations applicable to it in connection with:
        a. in the case of Pera, the operation of Pera' business as it relates to the Cloud Service, and
        b. in the case of Customer, the Customer Data and Customer's use of the Cloud Service.
    2. Good Industry Practices. Pera warrants that it will provide the Cloud Service:
        a. in substantial conformance with the Documentation; and
        b. with the degree of skill and care reasonably expected from a skilled and experienced global supplier of services substantially similar to the nature and complexity of the Cloud Service.
    3. Remedy. Customer's sole and exclusive remedies and Pera' entire liability for breach of the warranty under Section 7.2 will be:
        a. the re-performance of the deficient Cloud Service, and
        b. if Pera fails to re-perform, Customer may terminate its subscription for the affected Cloud Service. Any termination must occur within three months of Pera' failure to re-perform.
    4. System Availability.
        a. Pera warrants to maintain an average monthly system availability for the production system of the Cloud Service as defined in the applicable service level agreement or Supplement ("SLA").
        b. Customer's sole and exclusive remedy for Pera' breach of the SLA is the issuance of a credit in the amount described in the SLA. Customer will follow Pera's posted credit claim procedure. When the validity of the service credit is confirmed by Pera in writing (email permitted), Customer may apply the credit to a future invoice for the Cloud Service or request a refund for the amount of the credit if no future invoice is due.
        c. In the event Pera fails to meet the SLA (i) for four consecutive months, or (ii) for five or more months during any twelve months period, or (iii) at a system availability level of at least 95% for one calendar month, Customer may terminate its subscriptions for the affected Cloud Service by providing Pera with written notice within thirty days after the failure.
    5. Warranty Exclusions. The warranties in Sections 7.2 and 7.4 will not apply if:
        a. the Cloud Service is not used in accordance with the Agreement or Documentation,
        b. any non-conformity is caused by Customer, or by any product or service not provided by Pera, or
        c. the Cloud Service was provided for no fee.
    6. Disclaimer. Except as expressly provided in the Agreement, neither Pera nor its subcontractors make any representation or warranties, express or implied, statutory or otherwise, regarding any matter, including the merchantability, suitability, originality, or fitness for a particular use or purpose, non-infringement or results to be derived from the use of or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of Pera or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS
    1. Claims Brought Against Customer.
        a. Pera will defend Customer against claims brought against Customer and its Affiliates by any third party alleging that Customer's and its Affiliates' use of the Cloud Service infringes or misappropriates a patent claim, copyright, or trade secret right. Pera will indemnify Customer against all damages finally awarded against Customer (or the amount of any settlement Pera enters into) with respect to these claims.

b. Pera' obligations under Section 8.1 will not apply if the claim results from (i) Customer's breach of Section 2, (ii) use of the Cloud Service in conjunction with any product or service not provided by Pera, or (iii) use of the Cloud Service provided for no fee.
c. In the event a claim is made or likely to be made, Pera may (i) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (ii) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality. If these options are not reasonably available, Pera or Customer may terminate Customer's subscription to the affected Cloud Service upon written notice to the other.

2. Claims Brought Against Pera. Customer will defend Pera against claims brought against Pera and its Affiliates and subcontractors by any third-party related to Customer Data. Customer will indemnify Pera against all damages finally awarded against Pera and its Affiliates and subcontractors (or the amount of any settlement Customer enters into) with respect to these claims.
3. Third Party Claim Procedure.
    a. The party against whom a third-party claim is brought will timely notify the other party in writing of any claim, reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the party providing the defense.
    b. The party that is obligated to defend a claim will have the right to fully control the defense.
    c. Any settlement of a claim will not include a financial or specific performance obligation on, or admission of liability by, the party against whom the claim is brought. 8.4 Exclusive Remedy.
4. Exclusive Remedy. The provisions of Section 8 state the sole, exclusive, and entire liability of the parties, their Affiliates, Business Partners and subcontractors to the other party, and is the other party's sole remedy, with respect to covered third party claims and to the infringement or misappropriation of third-party intellectual property rights.

