Data Processing Agreement (DPA)

Last change: July 2026

These General Terms and Conditions (GTC)/ End User Licence Agreement (EULA) govern the use of the SAAS for AI-supported data analysis "QInsights", which is provided by QInsights BV. The service enables users to have uploaded documents automatically analysed and summarised according to various criteria ("Document Analysis").

General part

§ 1 Subject matter of the contract

1 The subject of these GTC/EULA are all services provided within the scope of the QInsights product.

2. The provider of deliveries or services under this contract is QInsights BV, Bierstraat 123C, 3011 XA Rotterdam, The Netherlands, hereinafter referred to as "QInsights BV".

3. Subject to explicit provisions to the contrary in these GTC/EULA, QInsights BV is the manufacturer and owner of all exploitation rights to the QInsights.

§ 2 Payment processing via third-party provider

Payment processing for the use of QInsights is either handled by the external payment service provider Stripe (e-sales partner), or directly by us. By selecting a paid option, the customer agrees to the terms and conditions of the payment service provider. Payment processing and related processes are subject to the terms and conditions of Stripe, or QInsights BV, respectively.

§ 3 Services and technical requirements

1 QInsights offers the customer the option of having uploaded documents automatically analysed and summarised by various criteria. For this purpose, the client uploads the documents to the website in their QInsights Account, and QInsights BV forwards them to a service provider via an interface. The created result is displayed in the user account.

2. The owed quality and the exact functional scope of QInsights can be found in the functional descriptions, which are available at QInsights Guide.

3. The automated analysis of the client's documents is not carried out by QINSIGHTS BV itself, but by service providers that QINSIGHTS BV has a contractual agreement with. The service providers use artificial intelligence for the document analysis. A regularly updated list of the service providers used can be found here: https://www.qinsights.ai/privacy

There is no entitlement to the use of a specific service provider or a specific method of artificial intelligence. The service providers used can be changed at any time if this does not result in any changes to QInsights. If the change of the service provider involves changes to QInsights, the change will only be made if there is a valid reason. A valid reason for a change exists in particular if QInsights is to be improved, an adaptation to new technical conditions is necessary, a uniform upgrade is required to avoid several parallel versions, or other important operational reasons necessitate the change.

QINSIGHTS BV is continuously developing QInsights and will improve QInsights through ongoing updates. Accordingly, QINSIGHTS BV is authorised to change QInsights at its own discretion. Unless it is a change or update that is necessary to maintain compliance with the contract, such changes will only be made if there is a valid reason. A valid reason for a change exists if QInsights is to be improved, an adaptation to new technical conditions is necessary, a uniform upgrade is required to avoid several parallel versions, or other important operational reasons necessitate the change. The customer will be informed of functional changes in an appropriate manner, e.g. through notices in the QInsights Account or per email.

§ 4 Use of QInsights

1. Product presentations, in particular on QINSIGHTS BV's websites, do not constitute an offer to conclude a contract.

2. Information provided by QINSIGHTS BV via telephone is non-binding.

3. To use QInsights, the customer must create a customer account on QINSIGHTS BV's website. A contract granting the right to use QInsights is concluded when the customer agrees to these GTC/EULA within his QInsights Account.

4. The customer is granted the opportunity to use QInsights as part of a free trial version up to one month, or a limit of 1 million tokens, whatever occurs first. During the free trial period, the customer has limited access to all functions of the paid full version. After one month, or after the free tokens are used, the trial phase ends automatically unless a paid contract extension is purchased. If the customer purchases a paid licence before the trial period expires, all data and results from the trial period will be transferred to the regular customer account and will remain available.

5. The customer is solely responsible for all activities carried out via their QInsights Account. The customer agrees to keep his login details confidential and not to grant third-parties access to his account. QINSIGHTS BV must be informed immediately if there is any suspicion of unauthorised use.

6. If the customer uses QInsights on behalf of a company or other organisation, they warrant that they are authorised to represent it in a legally binding manner. The obligations under this contract then also apply to the represented organisation.

7. The customer remains responsible for all content that they enter, store or transfer using QInsights. QINSIGHTS BV does not check their content. The customer warrants that they have all necessary rights and permissions to use and share this content.

8. The contract for the use of QInsights is concluded for an indefinite period of time. The contract for the use of QInsights ends when the QInsights Account is deleted by the customer or terminated by QINSIGHTS BV.

9. QINSIGHTS BV is permitted to collect and evaluate aggregated and anonymised data on the use of QInsights to improve or market the service and other products and services, provided that no personal data within the meaning of the GDPR is processed or disclosed.

§ 5 Rights of use

1. QINSIGHTS BV grants the customer the non-exclusive and non-transferable right to use QInsights as intended for the duration of the contract.

2. The customer may not make any changes to QInsights that go beyond what QINSIGHTS BV enables the customer to do by providing corresponding functions (e.g. in the settings).

