General Terms and Conditions of Asendia – Appendix 1
Data Protection Agreement

Preamble

This Appendix 1 (Data Protection Agreement) to the GTC (hereinafter referred to as the "**Data Protection Agreement**") specifies the data protection obligations of the contractual parties which derive from this Data Protection Agreement and the Order Processing described in Attachment A (Job Details) to this Data Protection Agreement. It applies to all activities related to the provision of the Services, during which employees of the Asendia Company or third parties employed by the Asendia Company may come into contact with the Personal Data of the Customer and/or Customer's clients.

1. Definitions

In this Data Protection Agreement, the terms listed below are used with the following meanings. The other terms are described in the GTC.

Term	Meaning
Contract	Contract means the contract for the provision of the Services concluded between the Customer and the Asendia Company based on the Asendia Company's GTC.
Controller	Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Subject	Data subject means the identified or identifiable natural person, the Personal Data relates to.
GDPR	Regulation means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
GTC	GTC means the General Terms and Conditions of the Asendia Company.
Instruction	Instruction means the Customer's requirement for the Asendia Company specifying the handling of Personal Data in terms of data protection (e.g. storage, pseudonymization, deletion, return).
Order	Order means the Services the Customer requests to be performed by the Asendia Company on basis of the GTC.
Order Processing	Order Processing means the processing activities described in Attachment A (Job Details) section 2.
Personal data	Personal data means all information relating to an identified or identifiable natural person; a natural person is deemed identifiable if he or she can be identified, directly or indirectly, in particular by reference to an identification such as a name, to an identification number, location data, an online identification, or to one or more factors specific to this natural person's physical, physiological, genetic, mental, economic, cultural or social identity.
Processor	Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

2. Scope and accountability

2.1. The Asendia Company shall perform the Contract. In this connection the Asendia Company will have access to Personal Data and/or may gain knowledge of said data. The conclusion of this Data Protection Agreement is therefore required pursuant to Art. 28 GDPR.

2.2. The Customer has selected the Asendia Company as a service provider as part of its duty of care pursuant to Art. 28 GDPR. A precondition for the reliability of the data processing as part of the Order is that the Customer issues the Order to the Asendia Company in writing or electronically. This Data Protection Agreement contains the Order for contract processing according to the will of the parties and in particular of the Customer within the meaning of Art 28(3) GDPR and regulates the data protection rights and duties of the parties with regard to the performance of the Services.

2.3. The Customer is the exclusive owner of the Personal Data as the Controller within the meaning of the GDPR. On the basis of this accountability, the Customer may request the correction, deletion, blocking and return of Personal Data during the term of the Data Protection Agreement and after termination of the Data Protection Agreement.

3. Object and term of the Order

3.1 The subject matter of the Order is specified in Attachment A (Job Details).

3.2 This Data Protection Agreement shall come into effect upon the Customer entering into the Contract and will end upon fulfilment of the respective Services and expiration of the applicable retention period set forth in Attachment A (Job Details) for the respective Personal Data processed to provide the Services. The right of termination of this Data Protection Agreement for good cause remains unaffected.

3.3 In case of doubt, the provisions of this Data Protection Agreement shall prevail over provisions of the Contract.

4. Description of the processing, data and Data Subjects

The scope and purpose of the data processing by the Asendia Company result from the Contract. The type of the processing as well as the type of data and group of Data Subjects are described in Attachment A (Job Details).

5. Technical and organizational measures

5.1. The Asendia Company undertakes vis-a-vis the Customer to comply with technical and organisational measures that are reasonable and necessary in order to ensure compliance with the applicable data protection regulations.

5.2. The Asendia Company must document all technical and organisational measures taken within the meaning of Art. 28(3) letter c GDPR, Art. 32 GDPR in conjunction with Art. 5(1) and (2) GDPR and provide these to the Customer for auditing purposes on the Customer's request in writing.

5.3. The measures serve to ensure data security and a risk-appropriate level of protection in terms of confidentiality, integrity, availability and reliability of the systems related to this Order. In this respect, the state of the art, implementation costs and the type, scope and purposes of the processing as well as the various probabilities of occurrence and degree of risk regarding the rights and freedom of natural persons within the meaning of Art. 32(1) GDPR must be taken into account.