9. LIMITATION OF LIABILITY
    1. Unlimited Liability. Neither party will exclude or limit its liability for damages resulting from:
        a. the parties' obligations under Section 8.1(a) and 8.2,
        b. unauthorized use or disclosure of Confidential Information,
        c. either party's breach of its data protection and security obligations that result in an unauthorized use or disclosure of personal data,
        d. death or bodily injury arising from either party's gross negligence or willful misconduct, or
        e. any failure by Customer to pay any fees due under the Agreement.
    2. Liability Cap. Subject to Sections 9.1 and 9.3, the maximum aggregate liability of either party (or its respective Affiliates or Pera' subcontractors) to the other or any other person or entity for all events (or series of connected events) arising in any twelve month period will not exceed the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve month period. Any "twelve-month period" commences on the Subscription Term start date or any of its yearly anniversaries.
    3. Exclusion of Damages. Subject to Section 9.1:
        a. neither party (nor its respective Affiliates or Pera' subcontractors) will be liable to the other party for any special, incidental, consequential, or indirect damages, loss of good will or business profits, work stoppage or for exemplary or punitive damages, and
        b. Pera will not be liable for any damages caused by any Cloud Service provided for no fee.
    4. Risk Allocation. The Agreement allocates the risks between Pera and Customer. The fees for the Cloud Service and Consulting Services reflect this allocation of risk and limitations of liability.

10. INTELLECTUAL PROPERTY RIGHTS
    1. PERA Ownership. Pera, Pera's Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Consulting Services, design contributions, related knowledge or processes, and any derivative works of them. All rights not expressly granted to Customer are reserved to Pera and its licensors.
    2. Customer Ownership. Customer retains all rights in and related to the Customer Data. Pera may use Customer-provided trademarks solely to provide and support the Cloud Service.
    3. Non-Assertion of Rights. Customer covenants, on behalf of itself and its successors and assigns, not to assert against Pera and its Affiliates or licensors, any rights, or any claims of any rights, in any Cloud Service, Cloud Materials, Documentation, or Consulting Services.

11. CONFIDENTIALITY
    1. Use of Confidential Information,
        a. The receiving party will protect all Confidential Information of the disclosing party as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Receiving party will not disclose any Confidential Information of the disclosing party to any person other than its personnel, representatives or Authorized Users whose access is necessary to enable it to exercise its rights or perform its obligations under the Agreement and who are under obligations of confidentiality substantially similar to

those in Section 11. Customer will not disclose the Agreement or the pricing to any third party.

b. Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section 11.

c. In the event of legal proceedings relating to the Confidential Information, the receiving party will cooperate with the disclosing party and comply with applicable law (all at disclosing party's expense) with respect to handling of the Confidential Information.

2. Exceptions. The restrictions on use or disclosure of Confidential Information will not apply to any Confidential Information that:
    a. is independently developed by the receiving party without reference to the disclosing party's Confidential Information,
    b. is generally available to the public without breach of the Agreement by the receiving party,
    c. at the time of disclosure, was known to the receiving party free of confidentiality restrictions, or
    d. the disclosing party agrees in writing is free of confidentiality restrictions.
3. Publicity. Customer grants Pera the right to use the name and the right to display its logo of Customer in its marketing materials, and website or other oral, electronic, or written promotions, which shall include naming Customer as a client of Pera and a brief scope of services provided. Customer agrees that Pera may share information on Customer with its Affiliates for marketing and other business purposes and that it has secured appropriate authorizations to share Customer employee contact information with Pera.

12. MISCELLANEOUS
    1. Severability If any provision of the Agreement is held to be invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.
    2. No Waiver. A waiver of any breach of the Agreement is not deemed a waiver of any other breach.
    3. Electronic Signature. Electronic signatures that comply with applicable law are deemed original signatures.
    4. Regulatory Matters. Pera Confidential Information is subject to export control laws of various countries, including the laws of the Netherlands, Brazil and China. Customer will not submit Pera Confidential Information to any government agency for licensing consideration or other regulatory approval, and will not export Pera Confidential Information to countries, persons or entities if prohibited by export laws.
    5. Notices. All notices will be in writing and given when delivered to the address set forth in an Order Form. Notices by Pera relating to the operation or support of the Cloud Service and those under Sections 3.4 and 5.1 may be in the form of an electronic notice to Customer's authorized representative or administrator identified in the Order Form.
    6. Assignment. Without Pera' prior written consent, Customer may not assign or transfer the Agreement (or any of its rights or obligations) to any party. Pera may assign the Agreement to Pera Affiliates.
    7. Subcontracting. Pera may subcontract parts of the Cloud Service or Consulting Services to third parties. Pera is responsible for breaches of the Agreement caused by its subcontractors.
    8. Relationship of the Parties. The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties is created by the Agreement.
    9. Force Majeure. Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. The time for performance will be extended for a period equal to the duration of the conditions preventing performance
    10. Governing Law. The Agreement and any claims relating to its subject matter will be governed by and construed under the laws of the Netherlands, without reference to its conflicts of law principles. All disputes will be subject to the exclusive jurisdiction of the courts located in the Netherlands.
    11. Entire Agreement. The Agreement constitutes the complete and exclusive statement of the agreement between Pera and Customer in connection with the parties' business relationship related to the subject matter of the Agreement. All previous representations, discussions, and writings (including any confidentiality agreements) are merged in and superseded by the Agreement and the parties disclaim any reliance on them. The Agreement may be modified solely in writing signed by both parties, except as permitted under Section 3.4. An Agreement will prevail over terms and conditions of any Customer-issued purchase order, which will have no force and effect, even if Pera accepts or does not otherwise reject the purchase order.
    12. Data Processing Agreement. Where Customer is processing personal data using the Services, the DPA shall govern the processing of such personal data.

