idiligo | PROCESSING AGREEMENT

The following Agreement is concluded between

Customer / Company
Responsible person
Postal address

- hereinafter: Client

as well as

Idiligo B.V.
Kabelweg 57
NL-1014 Amsterdam

- hereinafter: Processor.

§ 1 Preamble

The Contracting Parties are planning or already maintain a business relationship. This Agreement specifies in detail the obligations of the Contracting Parties with regard to data protection that result from the underlying agreement (hereinafter: "Main Agreement") in their processing described in detail. The activity described in the aforementioned agreement is data processing activities. Therefore, it is necessary that the Contracting Parties conclude an agreement for data processing as per Art. 28 of the EU General Data Protection Regulation (GDPR).
This Agreement applies to all activities in connection with the Main Agreement and for which the employees of the Processor or its agents process personal data of the Client.

§ 2 Responsibility

(1) Within the scope of this Agreement the Client is responsible for compliance with statutory regulations, in particular for the legality of data processing ("Controller" in accordance with Art. 4 (7) GDPR).
(2) The Processor itself shall maintain records of the processing activities carried out under its responsibility in accordance with Art. 30 GDPR. The Processor shall on request provide the Client with the disclosures necessary for an overview pursuant to Art. 30 GDPR.
(3) Insofar as the Processor in breach of this Agreement and of the GDPR determines the purposes and means of processing itself, the Processor shall be deemed to be the controller for this processing in accordance with Art. 4 (7) GDPR.

§ 3 Definitions

(1) A “processor” is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
(2) “Personal data” means any information relating to an identified or identifiable natural person (“data subject”);
(3) “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
(4) “Instruction” is an order of the Client directed at a certain handling of personal data with regard to data protection (for example, anonymisation, blocking, erasing, surrender) of the Data Processor.
(5) “Subcontractor” is every additional processor of the processor in accordance with Art. 28 (4) GDPR
(6) “Third party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
(7) “Third country” is a country outside the European Union and the European Economic Area.

§ 4 Subject and duration of the order/processing

(1) The subject of the order results from the Main Agreement, which is referred to here.
(2) Insofar as the subject does not result or does not result in full from the Main Agreement the subject of processing is: Idiligo B.V. Grants the Client a non-transferable, non-exclusive licence for the use of the Idiligo application, as per the provisions of the “General Terms and Conditions, 3. Licence and Use” of Idiligo B.V., in detail
    a) Idiligo provides access to the Idiligo application (user log-in via the Idiligo B.V. website).
    b) The Idiligo application enables the Client to set up its own users for its Idiligo account.
    c) The Client can develop and use independent scripts. It can, for example, also document client-specific information with these scripts.
    d) The Client shall receive access to its documented information.
(3) The term of the order shall be oriented on the term of the Main Agreement, provided nothing to the contrary results from the provisions of this Agreement.
(4) The right to termination without notice with good cause remains unaffected.

§ 5 Scope, type and purpose of processing as well as the type of personal data and categories of data subjects

(1) Insofar as the scope, type and purpose of processing do not result from the Main Agreement the following provisions apply in addition.

(2) The following data shall be constituents of the data processing in detail in particular

Type of data	Categories of data subjects of the Client
Personal master data	Customers
Contact data (email, telephone)	Employees
Customer data	Potential customers
Communications data (audio and video streaming, screen sharing)	Applicants
Contents data (files divided into scripts, text chat, whiteboard contents)	Suppliers
Activity reports (log files)	Subscribers
Signature data (characteristics of the digital signature)	Contractor
Contractual data (underlying legal documents in the event of a digital signature)	Agents / Partners
Calendar data (date, duration)	Independently employed employees
	Interlocutors of the Client
Support ticket data (messages and chat records between users and the contractor within the scope of support enquiries)	
Meta data (usage statistics) • Activity reports (log files) • IP addresses • Cookies • API traffic • Control/Signalling traffic • Media server log files • Platform access log files	

§ 6 Authority to issue instructions

(1) The Processor shall process personal data exclusively within the scope of the agreements made and in accordance with documented instructions of the Client unless an exception pursuant to Art. 28 (3) a GDPR applies.