3. The customer is not authorised to make QInsights available to third parties for use, either for a fee or free of charge. The customer is expressly prohibited from subletting QInsights.

4. The customer is not permitted to edit, modify or alter QInsights (in whole or in part) or to disassemble, decompile, reverse engineer or convert QInsights in whole or in part, nor may the customer permit or enable third parties to do so. Furthermore, the customer may not use QInsights to create, train or improve similar or competing products or services (directly or indirectly).

§ 6 Scope of use

1. The customer is not permitted to use QInsights in a manner that violates laws or the rights of third parties or unlawfully affects their rights or otherwise violates the provisions of these GTC/EULA or those of the service providers (as amended from time to time). In particular, the use of the function for the following purposes or the provision of the following content is prohibited:

    - **Illegal or harmful activities**, including the creation, distribution or promotion of illegal

content, discriminatory, violent, hateful or harassing content, and content that exploits or harms children,

- **Violation of third-party rights**, in particular privacy, intellectual property or other legally protected interests,
- **Impairment of security and integrity**, for example through hacking, circumvention of technical protection measures, distribution of malware or other attacks on systems or networks,
- **High-risk applications**, including use in connection with military purposes, critical infrastructure, medical, legal or financial advice, unless reviewed by qualified professionals.
- **Deception, fraud and manipulation**, including misleading statements, fraudulent business practices, multi-level marketing or unauthorised data processing,
- **Creation or distribution** of adult content, political campaigns or lobbying purposes.

2. The terms and conditions of the respective service providers are available on our website where we provide a link for each service provider: https://www.qinsights.ai/privacy

3. The customer is also not permitted to claim that the result generated by QInsights was produced by humans, although this is not the case.

§ 7 Data protection

1. QInsights BV collects and processes personal data in accordance with the GDPR.

2. Insofar as the customer processes personal data using QInsights, the customer acts as the data controller under data protection law. The customer is accordingly obliged to protect the data protection rights of third parties and confirms that it has fulfilled all requirements for the lawful processing of personal data, in particular that it has obtained all necessary consents.

3. The following provisions do not apply if the customer is a natural person and the processing of personal data is carried out exclusively for personal or family activities.

1. Data processing agreement

1.1 **Schedule 1** to these GTC/EULA contains the QINSIGHTS BV Data Processing Agreement ("**DPA**"). This DPA constitutes the mutual agreement of the parties with respect to the processing of personal data by QINSIGHTS BV when the customer uses QInsights in accordance with these GTC/EULA.

1.2 The DPA forms an integral part of the GTC. Upon the customer's consent to these GTC/EULA, the DPA shall also become effective between the parties.

1.3 In the event of any conflict or inconsistency between the DPA and these GTC/EULA, the DPA shall prevail to the extent of such conflict or inconsistency.

2. Standard contractual clauses

2.1 If the customer is located in a country outside the European Economic Area for which the European Commission has not issued an adequacy decision, **Schedule 2** shall further apply to the customer's use of QInsights in accordance with these GTC/EULA.

2.2 **Schedule 2** to these GTC/EULA contains the European Commission's standard contractual clauses in the form of Module 4 (Transfer from a Processor to a Controller) ("**SCC**").

2.3 The SCC form an integral part of the GTC. Upon the customer's consent to these GTC, the SCC shall also become effective between the Parties.

3. Definitions

Terms not otherwise defined in the DPA and/or the SCC shall have the meaning set out in the GDPR.

4. Information for the DPA and SCC

4.1 The following information contains the relevant information for Annex II of the DPA and Annex I Section B of the SCC:

Categories of data subjects whose personal data are processed

All persons whose personal data is contained in the documents provided by the customer for document analysis via QInsights.

Categories of personal data processed

All data contained in the documents provided by the customer for document analysis via QInsights.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Targeted processing of sensitive personal data as defined in Art. 9 (1) GDPR does not occur. If a

text submitted by the customer nevertheless contains such data, the customer may transmit it only if:

- the affected individual has been duly informed in accordance with Articles 13 and 14 GDPR prior to transmission
- valid consent within the meaning of Article 9(2)(a) GDPR has been obtained or another permitted basis under Article 9(2) GDPR applies, and
- the processing is necessary for the specific purpose for which it is carried out.

If these conditions are not met, the customer shall pseudonymize or anonymize sensitive data before uploading it, provided that pseudonymization or anonymization does not conflict with the intended purpose of processing.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuously during the customer's use of QInsights.

Nature of the processing

Automated document analysis using artificial intelligence.

Pupose(s) of the data transfer and further processing

Automated document analysis using artificial intelligence.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data provided by the customer will be processed for the duration of the contractual relationship. To protect the data and to comply with data protection principles, customer accounts that have been inactive for a longer period of time are automatically deleted.

In the case of processing by (sub)processors, subject matter, nature and duration of the processing.