Data Processing Agreement

PERSONAL DATA PROCESSING AGREEMENT FOR PERA CLOUD SERVICES

This Data Processing Addendum ("DPA") is entered into BETWEEN (1) Customer; and (2) Pera.

1. BACKGROUND
    1. Purpose and Application. This document is incorporated into the Agreement and forms part of a written (including in electronic form) contract between Pera and Customer. This DPA applies to Personal Data processed by Pera and its Sub processors in connection with its provision of the Cloud Service.
    2. Structure. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.
    3. GDPR. Pera and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("GDPR"), with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.
    4. Governance. Pera acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents, and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use Pera as a Processor. Where authorizations, consent, instructions, or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where Pera informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.
2. DEFINITIONS Capitalized terms not defined herein will have the meanings given to them in the Agreement.
    1. "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to Pera be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.
    2. "Data Center" means the location where the production instance of the Cloud Service is hosted for the Customer in the region agreed in an Order Form.
    3. "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy regarding the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by Pera on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).
    4. "Data Subject" means an identified or identifiable natural person as defined by Data Protection Law.
    5. "EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein, and Norway.
    6. "Personal Data" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by Pera or its Sub processors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).
    7. "Personal Data Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.
    8. "Processor" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as sub processor of a processor which processes personal data on behalf of the controller.
    9. "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix 4.
    10. "Sub processor" means Pera affiliates, and third parties engaged by Pera in connection with the Cloud Service and which process Personal Data in accordance with this DPA.
3. DURATION

1. This DPA terminates after and insofar as the Processor has anonymised, deleted, or returned all Personal Data in accordance with article 10.
2. Neither of the Parties may terminate this DPA before the Contract terminates.

4. SECURITY OF PROCESSING
    1. Appropriate Technical and Organizational Measures. Pera has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate considering the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.
    2. Changes. Pera applies the technical and organizational measures set forth in Appendix 2 to Pera' entire customer base hosted out of the same Data Center and receiving the same Cloud Service. Pera may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.
5. PERA OBLIGATIONS
    1. Instructions from Customer. Pera will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions, and each use of the Cloud Service then constitutes further instructions. Pera will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or Pera otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Pera will immediately notify Customer (email permitted).
    2. Processing on Legal Requirement. Pera may also process Personal Data where required to do so by applicable law. In such a case, Pera shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.
    3. Personnel. To process Personal Data, Pera and its Sub processors shall only grant access to authorized personnel who have committed themselves to confidentiality. Pera and its Sub processors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.
    4. Cooperation. At Customer's request, Pera will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Pera' processing of Personal Data or any Personal Data Breach. Pera shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing. Pera will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.
    5. Personal Data Breach Notification. Pera will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. Pera may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Pera.
    6. Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, Pera will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.
6. DATA EXPORT, RETURN AND ANONYMISATION
    1. Export and Retrieval by Customer. During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Pera and Customer will find a reasonable method to allow Customer access to Personal Data.
    2. Return and Anonymization of Personal Data. At the end of the Subscription Term and at the request of Customer, Pera will return the Personal Data to Customer. Pera may furthermore anonymise the Personal Data for archiving purposes in the public interest, scientific or historical research purposes and/or statistical purposes in accordance with article 89 GDPR and will inform the Data Subjects accordingly about these activities.
7. CERTIFICATIONS AND AUDITS
    1. Customer Audit. Customer or its independent third-party auditor reasonably acceptable to Pera (which shall not include any third party auditors who are either a competitor of Pera or not suitably qualified or independent) may audit Pera' control environment and security practices relevant to Personal Data processed by Pera only if:
        a. Pera has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope

as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third-party auditor or Pera;

b. A Personal Data Breach has occurred.
c. An audit is formally requested by Customer's data protection authority; or
d. Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve-month period unless mandatory Data Protection Law requires more frequent audits.