Insofar as the Client deems it necessary authorised persons can be appointed. The Client shall notify the Processor of these persons in writing or in text form. In the event these authorised persons of the Client change the Processor shall be notified in writing or in text form with a specification of the new person(s).

(2) Instructions shall initially be set by the Main Agreement and can subsequently be amended, supplemented or replaced by individual instructions given by the Client in writing or in an electronic format (text form) notified to the position designated by the Processor (individual instruction). Instructions that are not provided in the Main Agreement shall be treated as an application to amend performance.

(3) Verbal instructions shall be confirmed in writing or in text form without delay.

(4) The Processor shall inform the Client without delay if in its opinion an instruction breaches applicable laws. The Processor may suspend implementation of the instruction until it has been confirmed or amended by the Client.

(5) The Processor guarantees that it is prohibited for employees involved with the processing of the data and for other persons employed for the Processor to process the data outside the relevant authorisation.

(6) Any amendments to the subject of processing and procedural amendments are covered by the authorisation of the Client and shall be documented accordingly. In the event of any amendment to the order that is deemed to be material by the Processor, the Processor shall have the right to object. If despite the objection of the Processor the Client insists on the amendment this amendment shall be deemed to be good cause and shall allow the immediate termination of the Processing Agreement affected by the instruction as well as the constituents of the Main Agreement affected by the Processing Agreement.

Any amendments to the subject of processing and procedural amendments are covered by the authorisation of the Client and shall be documented accordingly. In the event of any material amendment to the order the Processor shall have the right to object. If despite the objection of the Processor the Client insists on the amendment this amendment shall be deemed to be good cause and shall allow the immediate termination of the Processing Agreement affected by the instruction as well as the constituents of the Main Agreement affected by the Processing Agreement.

§ 7 Place of performance / Transmission to third countries

The Processor shall provide the contractual performances in the European Union (EU) or in the European Economic Area (EEA) or in a third country. Any subcontractors shall provide the relevant performances in the European Union (EU) or in the European Economic Area (EEA) or in a third country. If the Processor or a subcontractor provides any performances in a third country the Processor guarantees compliance with the requirements of the GDPR in this respect and shall prove this on demand by the Client.

(1) Provided the data processing pursuant to this Agreement and statutory requirements for processing personal data on behalf of a controller or for the transmission of personal data abroad may permissibly be carried out outside Germany, the Processor shall ensure compliance with and the implementation of the statutory requirements to safeguard an adequate level of data protection for outsourcing and for cross-border data traffic.

§ 8 Safeguarding data secrecy/confidentiality and business secrets

(1) The Processor guarantees that the persons authorised to process the personal data have been obliged to retain confidentiality or are subject to an appropriate legal obligation to retain secrecy. The obligation to retain confidentiality/secrecy also continues after the end of the order.

(2) The Processor is also obliged to treat all knowledge of business secrets and data security measures of the Client obtained within the scope of the contractual relationship as confidential.

(3) Furthermore, all persons of the Processor must be obliged to comply with the safeguarding of business secrets of the Client and must be referred to section 4 GeschGehG.

§ 9 Technical and organisational measures

(1) The Processor shall arrange internal organisation in its area of responsibility so that the special requirements of data protection are met. The Processor shall take technical and organisational measures to ensure the appropriate protection of the personal data of the Client that meet the requirements of the GDPR (Art. 28 (3) c, 32 GDPR).

(2) The Processor shall take such technical and organisational measures that ensure the permanent confidentiality, integrity, availability and resilience of the systems and services connected with the processing.

(3) The Processor guarantees it shall meet its obligations pursuant to Art. 32 (1) d GDPR and shall utilise a procedure regularly to review the effectiveness of the technical and organisational measures to guarantee the security of processing.

(4) The following shall be deemed to be agreed to ensure compliance with the agreed protective measures:

- With regard to compliance with the agreed protective measures and their audited effectiveness reference is made to the codes of conduct approved pursuant to Art. 40 GDPR to which the Processor agreed on 25 September 2020 and compliance with which was audited and confirmed on 6 October 2020.

(5) The Processor reserves the right to amend the security measures taken; however, it must be guaranteed that the minimum contractually agreed level of protection is maintained.