When using QInsights, data is stored on a cloud server and forwarded to a service provider for further processing using artificial intelligence. A regularly updated list of the service providers used can be found here: https://www.qinsights.ai/privacy The processing serves the document analysis by the used service provider. The data will in turn be deleted immediately by the service provider after the need for processing has ceased.

4.2 The following information contains the relevant information for Annex I Section A of the SCC:

Activities relevant to the data transferred under these clauses: Provision of QInsights

§ 8 Warranty and liability

a) The document analyses are generated by QINSIGHTS BV with the help of a service provider on the basis of artificial intelligence. Accordingly, typical inaccuracies and errors are to be expected. QINSIGHTS BV does not guarantee the accuracy, correctness, completeness and/or reliability of the document analyses.

b) QINSIGHTS BV is liable without limitation for intent and gross negligence as well as for slight negligence in the event of damage resulting from injury to body, life or health. In other cases of slight negligence, QINSIGHTS BV is only liable in the event of a breach of such obligations that make the reasonable and proper performance of the contract possible in the first place and on the fulfilment of which the customer accordingly relies on and may rely (cardinal obligations) and only limited to compensation for the foreseeable, typically occurring damage. Other claims for damages are excluded. Furthermore, limitations and exclusions in this clause do not apply to claims by the customer in the event of fraudulent concealment of a defect by QINSIGHTS BV due to the absence of an assured characteristic, the breach of a warranty promise and claims in accordance with §§ 1, 4 of the Product Liability Act.

c) Notwithstanding the preceding paragraph, warranty and liability are excluded for consequences arising from the customer making changes to QInsights itself or with the help of a third party or operating QInsights improperly or incorrectly.

d) QINSIGHTS BV does not accept any liability for the loss of data, unless QINSIGHTS BV caused the loss intentionally or through gross negligence and the customer had taken reasonable precautions to ensure that a data backup was carried out according to the latest technological standards and at appropriate intervals (at least once per day), so that the data could reasonably be reconstructed.

e) QINSIGHTS BV is not liable to the customer for delays in performance resulting from force majeure, namely circumstances beyond QINSIGHTS BV's control. The same applies if QINSIGHTS BV is unable to provide its service in accordance with these GTC/EULA due to a lack of information or cooperation from the customer.

f)Any further liability is excluded, irrespective of the legal grounds.

g) Insofar as QINSIGHTS BV's liability is excluded or limited, this also applies to the personal liability of QINSIGHTS BV's employees, representatives and vicarious agents.

§ 9 High-risk activities

QInsights is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the software could lead directly to death, personal injury, or severe physical or property damage (collectively, High Risk Activities). QINSIGHTS BV expressly disclaims any express or implied warranty of fitness of QInsights for high-risk activities.

§ 10 Copyright

1. QInsights is protected by Dutch copyright law and international copyright treaties as well as by other laws and treaties on intellectual property..

2. The ownership and copyright exploitation rights in QInsights (including but not limited to images, photographs, animations, video, audio, music, text and "applets" contained in QInsights), the printed accompanying material and all copies of QInsights are owned by QINSIGHTS BV.

3. By using QInsights, the customer does not acquire any rights to the intellectual property of QInsights apart from the rights of use granted to him/her on the basis of these GTC/EULA.

§ 11 Special conditions for traders

The following provisions apply exclusively to professional customers—that is, natural or legal persons acting in the course of their trade, business, craft, or professional activities—and not to consumers. This includes, in particular, universities, research institutions, companies, self-employed professionals, and other organisations acting for professional or institutional purposes.Scope of application

1.1 These GTC/EULA apply exclusively; QINSIGHTS BV does not recognise any terms and conditions of the customer that conflict with or deviate from these GTC/EULA unless QINSIGHTS BV has expressly agreed to their validity in writing. These GTC/EULA also apply if QINSIGHTS BV executes the customer's order without reservation in the knowledge that the customer's terms and conditions conflict with or deviate from these GTC/EULA.

1.2 All agreements made between QINSIGHTS BV and the customer for the execution of an order must be made in writing or in text form (e.g. by e-mail or letter).

2. Prices and terms of payment for orders outside the webshop

2.1 For delivery the prices stated in QINSIGHTS BV's offer at the time of the order apply.

2.2 Orders from European countries must be placed in EURO; orders in US dollars are not permitted.

2.3 Unless otherwise stated, the prices quoted are exclusive of VAT (which shall be shown separately on the invoice at the statutory rate on the date of invoicing), but inclusive of shipping or transport costs to the agreed place of delivery.

2.4 Payment of the purchase price is due immediately after conclusion of the contract. Payments must be made by the methods listed on the website; other methods of payment require the prior consent of QINSIGHTS BV. With the exception of purchases on account, payment is made before delivery. Annual licences must be paid for in full in advance for the entire licence period. If the customer has purchased products or services with recurring payment obligations (subscriptions), the prices are due at the agreed interval.