2. Other Controller Audit. Any other Controller may audit Pera' control environment and security practices relevant to Personal Data processed by Pera in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by Pera on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.
3. Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to Pera.
4. Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by Pera of this DPA, then Pera shall bear its own expenses of an audit. If an audit determines that Pera has breached its obligations under the DPA, Pera will promptly remedy the breach at its own cost.

8. SUBPROCESSORS
    1. Permitted Use. Pera is granted a general authorization to subcontract the processing of Personal Data to Sub processors, provided that:
        a. Pera shall engage Sub processors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Sub processor's processing of Personal Data. Pera shall be liable for any breaches by the Sub processor in accordance with the terms of this Agreement.
        b. Pera will evaluate the security, privacy and confidentiality practices of a Sub processor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and
        c. Pera' list of Sub processors in place on the effective date of the Agreement will be made available to Customer, upon request including the name, address, and role of each Sub processor Pera uses to provide the Cloud Service.
    2. New Sub processors. Pera's use of Sub processors is at its discretion, provided that:
        a. Pera will inform Customer in advance (by email or by posting within the Cloud Service) of any intended additions or replacements to the list of Sub processors including name, address and role of the new Sub processor; and
        b. Customer may object to such changes as set out in Section 6.3
    3. Objections to New Sub processors.
        a. If Customer has a legitimate reason under Data Protection Law to object to the new Sub processors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Sub processor is intended to be used) on written notice to Pera. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of Pera' notice to Customer informing Customer of the new Sub processor. If Customer does not terminate within this thirty-day period, Customer is deemed to have accepted the new Sub processor.
        b. Within the thirty-day period from the date of Pera' notice to Customer informing Customer of the new Sub processor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect Pera' right to use the new Sub processor(s) after the thirty-day period.
        c. Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.
    4. Emergency Replacement. Pera may replace a Sub processor without advance notice where the reason for the change is outside of Pera's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Pera will inform Customer of the replacement Sub processor as soon as possible following its appointment. Section 6.3 applies accordingly.
9. INTERNATIONAL PROCESSING

1. Conditions for International Processing. Pera shall be entitled to process Personal Data, including by using Sub processors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.
2. Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as a safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

a. Pera and Customer enter into the Standard Contractual Clauses.

b. Customer enters into the Standard Contractual Clauses with each relevant Sub processor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by Pera and the Sub processor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Sub processor (represented by Pera) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when Pera has expressly confirmed that a Sub processor is eligible for it through the Sub processor list provided under Section 6.1(c), or a notice to Customer; and/or

c. Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with Pera and/or the relevant Sub processors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter the Standard Contractual Clauses on behalf of the other Controllers.

3. Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and sub processor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.
4. Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the laws of the Netherlands.

10. DOCUMENTATION: RECORDS OF PROCESSING Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), to enable the other party to comply with any obligations relating to maintaining records of processing.
11. OTHER PROVISIONS
    1. If any (or part of any) provision of this DPA is found to be invalid, unenforceable, or illegal by a competent court, the other provisions shall remain in force. If any invalid, unenforceable or illegal provision would be valid, enforceable, or legal if some part of it were deleted or modified, that provision shall apply with whatever modification is necessary to give effect to the intention of the Parties.
    2. Each Party is prohibited from transferring this DPA or rights and/or obligations under this DPA entirely or partly to another party, without approval from the other Party.
    3. Any notice to be given by a Party pursuant to this Agreement shall be in writing (including by e-mail) and shall be sent to the address of the applicable Party as set out in the preamble to this DPA. Each Party may change its address by giving notice to the other Parties.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses – Processing Personal Data

The nature and purpose of the Processing activities	Processor is a a Machine Learning & Natural Language Processing (NLP) company that analyzes people's use of language and answers to psychometric questions in order to make predictions about said persons behavior, preferences, personality, and likelihood of being a fit to a given job position/function, team, organizational culture, etc.
The types of Personal Data	Name, gender, mobile number, e-mail address, employment data (employer, role, years in the role, performance ratings, etc), possible personal data contained in answers to open ended questions.
The categories of Data Subjects	Current and potential employees of Processor's clients
The categories of Personal Data recipients	Processor's clients and her authorised employees; Processor and her authorized employees, Subprocessors that are bound to the same protection obligations as those imposed by this DPA,