(6) The Processor shall document the implementation of the technical and organisational measures presented in advance of the award of the order that are required before the commencement of processing, in particular with regard to the concrete execution of the order, and shall surrender this documentation to the Client for review and approval.

(7) A presentation of the technical and organisational measures agreed is provided in Annex 1 to this Agreement.

§ 10 Subcontracting, additional processors (subcontractors)

(1) Subcontracting in accordance with this regulation is understood to be services that relate directly to the provision of performance from the Main Agreement. This does not include ancillary performances that the Processor utilises, for example, as telecommunications services, postal/transport services, maintenance and user services or the disposal of data carriers, as well as other measures to guarantee the confidentiality, availability, integrity and resilience of the hardware and software of data processing facilities.
In order to guarantee data protection and the data security of the Client's data, including for outsourced ancillary services, the Processor is, however, obliged to conclude appropriate and legally-compliant contractual agreements as well as to take control measures.

(2) The Client empowers the Processor to utilise additional processors (subcontractors) as per the paragraphs in section 10 of this Agreement. This empowerment is general written authorisation in accordance with Art. 28 (2) GDPR.

(3) The forwarding of the Client's personal data to a subcontractor and its initial activity are only permitted in compliance with all the conditions for subcontracting.

(4) If a subcontractor provides the agreed performance outside the EU/EEA the Processor shall take appropriate measures to ensure data protection is carried out in a legally permissible manner. The same applies if service providers are used in accordance with paragraph 1 (2).

(5) Any further outsourcing by the subcontractor requires the explicit agreement of the Main Client (in text form at least). All the contractual regulations in the contractual chain must also be imposed on the additional subcontractors.

(6) At the time of the conclusion of this Agreement the companies detailed in Annex 3 are active for the Processor with sub-performances and also directly process and/or use the Client's data in this connection. Consent for these subcontractors to carry out activities is deemed to be issued.

(7) The Client may only object to the engagement of a subcontractor with good cause.

§ 11 Rectification, erasure and blocking of data

(1) During the current commission the Processor shall only rectify, erase or block data that is the subject of the Agreement in accordance with the instructions of the Client.

(2) Insofar as a data subject contacts the Processor directly for the purpose of the rectification, erasure or blocking of their data the Processor shall refer this attempt to the Client without delay.

§ 12 Support by the Processor with the obligations pursuant to Art. 12 – 23, 33-36 GDPR

(1) The Processor shall within the scope of its possibilities support the Client to meet enquiries and claims of data subject as per Art. 12- 23 GDPR (information obligations, rights of data subjects, right to be forgotten, right to data portability etc.)

(2) The Processor shall support the Client to fulfil the information obligations towards the competent supervisory authority or towards data subjects affected by a breach of the protection of personal data pursuant to Art. 33, 34 GDPR.

(3) The Processor shall support the Client in the data protection impact assessment pursuant to Art. 35 GDPR with all the information available to it. In the event of the necessity of a prior consultation with the competent supervisory authority pursuant to Art. 36 GDPR the Processor shall also support the Client here.

§ 13 Notification obligations of the Processor

(1) The Processor shall inform the Client without delay

a) in the event of any breaches committed by the Processor or by any persons employed by it within the scope of the order of regulations for the protection of the Client's personal data or of findings made in the Agreement. The Processor shall take the necessary measures to secure the data and to reduce possible disadvantageous consequences for data subjects and for this purpose shall reach agreement with the Client without delay;

b) if in its opinion an instruction breaches applicable laws

c) about control actions and measures of the supervisory authorities insofar as these relate to the subject of this Agreement. This also applies insofar as a competent government agency conducts investigations at the Processor within the scope of administrative or criminal proceedings with regard to the processing of personal data at the Processor.

(2) If the Client's data at the Processor is endangered by attachment or seizure as a result of insolvency or settlement proceedings or by any other third-party incidents or actions the Processor shall inform the Client of this without delay. The Processor shall inform all those responsible in this connection without delay that the control and ownership of this data rests exclusively with the Client as the "controller" in accordance with the General Data Protection Regulation.