2.5 The deduction of cash discount is subject to a prior separate agreement.

2.6 In the case of purchases on account, the invoice amount shall be paid without deduction immediately upon receipt of the invoice, unless otherwise stated in the order confirmation. The customer shall bear any costs of money transfer itself.

2.7 Should the customer be in default of payment, QINSIGHTS BV is entitled to demand interest on arrears and a further lump sum of EUR 40.00, unless the customer can prove that no damage or lower damage has been incurred. The interest rate shall be 9 (nine) percentage points higher than the given base rate. If QINSIGHTS BV is able to prove higher damages caused by the default, QINSIGHTS BV is entitled to claim these damages. Any lump sum already claimed under this provision shall be credited towards the claim for damages.

2.8 The customer shall only be entitled to offset rights if his counterclaims have been legally established or acknowledged by QINSIGHTS BV. The customer is only entitled to exercise a right of retention to the extent that his counterclaim is based on the same contractual relationship.

2.9 If the customer is in default of acceptance or if they violate other cooperation obligations, QINSIGHTS BV is entitled to demand damages incurred, including possible additional charges. In this case, the risk of accidental loss or accidental deterioration of the contractual item also passes to the customer at the time at which the latter is in default of acceptance.

3. Right of Revocation

A serious breach by the Customer of the GTC/EULA entitles QINSIGHTS BV to revoke the contract with the Customer.

4. Warranty and limitation of liability

In addition to § 8, the following provisions on warranty and limitation of liability shall apply to the acquisition and use of QInsights:

4.1 The customer is not entitled to remedy defects itself and to demand reimbursement of the

expenses required for this unless the customer has properly notified QINSIGHTS BV of the defect and provided QINSIGHTS BV with the information required to reproduce the defect and QINSIGHTS BV has not remedied the defect within a reasonable period of time.

4.2 Claims for compensation for damages and expenses for reimbursement shall become time barred within 12 months. This 12-month period begins at the earliest with the notification of the defect by the Customer and at the latest at the end of the year in which the Customer recognized the defect or could have recognized it without negligence.

4.3 QINSIGHTS BV is not liable for damage that has not occurred to QInsights itself; in particular, QINSIGHTS BV is not liable for lost profits of the customer that are attributable to the use of the products.

5. Miscellaneous

5.1 QINSIGHTS BV is authorised to name the client as a reference for the purpose of external presentation on the website. This may also include the use of the logo (corporate identity), with which the customer agrees. QINSIGHTS BV reserves the right to name the reference up to 3 calendar years after termination of the contract.

5.2 For contracts with merchants, legal entities under public law or special funds under public law, the place of fulfilment for delivery and payment as well as the place of jurisdiction shall be the registered office of QINSIGHTS BV in Rotterdam, Netherlands

§ 12 Special conditions for consumers (Withdrawal)

The provisions of Section 12 apply only where the customer acts as a consumer within the meaning of Article 6:230g(1)(a) of the Dutch Civil Code (Burgerlijk Wetboek), namely as a natural person acting for purposes outside their trade, business, craft or professional activity.

1. Right of withdrawal

1.1 You have the right to withdraw from this contract within 14 days without giving any reason. The withdrawal period will expire after 14 days from the day of the conclusion of the contract.

1.2 To exercise the right of withdrawal, you must inform us, (QINSIGHTS BV, Bierstraat 123c, 3011XA Rotteram, The Netherlands, Tel.: +31 (0)6 39205531, E-Mail: support@qinsights.ai, of your decision to withdraw from this contract by an unequivocal statement (e.g. a letter sent by post or email). You may use the model withdrawal form below, but it is not obligatory.

1.3 To meet the withdrawal deadline, it is sufficient for you to send your communication concerning your exercise of the right of withdrawal before the withdrawal period has expired.

2. Effects of withdrawal

2.1 If you withdraw from this contract, we shall reimburse to you all payments received from you,

including the costs of delivery (with the exception of the supplementary costs resulting from your choice of a type of delivery other than the least expensive type of standard delivery offered by us), without undue delay and in any event not later than 14 days from the day on which we are informed about your decision to withdraw from this contract. We will carry out such reimbursement using the same means of payment as you used for the initial transaction, unless you have expressly agreed otherwise; in any event, you will not incur any fees as a result of such reimbursement.

2.2 You are only liable for any diminished value of the goods resulting from the handling other than what is necessary to establish the nature, characteristics and functioning of the goods.

3. Important note

Under Article 6:230p(g) of the Dutch Civil Code (Burgerlijk Wetboek), the right of withdrawal for digital content not supplied on a tangible medium expires once performance has begun, provided that the consumer has given prior express consent to the commencement of performance and has acknowledged that this results in the loss of the right of withdrawal.

QINSIGHTS BV began with the performance of the contract,

1. the consumer had expressly consented to QINSIGHTS BV beginning with the performance of the contract prior to expiry of the withdrawal period,

2. the consumer had acknowledged that by their consent, they would lose the right to withdraw from the contract upon the performance of the contract having commenced, and

3. QINSIGHTS BV has provided the consumer with a confirmation of the contract.

QINSIGHTS BV begins with the execution of the contract in the sense described above at the time when the consumer uploads a document via the QInsights Account and starts a document analysis by QInsights.