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

Processor adopts the following standards and measures to ensure the security of Processing:

Technical Measures	Answer	Comments
Data centre	Use of certified (SOC 2 and/or PCI DSS and/or SSAE 16) data centres	Processor uses SOC 2 certified data centres.
Host/Cloud provider	Amazon Web Services ('AWS').	To use the application developed by Processor and process the Personal Data, Processor uses the services of AWS. The data which is received, including the Personal Data, is hosted in a so called Virtual Private Cloud environment.
Classification	AWS operates all their data centres with a so-called Tier III+ guidelines.	AWS has chosen not to use a certified Uptime Institute based tiering level in order to keep an amount of flexibility to expand and improve their performance.
Server locations	Production Servers in Ireland and backups in Germany.	AWS keeps seven servers, they are located in Germany, the United Kingdom and Ireland.
Backup data centre		Processor implements all necessary measures in terms of backup and restoration, including regular tests of the reliability and completeness of the backups. Processor encrypts all backups

		Processor keeps audit logs and web server logs with a retention period of 12 months.
Communications security	Access restriction	Processor restricts - at network-level - any access from Internet to private infrastructures services, operating systems and middleware interfaces (e.g. Database listener, SSH, back-end API)
	Environment segregation	Processor segregates - at network-level - production and development/staging environments.
	Encryption	Processor ensures that any remote access from Internet to her infrastructure uses strong encryption.
System acquisition, development and maintenance	OWASP vulnerabilities	Processor develops and maintains applications and Application Programming Interfaces (API) according to OWASP Top 10 vulnerabilities and risks.
	Multi-Factor Authentication	Processor enforces Multi-Factor Authentication for any access to source management platforms (e.g. GitHub, bitbucket.) to avoid any data breaches. That code is not publicly accessible.
	Approval of Controller	Processor guarantees that the Personal Data are never exported to or used in a non-production environment (including for testing purposes) without previous formal approval of Controller.
Penetration test frequency	Annually	Processor achieves a penetration test of the solution and associated infrastructure used to carry out the Contract on an annually basis and at its own costs and communicates the executive summary and related mitigation action plan to the Controller upon its request.
Vulnerability scan frequency	Quarterly	Processor achieves network, system and application vulnerability scans at minimum on a quarterly basis.
Advisories monitoring frequency	Daily	Processor monitors AWS security advisories from all hardware and software used to carry out the Contract.
Vulnerability remediation delays	12 hours in case of critical vulnerability that can be exploited directly from Internet without requiring authentication and that could lead to a direct compromise of Personal Data and	Processor ensures that applicable security hotfixes (or workaround) recommended by AWS and possible other hardware/software vendors are

	where an exploitation proof-of-concept exist. 48 hours in case of a high vulnerability that can be exploited directly from Internet that could lead to a direct compromise of Personal Data or Processors' systems but where an exploitation proof-of-concept does not exist or exploitation requires an action from a logged user. 2 months in case of a medium vulnerability that can lead to a direct compromise of Personal Data or Processors' systems where exploitation requires the attacker to have an advantage, such as having stolen legitimate credentials by sending a malicious link to a victim, sniffing network traffic or gaining unauthorized access. Next release in case of a low vulnerability that can never lead to direct or indirect compromise of Personal Data.	installed within the defined vulnerability remediation delays. Processor ensures that any identified vulnerabilities are remediated in no delay and no later than the defined vulnerability remediation delays. Processor ensures that in case of a critical vulnerability measures are put in place immediately to avoid the exploitation of the vulnerability.
Data recovery capabilities	Daily snapshot Recovery time objective is 4 hours	Processor takes a so-called snapshot every day, which is kept for thirty days. Processor ensures a maximum time allowed to recover failed application or provide products and services after a disruptive incident occurs.
Cryptography	Encryption (e.g. HTTPS) Secure File Transfer Protocol	Processor encrypts all data in transit and DB backups at rest. Processor has implemented a process to protect and manage lifecycle of cryptographic keys.
Operations security	Installation, configuration and operational guides on all security devices, network components, servers and middleware.	Processor defines and applies guides that follow best practises as those from National Institute of Standards and Technology (NIST) or Centre for Information Security (CIS).