§ 14 Return and erasure of data and data carriers at the end of the Agreement

(1) After the completion of the provision of processing performances the Processor must either erase or return all personal data at the choice of the Client, provided there is no obligation for the Processor to retain the personal data pursuant to Union law or the national law applicable to the Processor. The record of erasure shall be submitted on demand.

(2) Insofar as any transport of the storage medium is essential before erasure the Processor shall take appropriate measures to protect this, in particular against theft, unauthorised reading, copying or amendment. The measures and the erasure procedure to be applied shall if required be agreed in detail in addition to the service specifications.

(3) Documentation that provides evidence of correct data processing in accordance with the order shall be stored by the Processor in accordance with the relevant retention periods beyond the end of the Agreement. The Processor may meet its obligations at the end of the Agreement by surrendering this documentation to the Client.

(4) If it is not possible to return the data the Client shall inform the Processor of this in good time in writing. The Processor shall then be entitled to erase personal data on behalf of the Client.

(5) In the event of test and waste materials an individual commission with regard to erasure is not necessary; these must be erased.

§ 15 Control rights of the Client, and toleration and cooperation rights

(1) The Processor shall prove compliance with the obligations set in this Agreement to the Client by suitable means.

(2) The Processor can provide evidence by submission of the following information in particular:

a) Conducting an in-house audit
b) Attestation from an independent expert
c) Internal company codes of conduct including external evidence of compliance with these
d) Data protection and/or information security certificate (e.g. ISO 27001)
e) Codes of conduct approved pursuant to Art. 40 GDPR
f) Certificates pursuant to Art. 42 GDPR

(3) If an auditor commissioned by the Client is a competitor of the Processor, the Processor has the right to object to this auditor.

(4) The Processor shall support the conduct of order checks by means of regular audits by the Client with regard to the execution or fulfilment of the Agreement, in particular compliance with and any necessary adjustment of rules and measures to conduct the order. In particular, the Processor is obliged within an appropriate deadline to give the Client all information required to conduct controls on written demand, which may also be made in an electronic format.

(5) The Client shall inform the Processor in full and without delay if during the audit any errors or irregularities with regard to the provisions of data protection law are identified.

§ 16 Appointment of a Data Protection Officer

(1) The Processor shall appoint a Data Protection Officer provided the conditions of Art. 37 GDPR are met.

(2) Any change in the Data Protection Officer shall be reported to the Client without delay in writing or in text form. The Processor guarantees that the requirements of the Data Protection Officer and their activities as per Art. 38 GDPR are met.

(3) If no Data Protection Officer at the Processor is appointed the Processor shall specify a contact person for the Client.

(4) If the registered office of the Processor is outside the Union the Processor shall designate a representative in the Union pursuant to Art. 27 (1), (3) 2 GDPR.

(5) The persons to be specified pursuant to paragraphs 1 to 4 are named in Annex 2 to this Agreement.

§ 17 Liability

(1) The Client and the Processor shall be jointly liable for damage caused by processing that is not in accordance with the GDPR externally towards the relevant data subject.

(2) The Processor shall be liable exclusively for damage that relates to processing it has carried out during which

a) it did not meet obligations resulting from the GDPR and imposed especially on processors, or

b) it acted in non-compliance with the legally issued instructions of the Client, or

c) it acted contrary to the legally issued instructions of the Client.

(3) Insofar as the Client is obliged to pay compensation to a data subject, it is reserved the right to take recourse against the Processor.

(4) In the relationship between the Client and Processor the Processor shall be liable for damage caused by processing, however only if it

a) did not meet obligations especially imposed on it by the GDPR, or

b) acted in non-compliance with the legally issued instructions of the Client or contrary to these instructions.

(5) Any further claims to liability pursuant to general law remain unaffected.

§ 18 Written form clause

(1) Any amendments o supplements to this Annex and all its constituents – including any assurances given by the Processor – must be made in writing, which can also include an electronic format (text form), and an explicit indication that an amendment or supplement to these conditions is involved. This also applies to any waiver of this form requirement.

§ 19 Severability clause

(1) In the event of any objections to the regulations of this Agreement on data protection, the rules of the Main Agreement shall take precedence.