4. Model withdrawal form

(Complete and return this form only if you wish to withdraw from the contract).

To: QINSIGHTS BV https://www.qinsights.ai/privacy e-mail: support@qinsights.ai:

I/We (*) hereby give notice that I/We (*) withdraw from my/our (*) contract of sale of the following goods (*)/for the provision of the following service (*),

Ordered on (*)/received on (*),

Name of consumer(s),

Address of consumer(s),

Signature of consumer(s) (only if this form is notified on paper),

Date

(*) Delete as applicable

§ 13 Final provisions

2. The law of the Netherlands shall apply. The provisions of the Vienna UN Convention for the International Sale of Goods (CISG) of 11.04.1980 on contracts for the international sale of goods (UN Sales Convention) shall not apply. The statutory provisions on the limitation of the choice of law and on the applicability of mandatory provisions of the state in which the customer has his/her habitual residence as a consumer shall remain unaffected. Insofar as permitted by law, the exclusive place of jurisdiction for all disputes arising from or in connection with these GTC/EULA is Rotterdam.

3. Under Article 6:230p(g) of the Dutch Civil Code (Burgerlijk Wetboek), the consumer has no right of withdrawal in respect of digital content not supplied on a tangible medium once performance has begun, provided that:

   - the consumer has given prior express consent for performance to begin;
   - the consumer has acknowledged that this means waiving the right of withdrawal; and
   - the trader has provided the consumer with confirmation of that consent and acknowledgement as required by law.

4. Should a provision in these GTC/EULA or a provision within the scope of other agreements be or become invalid, this shall not affect the validity of all other agreements or provisions. The statutory provision shall apply in place of the invalid provision.

5. QINSIGHTS BV is entitled to unilaterally amend these GTC/EULA if there is a valid reason for doing so (e.g. in the case of a necessary adjustment to changes in the legal or technical framework conditions). Customers will be informed of an amendment in advance by e-mail, stating the content of the amended provisions. If the customer does not object to the notification of amendment within 4 weeks after receipt of the e-mail, the amended provisions shall be deemed agreed.

6. The language of the contract shall be English. These GTC/EULA have been drawn up in English..

Schedule 1

Commission Implementation decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Art. 28

1.1 (7) GDPR STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

1.1.1 Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

1.1.2 Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

1.1.3 Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

1.1.4 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

1.1.5 Docking clause

[intentionally left blank]

1.2 SECTION II - OBLIGATIONS OF THE PARTIES

Clause 6

1.2.1 Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

1.2.2 Obligations of the Parties

1.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

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

1.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

1.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

1.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

1.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

1.6. Documentation and compliance

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

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

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the-processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

1.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least five business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub- processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub- processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub- processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the subprocessor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor

whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

1.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub- processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

1.2.3 Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8 (b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies 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 controller to

mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

1.2.4 Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

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

(1) 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;

(2) the likely consequences of the personal data breach;

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

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject,

when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least: a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

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

(b) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

1.3 SECTION III - FINAL PROVISIONS

Clause 10

1.3.1 Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

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

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

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

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

1.4 ANNEX I - LIST OF PARTIES

1.4.1 Controller:

The controller is the customer in accordance with the General Terms & Conditions (GTC) and End User License Agreement (EULA) of QINSIGHTS BV.

Signature and accession date: Effective with agreement to the General Terms & Conditions (GTC) by the customer.

1.4.2 Processor:

Name: QINSIGHTS BV

Address: Bierstraat 123c, 3011 XA Rotterdam, NL.

Contact person's name, position and contact details: The data protection officer of QINSIGHTS BV can be reached at support@qinsights.ai.

Signature and accession date: Effective with agreement to the General Terms & Conditions (GTC) by the customer.

1.5 ANNEX II - DESCRIPTION OF THE PROCESSING

See relevant information in the data protection section of these GTC/EULA.

1.6 ANNEX III - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

1. Measures for the security of processing (Art. 32 para. 1 GDPR)

1.1 Access control

Measures suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used.

- Alarm system
- Security locks

- Locking system with code card
- Bell system with camera
- Visitors' book
- Care in the selection of security staff
- Care in the selection of the cleaning service

1.2 Access control

Measures suitable for preventing data processing systems (computers) from being used by unauthorised persons.

- Login with user name + password
- Use of anti-virus software
- Use of firewall software
- Use of VPN for remote access
- Creation of user profiles
- Assignment/administration of user authorisations
- Allocation of passwords
- Guidelines for: "Secure password" and "Delete/Destroy"

1.3 Access control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

- Use of shredders
- Physical erasure of data media
- Proper destruction of data media (DIN 32757)
- Logging of access to applications, specifically when entering, changing and deleting data
- Administration of rights by system administrator

- Number of administrators reduced to the "bare minimum"

1.4 Segregation control

Measures to ensure that data collected for different purposes can be processed separately.