Organisational measures	Answer	Comments
Information security policy	Security Policy, Pera People Science B.V.	The security policy used by Processor is approved by the management of its

		company and communicated to all employees and relevant external parties.
Organization of information security	DPO	security@getpera.com
Human resource security	Confidentiality clause Security awareness program Revoke Access	All employees and contractors sign a confidentiality clause and are informed about the security policy used by Processor and follow a security awareness program. Former employees/contractors access is disabled to any asset used to carry out the Contract with the Controller after departure or when not required anymore within (at maximum) a period of 1 month.
Asset management	Return/destruction Personal Data	Processor undertakes, upon expiration or termination of the Contract for any reason whatsoever, to destroy and / or return to Controller in a maximum of 60 days, all Personal Data, files or other items provided by the Controller or Data Subjects or resulting from the processing of Personal Data.
Access control	Use of nominative account/formal procedure in order to be able to affect each action to a specific user. Store passwords only using a strong encryption hash (e.g. SHA-256 or MD5 with a 8 bytes random salt or higher)	Processor adopts organizational measures to permit access to the Personal Data only by duly authorized persons. Processor enforces related access-control rules to any cloud storage services (e.g. S3 buckets) used to store Personal Data of the Controller or needed to carry out the Contract.

Appendix 3

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

(Pursuant to Commission Decision of 5 February 2010 (2010/87/EU))

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer also on behalf of the other Controllers

(in the Clauses hereinafter referred to as the 'data exporter')

and

Pera People Science B.V.

(in the Clauses hereinafter referred to as the 'data importer')

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in the General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and of the Council of 27 April 2016.
(b) 'the Data Exporter' means the controller who transfers the personal data.
(c) 'the Data Importer' means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 45 of GDPR.
(d) 'the sub processor' means any processor engaged by the Data Importer or by any other sub processor of the Data Importer who agrees to receive from the Data Importer or from any other sub processor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established.
(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure, or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.
4. The Parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State.

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses.

(c) that the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract.

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures.

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of GDPR.

(g) to forward any notification received from the Data Importer or any sub processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension.

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information.

(i) that, in the event of sub processing, the processing activity is carried out in accordance with Clause 11 by a sub processor providing at least the same level of protection for the personal data and the rights of data subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the Data Importer[1]

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its

[1] Mandatory requirements of the national legislation applicable to the Data Importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 23 of the Regulation (EU) 2016/679, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract.

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred.

(d) that it will promptly notify the Data Exporter about:
(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
(ii) any accidental or unauthorised access, and
(iii) any request received directly from the data subjects without responding to that request unless it has been otherwise authorised to do so.

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority regarding the processing of the data transferred.

(f) at the request of the Data Exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter, or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority.

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Data Exporter.

(h) that, in the event of sub processing, it has previously informed the Data Exporter and obtained its prior written consent.

(i) that the processing services by the sub processor will be carried out in accordance with Clause 11.

(j) to send promptly a copy of any sub processor agreement it concludes under the Clauses to the Data Exporter.

Clause 6: Liability

1. The Parties agree that any data subject, who has suffered damage because of any breach of the obligations referred to in Clause 3 or in Clause 11 by any Party or sub processor is entitled to receive compensation from the Data Exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his sub processor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the data subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
   The Data Importer may not rely on a breach by a sub processor of its obligations to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the sub processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the sub processor agrees that the data subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.
4. The Parties agree that if one Party is held liable for a violation of the clauses committed by the other Party, the latter will, to the extent to which it is liable, indemnify the first Party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon: (a) the Data Exporter promptly notifying the Data Importer of a claim; and (b) the Data Importer being given the possibility to cooperate with the Data Exporter in the defence and settlement of the claim.

Clause 7: Mediation and jurisdiction

1. The Data Importer agrees that if the data subject invokes against its third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority.
   (b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.
2. The Parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The Parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any sub processor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.
3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any sub processor preventing the conduct of an audit of the Data Importer, or any sub processor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established, namely the Netherlands.

Clause 10: Variation of the contract

The Parties undertake not to vary or modify the Clauses. This does not preclude the Parties from adding clauses on business related issues where required if they do not contradict the Clause.

Clause 11: Sub processing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub processor as are imposed on the Data Importer under the Clauses[2]. Where the sub processor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the sub processor's obligations under such agreement.
2. The prior written contract between the Data Importer and the sub processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established, namely the Netherlands.
4. The Data Exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The Parties agree that on the termination of the provision of data processing services, the Data Importer and the sub processor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy or anonymize all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying or anonymizing all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The Data Importer and the sub processor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[2] This requirement may be satisfied by the sub processor co-signing the contract entered between the data exporter and the Data Importer under this Decision.