(2) Should any provisions of this Agreement prove to be ineffective or impracticable in full or in part or as a result of amendments to legislation after conclusion of the Agreement become ineffective or impracticable, this shall not affect the remaining provisions of the Agreement or the effectiveness of the Agreement in its entirety.

(3) An effective and practicable provision shall replace the ineffective or impracticable provision that comes as close as possible to the sense and purpose of the void provision.

(4) If this Agreement proves to include an omission provisions shall be deemed to be agreed that correspond to the sense and purpose of the Agreement and that in the event of consideration of which would have been agreed.

§ 20 Applicability

(1) This Agreement shall apply on its signature by the Contracting Parties.

(2) From 25 May 2018 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 27 April 2016 for the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) applies.

§ 21 Choice of law and court of jurisdiction

(1) Dutch law applies.

(2) The court of jurisdiction is the registered office of the Processor.

[Town/City], [DD.MM.YYYY]	Amsterdam, [DD.MM.YYYY]
[Full name AG]	Idiligo B.V.
_____	_____
[Client]	[Processor / Contractor]

Annexes:

Annex 1: Technical and organisational measures

Annex 2: Appointment of a Data Protection Officer, contact person and/or representation within the Union

Annex 3: Subcontractors utilised

Annex 4: Agreed places of performance as per section 7

Annex 1

Technical-organisational measures

1. Confidentiality (Art. 32 (1) a, b GDPR)

Entrance controls

Unauthorised entrance must be prevented, which is understood to mean in spatial terms.
Technical and organisational measures to control entrance, in particular also to legitimise those authorised:

- ☒ Setting authorised persons including the scope of the relevant authority.
- ☒ Careful selection of cleaning staff
- ☒ Issuing entrance entitlement identification
- ☒ Existence of regulations for externals (accompaniment of visitors by employees, separation of processing and public zones)
- ☒ Implementation of a key regulation
- ☒ Logging incoming and outgoing persons
- ☐ Physical measures exist and are regularly tested:
- ☒ Secured entrance (e.g. lockable doors, security locks)
- ☒ Securing doors (electrical door openers)
- ☒ Alarmed windows
- ☐ Equipment is secured against theft, manipulation or damage
- ☐ Monitoring facility (e.g. alarm system, video surveillance)
- ☐ Single-entrance facility (e.g. turnstile, double-door lock)
- ☐ Security staff, gatekeeper
- ☐ Division into different security zones

Other:

Physical access controls

The penetration of unauthorised persons in the DP systems and the unauthorised use of systems must be prevented.

Technical and organisational measures with regard to user identification and authentication:

- ☒ Conception and implementation of an authorisation concept
- ☒ Authorisation concept for terminals (computers)
- ☒ Authorisation concept for software/systems
- ☒ Identification and authorisation check of users
- ☒ Implementing a system to administer user identities
- ☐ Monitoring access attempts with reaction to security incidents
- ☒ Setting and checking access authorities
- ☐ Authentication procedure according to protection requirements for information (Classification)
- ☒ Encryption
- ☐ Blocking external interfaces (USB etc.)
- ☒ Appropriate password protection (rules of conduct, encrypted archives)
- ☒ Special security software (anti-malware, virus scanner, software and hardware firewall)
- ☐ Two-factor authentication
- ☐ Existence of rules for externals
- ☐ Access function via token

Other:

Access controls

Unauthorised activities in DP systems outside the authorisations granted must be prevented.

Needs-oriented configuration of the authorisation concept and access rights as well as their monitoring and logging on the basis of:

- ☒ Authorisation and roles concept for applications
- ☒ Implementation of rules for access and user authorisation
- ☒ Reviewing authorisations
- ☒ Function restriction (functional/time)
- ☒ Access restrictions (as per “need-to-know” and “least privilege”)
- ☒ Encrypted data storage
- ☒ Logging accesses made to applications, in particular when inputting, amending and erasing data
- ☒ Logging unauthorised access attempts
- ☐ Regular evaluation
- ☒ Ad-hoc evaluation
- ☒ Implementation of rules to erase data
- ☐ Implementation of rules to dispose of storage media (use of document shredders or service providers as per DIN 66933)
- ☐ Implementation of rules for handling electronic storage media
- ☒ Integrity checks

Other:

Separation controls

Data that was collected for different purposes has to be processed separately.