- Separation of development and test environment
- Strictly separate storage of data in different client systems
- Providing data records with purpose attributes/data fields
- Determination of database rights
- Control via authorisation concept

1.5 Pseudonymisation

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures:

- Internal instruction to anonymise / pseudonymise personal data where possible in the event of disclosure.

2. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

2.1 Data Protection measures

- Software solutions for data protection management in use
- Central documentation of all procedures and regulations on data protection with access for employees as required / authorised on the intranet
- Regular review of the effectiveness of the technical protection measures
- Staff training: trained and committed to confidentiality/data secrecy
- Data protection impact assessment is carried out as required
- QINSIGHTS BV complies with the information obligations according to Art. 13 and 14 GDPR

- Formalised process for processing requests for information from data subjects is in place.

2.2 Incident response management

Support in responding to security breaches

- Documentation of security incidents and data breaches, e.g. via the ticket system.
- All employees are instructed and trained to ensure that data protection incidents are recognised and reported immediately to the DPO.

2.3 Order control (outsourcing to third parties)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

- Selection of the contractor under due diligence aspects (in particular with regard to information security).
- Regular monitoring of contractors
- The principle of necessity and data minimisation is taken into account.
- The necessary agreements on commissioned processing or EU standard contractual clauses are concluded.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller:

The current version of the security standards of the respective third-party service provider apply. A regularly updated list of the service providers used can be found here: https://www.qin-sights.ai/privacy

2 Schedule 2

Commission implementing decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

Standard Contractual Clauses MODULE

FOUR: Transfer processor to controller

2.1 SECTION I

Clause 1

2.1.1 Purpose and scope

(1)The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(2)The Parties:

(1) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(2) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer"),

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(3) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(4) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

2.1.2 Effect and invariability of the Clauses

(5) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or

processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(6) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

2.1.3 Third-party beneficiaries

(7) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions

(1) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(2) Clause 8.1 (b) and Clause 8.3(b);

(3) [intentionally left blank];

(4) [intentionally left blank];

(5) Clause 13;

(6) Clause 15.1(c), (d) and (e);

(7) Clause 16(e);

(8) Clause 18.

(8) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

2.1.4 Interpretation

(9) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(10) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(11) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

2.1.5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

2.1.6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

2.1.7 Docking Clause

[intentionally left blank]

2.2 SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

2.2.1 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(12) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(13) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(14) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub- processing or as regards cooperation with competent supervisory authorities.

(15) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(16) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data7, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(17) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(18) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

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

(20) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

2.2.2 Use of sub-processors

[intentionally left blank]

Clause 10

2.2.3 Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

2.2.4 Redress

(21) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

2.2.5 Liability

(22) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(23) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(24) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(25) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(26) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

2.2.6 Supervision

[intentionally left blank]

2.3 SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

2.3.1 Local laws and practices affecting compliance with the Clauses

[intentionally left blank]

Clause 15

2.3.2 Obligations of the data importer in case of access by public authorities

[intentionally left blank]

2.4 SECTION IV – FINAL PROVISIONS

Clause 16

2.4.1 Non-compliance with the Clauses and termination

(27) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(28) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(29) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(1) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(2) the data importer is in substantial or persistent breach of these Clauses; or

(3) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(30) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(31) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which

the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

2.4.2 Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

Clause 18

2.4.3 Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of The Netherlands.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

2.4.4 Data exporter:

Name: QINSIGHTS BV

Address: Bierstraat 123c, 3011 XA Rotterdam, NL

Contact person's name, position and contact details: The data protection officer of QINSIGHTS BV can be reached at support@qinsights.ai

Activities relevant to the data transferred under these Clauses: See relevant information in the respective sections on data protection of these GTC/EULA.

Signature and date: Effective with agreement to the General Terms & Conditions (GTC) and End User License Agreement (EULA) by the customer.

Role (controller/processor): Processor

2.4.5 Data importer:

The controller is the customer in accordance with the General Terms & Conditions (GTC) and End User License Agreement (EULA) of QINSIGHTS BV.

Activities relevant to the data transferred under these Clauses: See relevant information in the section on data protection of these GTC/EULA.

Signature and date: Effective with agreement to the General Terms & Conditions (GTC) and End User License Agreement (EULA) by the customer.

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

See relevant information in the data protection section of these GTC/EULA.

3 Annex Technical and Organisational Measures

3.1 Scope

QInsights B.V. implements the following technical and organisational measures to ensure a level of security appropriate to the risks associated with the processing of personal data.

The measures apply to personal data processed in connection with the QInsights platform, including Customer Content uploaded by customers, account information, technical data and related service information.

The measures are reviewed and updated where necessary, taking account of:

- the state of the art;
- implementation costs;
- the nature, scope, context and purposes of processing;
- the sensitivity of the personal data;
- the likelihood and severity of risks to data subjects; and
- changes to the QInsights service and its infrastructure.

3.2 Physical Access and System Access Control

QInsights is provided as a cloud-based software service. Customer Content is hosted by contracted cloud infrastructure providers and is not stored on publicly accessible local systems.

Physical security of data-centre infrastructure is managed by the relevant hosting providers, currently including Hetzner Online GmbH and Google Cloud EMEA Limited.

The providers apply physical security measures appropriate to data-centre operations, including restricted facility access, monitoring and environmental safeguards.

Access to QInsights systems is restricted through authentication mechanisms.

Measures include:

- individual user accounts;
- username and password authentication;
- password requirements;
- Multifactor authentication for all users optional
- restricted administrative access;
- user access rights based on operational necessity;
- firewall and network-security controls;

- secure remote access mechanisms where required; and
- antivirus and endpoint-protection measures on administrative devices.

3.3 Authorisation and Access-Control Concept

Access to personal data is limited to authorised persons who require access for the performance of their duties.

QInsights applies the principle of least privilege. Administrative privileges are limited to the minimum number of authorised persons necessary to operate and maintain the service.

Measures include:

- role-based assignment of permissions;
- separation between ordinary user access and administrative access;
- restricted access to production systems;
- allocation and administration of access rights by authorised administrators;
- removal or adjustment of access rights when roles change;
- termination of access when a person no longer requires it;
- logging of relevant administrative access and changes; and
- periodic review of access permissions.

Customer users may access only the projects and data made available within their own account or organisational workspace.

QInsights personnel do not routinely access Customer Content. Access may occur only where necessary for:

- customer-requested support;
- technical troubleshooting;
- investigation of a security incident;
- maintenance of the service; or
- compliance with a legal obligation.

3.4 Encryption and Transmission Security

Personal data processed through QInsights is protected during transmission and storage.

Measures include:

- encryption of data in transit using Transport Layer Security;
- encrypted communication between relevant system components;

- encryption of data at rest using AES-256 or equivalent encryption provided by the hosting infrastructure;
- use of encrypted transport protocols for communication between user devices, data centres and service providers; and
- secure API connections to AI and transcription providers.

Customer Content transferred to Microsoft Azure OpenAI Service or AssemblyAI is transmitted through encrypted connections.

QInsights does not make Customer Content publicly accessible.

3.5 Tenant and Data Segregation

Customer Content is logically separated from the data of other customers.

Measures include:

- separation of customer accounts and projects;
- access controls based on account, organisation and project permissions;
- logical segregation within the application and database;
- separation of production, development and test environments;
- restricted database permissions;
- prohibition on using production Customer Content in development or testing unless specifically authorised; and
- transfer of data to service providers only where required for the selected function.

Customer Content is not shared with other customers.

QInsights applies data minimisation by limiting each provider's access to the data required for the relevant service. For example:

- Microsoft Azure OpenAI Service receives only the data required to generate the requested analysis;
- AssemblyAI receives audio or video files only when a customer requests transcription; and
- Paddle does not receive Customer Content.

3.6 Availability, Backup and Recovery

QInsights uses cloud infrastructure designed to support the availability and resilience of the service.

Measures include:

- hosting with established cloud infrastructure providers;

- system monitoring;
- redundancy and availability measures provided by the hosting environment;
- backup procedures (once per day);
- recovery procedures for system or data loss;
- protection against accidental destruction or loss; and
- procedures for restoring service following an operational incident.

3.7 Logging and Monitoring

QInsights maintains logging and monitoring measures to support security, system operation and investigation of incidents.

Measures include:

- recording relevant login events;
- recording administrative access and changes;
- logging application events;
- monitoring system availability and performance;
- detection of unusual or unauthorised activity;
- documentation of security incidents;
- retention of logs for security and troubleshooting purposes; and
- review of logs where an incident or technical problem is suspected.

Logs are accessible only to authorised personnel and are not used for unrelated purposes.

3.8 Deletion and Retention

Personal data is retained only for as long as necessary for the purposes for which it is processed, unless a longer period is required by law or contract.

Customers control which Customer Content they upload to QInsights.

Measures include:

- deletion of projects and files through the QInsights service or upon customer request;
- deletion of Customer Content from active systems after the relevant retention period;
- restricted retention of data in backups until the backup cycle is completed;
- retention of billing and transaction information where required by tax or accounting law;
- deletion or anonymisation of data that is no longer required; and

- contractual deletion obligations for subprocessors.

Customer Content is retained for the duration of the customer's active account unless the customer deletes it earlier.

3.9 Microsoft Azure OpenAI Service

Data submitted to Microsoft Azure OpenAI Service is processed only to generate the requested output.

Customer prompts, completions, embeddings and uploaded data are not made available to OpenAI and are not used to train Microsoft or third-party foundation models without the customer's permission or instruction.