Measures for separate processing (storage, amendment, erasure, transmission) of data with different purposes:

- ☐ Multi-client capability:
- ☒ Physical separation
- ☒ Logical client separation (software)
- ☒ Separation of productive and test systems
- ☐ Sandboxing
- ☒ Setting database rights
- ☐ Documentation of functional separation
- ☒ Presence of directives and work instructions
- ☐ Presence of procedure documentation
- ☒ Regular reviews of intended use of information and IT systems

Other:

Pseudonymisation and encryption

Processing personal data in a manner in which the data can no longer be allocated to a specific data subject without drawing on additional information, if this additional information is separately stored and is subject to corresponding technical and organisational measures;

- [x] Trusted third party
- [ ] Blind signature
- [ ] Software-based encryption for data storage
- [ ] Hardware-based encryption for data storage

Other:

2. Integrity (Art. 32 (1) b GDPR)

Transfer controls

Aspects of the transfer and transmission of personal data must be regulated: Electronic transmission, data transport, communication controls. Measures in the event of the transport, transmission and communication or storage on data carriers (manual or electronic), as well as in the event of subsequent testing:

For electronic data carriers:

- [x] Encryption of data transmission (e.g. VPN, S/MIME)
- [ ] Electronic signature
- [x] Logging data transfer or transmission
- [x] Conducting ad-hoc plausibility, completeness and accuracy checks
- [ ] Measures to prevent uncontrolled flows of information (deactivating USB interfaces, regular checks of permissible recipients, technical restriction to permissible recipients)
- [ ] Documentation of the forms of data transfer (e.g. printout, data carrier, automated communication)
- [ ] Transferring data in anonymised or pseudonymised form
- [ ] Listing of recipients of data
- [ ] Documentation of interfaces and call-off and communication programs

For printouts and data carriers:

- [x] Conducting regular inventory controls
- [ ] Careful selection of transport staff and vehicles
- [ ] Ad-hoc securing of transport (e.g. receptacles, encrypting storage media, transfer logs)

Other:

Input controls

It must be guaranteed that data administration and maintenance is traceable or documented.

Measures for subsequent checks whether and by whom data was entered, changed or removed (erased) are:

- ☐ Logging entries and checking the logs
- ☒ Traceability of input, amendment and erasure of data by individual user names (not user groups)
- ☐ Storage of forms from which data has been transcribed by automated processing
- ☒ Issue of right to input, amend and erase data on the basis of an authorisation concept
- ☒ Organisationally set responsibilities for entry

Other:

3. Availability and resilience (Art. 32 (1) b, c GDPR)

Availability controls

Data must be protected against accidental destruction or loss.

Data backup measures (physical/logical):

- ☐ Regular checks of the system condition (monitoring)
- ☒ Quick recoverability of the normal system condition
- ☐ Backup and restart concept (regular data backups):
- ☐ Offline ☒ Online ☒ Onsite ☐ Offsite ☐
- ☒ Data archiving concept
- ☒ Presence of an emergency concept (business continuity, disaster recovery)
- ☐ Regular tests of the emergency concept
- ☒ Presence of redundant IT systems (e.g. servers, memory)
- ☐ Replicability of virtual machines
- ☒ Functional physical protection equipment (fire protection, energy: uninterruptible power supply, air conditioning)
- ☐ Reporting paths and emergency plans

Other:

Resilience checks

Data processing should be tolerant of disruptions and faults.

- ☒ Virus protection/Anti-malware/Anti-ransomware
- ☒ Generously available network capacity
- ☒ Hardware hardened in particular against DoS and DDoS attacks
- ☐ IDS/IPS
- ☒ Suitable system architecture/DMZ
- ☒ Firewall