3.10 AssemblyAI

Audio and video files are transferred to AssemblyAI only when the customer requests transcription.

The files are processed for the purpose of producing transcripts, timestamps and speaker information.

Data uploaded to AssemblyAI is not retained and is removed immediately after inference is provided.

3.11 Incident Management

QInsights maintains procedures for detecting, reporting, assessing and responding to information-security incidents and personal-data breaches.

Measures include:

- internal reporting procedures for suspected incidents;
- documentation of security incidents and personal-data breaches;
- assessment of the scope and impact of an incident;
- containment and remediation measures;
- preservation of relevant evidence and logs;
- identification of affected systems and data;
- cooperation with subprocessors;
- notification of affected customers without undue delay where required;
- assistance to customers with their obligations under Articles 33 and 34 GDPR; and
- review of incidents to identify corrective and preventive measures.

Employees and contractors are instructed to report suspected incidents immediately.

Responsible incident-response contact: Wissem Golli, Email: w.golli@qinsights.ai

3.12 Personnel and Confidentiality

Access to personal data is limited to personnel who require it for their assigned responsibilities.

Measures include:

- confidentiality obligations for employees and contractors;
- data-protection and security instructions;
- training on recognising and reporting security incidents;
- restricted access according to job responsibilities;
- careful selection of employees and contractors;
- termination of access when no longer required; and
- internal policies concerning passwords, data handling and deletion.

Authorised personnel are required to process personal data only in accordance with QInsights' instructions and applicable contractual obligations. All employees and contractors sign confidentiality agreements.

3.13 Subprocessors and Vendor Management

QInsights engages subprocessors only where necessary to provide the service.

Current providers include (see also Compliance document)

- Hetzner Online GmbH for cloud infrastructure;
- Google Cloud EMEA Limited for infrastructure;
- Microsoft Ireland Operations Limited for Microsoft Azure and Azure OpenAI Service;
- AssemblyAI, Inc. for transcription; and
- Paddle.com Market Limited as Merchant of Record for payment and subscription processing.

Before engaging a provider, QInsights assesses the provider with regard to:

- information security;
- privacy and data-protection practices;
- processing locations;
- contractual safeguards;
- confidentiality;
- data-retention practices;

- use of customer data for model training;
- applicable certifications; and
- international-transfer mechanisms.

Subprocessors processing Customer Content are contractually bound by data-protection obligations that are materially equivalent to those imposed on QInsights.

QInsights maintains an up-to-date subprocessor list and informs customers via email of material additions or replacements in accordance with the DPA.

Sup-processors are reviewed yearly.

3.14 1Review, Assessment and Continuous Improvement

QInsights regularly reviews the appropriateness and effectiveness of its technical and organisational measures.

Measures include:

- review of technical safeguards;
- review of access rights;
- review of subprocessors;
- monitoring of changes to applicable data-protection requirements;
- assessment of new service providers before use;
- assessment of new AI models before deployment;
- review of security incidents and corrective measures;
- updates to policies and procedures;
- staff training; and
- data-protection impact assessments where required.

Before introducing a new AI model or provider that processes Customer Content, QInsights assesses:

- processing location;
- data retention;
- model-training practices;
- security controls;
- contractual protections;
- international-transfer implications; and
- compatibility with the QInsights DPA and Privacy Policy.

Customers are informed of relevant changes in accordance with the DPA and applicable contractual obligations.

TOMs are formally reviewed annually. This is the responsibility of Susanne Friese, email: s.friese@qinsights.ai

Currently, Qinsights does not hold any independent security certificates.

3.15 Data Protection by Design and Data Minimisation

QInsights applies data-protection-by-design and data-minimisation principles in the development and operation of the service.

Measures include:

- customers select which data they upload;
- only data required for the requested function is transmitted to the relevant provider;
- Customer Content is not used to train underlying AI models;
- customers may anonymise data before upload;
- QInsights provides an offline anonymisation tool, which operates entirely on the customers' device without sending the source files to Qinsights.
- access is restricted according to role and operational necessity;
- Customer Content is separated from other customers' data; and
- data is deleted when no longer required.

The customer remains responsible for determining whether personal data, including special-category data, is necessary for the relevant research purpose.

3.16 Special-Category Research Data

Customer Content may include special categories of personal data within the meaning of Article 9 GDPR.

QInsights processes such data solely:

- on behalf of the customer;
- according to the customer's documented instructions;
- for the purpose of providing the requested QInsights service; and
- subject to the security measures described in this document.

The customer, as data controller, is responsible for:

- identifying an appropriate legal basis under Articles 6 and 9 GDPR;
- determining whether the processing constitutes scientific research;

- implementing safeguards required under Article 89 GDPR or applicable national law;
- informing data subjects where required;
- ensuring that uploaded data is limited to what is necessary; and
- applying anonymisation or pseudonymisation where appropriate.

QInsights does not determine the research purpose, select research participants or decide which categories of personal data are uploaded.