4. Procedure for regular review, assessment and evaluation (Art. 32 (1) d GDPR; Art. 25 (1) GDPR)

- [x] Fixed written regulations of responsibilities for data protection
- [x] Fixed written regulations of responsibilities for information security
- [ ] Existence of appropriate information security management system
- [ ] Existence of appropriate incident response management system
- [x] Conduct of an information classification
- [x] Regular training and sensitisation of employees and managers
- [x] Data protection-friendly pre-settings (Art. 25 (2) GDPR);
- [ ] Order checks in order to guarantee data processing as per instructions:
  - [ ] Strict compliance with the agreements made and testing in this respect
  - [x] Concept of how regular checks of the order process are made (e.g. submission of self-assessments, submission of agreements with subcontractors, contractor carries out checks at subcontractors)
  - [ ] No data processing in accordance with Art. 28 GDPR without corresponding instructions from the Client, e.g. on the basis of a clear contract design, formalised order management, strict selection of service providers, vetting duty, follow-up checks.

Other:

Annex 2

Appointment of a Data Protection Officer, contact person and/or representation within the Union as per section 16 Processing Agreement

The Processor appoints:

As Data Protection Officer Dr Timo Hoffmann

Address: Eckweg 1, 78048 Villingen-Schwenningen

Email: timo.hoffmann@hub24.de

Contact: Mr Frank Korthouwer

Address: Kabelweg 57, 1014 BA Amsterdam

Tel.: +31 23 3000000

Email: frank.korthouwer@idiligo.com

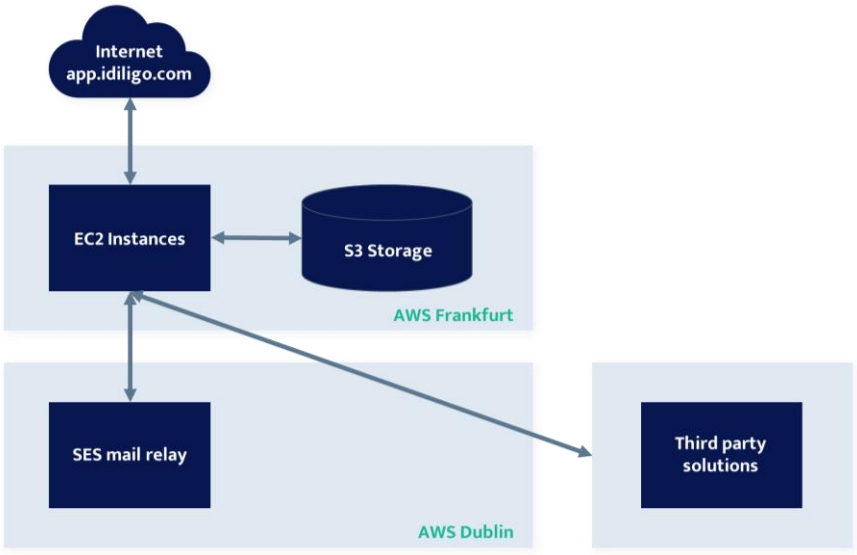
Annex 3

Subcontracting at the Data Processor at the time of the order placement

Name of subcontractor	Description of the sub-performances	Place of performance provision
Amazon (AWS)	Storage of data in Amazon S3 memory. Both EC2 and S3	Frankfurt, Germany
Amazon (AWS)	SES Mail Relay Function	Dublin, Ireland
Digital Intelligence	Development of Idiligo Application	Amsterdam, Netherlands
The Rocket Science Group LLC d/b/a Mailchimp	Customer information by email	Third countries, EU
Exact	Invoice dispatch	EU
Intelligent Solution Services AG	Digital signature	Stuttgart, Germany

Security Management & Architecture

- The Elastic Compute Cloud (EC2) from Amazon offers a function called security groups, which is similar to an incoming network firewall, in which Idiligo gives the logs, ports and source IP areas that can be reached for EC2 instances.
  Memory & Backups
- Documents that were uploaded or generated during interactive Idiligo meetings are stored in S3. The data is stored encrypted with AWS Key Management Service (KMS).
  Idiligo implements a daily backup of customer-specific information with a maximum history of 8 days in a separate Amazon S3 environment.



Annex 4

Agreed places of performance as per section 7 of the Agreement

Name and address of the **Processor**	Name and address of the **subcontractor**	Place of performance provision
Idiligo B.V. Kabelweg 57, 1014 BA Amsterdam, Netherlands	Amazon (AWS) Frankfurt	Germany