5.4. The level of the technical and organisational measures existing at the time the Contract is concluded is attached to this Data Protection Agreement as Attachment B (Technical and Organisational Data Protection Measures). The parties agree that changes to the technical and organisational measures may become necessary in Order to adapt them to technical and legal circumstances. The Customer may at any time request a current version of the technical and organisational measures implemented by the Asendia Company.

6. Rectification, restriction and deletion of data

6.1. The Asendia Company must not independently rectify, delete or restrict the processing of the Personal Data that it processes on behalf of the Customer and may only do so according to the Customer's documented Instructions. If a Data Subject contacts the Asendia Company directly in this respect, the Asendia Company will forward the request to the Customer for release without undue delay.

6.2. The rights to deletion, restriction, rectification, data portability and right to information are to be implemented by the Asendia Company as soon as possible, but only according to the Customer's documented Instructions.

6.3. Copies or duplicates of data shall not to be created without the knowledge of the Customer. This excludes copies or duplicates required to perform the Contract, backup copies to the extent that these are required in order to guarantee proper data processing, as well as data that is necessary with respect to the compliance with legal retention obligations.

6.4. After the end of the Contract or earlier upon request by the Customer – but no later than at the termination of Data Protection Agreement – the Asendia Company shall destroy all of Customer's Personal Data required for the provision of the Services in the Asendia Company's possession in compliance with data protection regulations. The same applies to test and scrap material. The deletion report must be presented upon request.

6.5. Documentation which serves as proof of proper data processing in accordance with the Order must be retained by the Asendia Company after the end of the Contract and/or Data Protection Agreement in accordance with the respectively applicable retention periods. The Asendia Company can return them to the Customer at the end of the Data Protection Agreement to be relieved of its obligations.

7. Duties of the Asendia Company

7.1. The Asendia Company is not permitted to process any of the Customer's Personal Data which is not related to the performance of the Services unless the Customer has provided authorisation in writing to this effect.

7.2. The Asendia Company confirms that it has appointed a company data protection officer within the meaning of Art. 38, 39 GDPR. If the data protection officer is replaced Asendia will publicize this in an appropriate form without delay.

7.3. The Customer is responsible for the assessment of the admissibility of the data processing.

7.4. The Asendia Company shall notify the Customer without delay if it believes that any Instruction issued by the Customer is illegal. The Asendia Company has the right to suspend implementation of the respective Instruction until it has been confirmed or modified by the Customer.

7.5. The Asendia Company shall inform the Customer immediately in the event of significant disruptions to the operating processes, if data protection is suspected of being compromised, or if other irregularities exist with respect to the processing of the Customer's data.

7.6. If the Asendia Company determines or if certain facts justify the assumption that Personal Data processed by the Asendia Company for the Customer are subject to a violation of the legal protection of Personal Data pursuant to Art. 33 GDPR (data protection violation and/or a data breach) e.g., where these have been illegally transferred or if third parties have illegally gained knowledge of said data in any other way, the Asendia Company shall notify the Customer without delay of the time, type and scope of the violation(s) or breach(es) in writing or in text form (fax/email). The notification sent to the Customer must contain at least the following information:

7.6.1. A description of the type of breach of Personal Data protection, if possible specifying the categories and approximate number of Data Subjects, categories affected and approximate number of Personal Data records affected.

7.6.2. The names and contact information of the data protection officer or another contact for additional information.

7.6.3. A description of the likely consequences of the breach of Personal Data protection.

7.6.4. A description of the measures taken or proposed to remedy the data protection breach and, if required, measures to minimize the potential detrimental effects.

Moreover, the Asendia Company is obliged to immediately notify the Customer of any measures taken by the Asendia Company to prevent the illegal transmission and/or unauthorised access by third parties.

7.7. The Asendia Company shall provide to the Customer upon request the information required for the processing activities register pursuant to Art. 30(1) GDPR and as Order Processor also maintains a register of processing activities pursuant to Art. 30(2) GDPR.

7.8. The Asendia Company shall ensure that the Asendia Company's employees and third parties responsible for processing the Customer's Personal Data have signed a non-disclosure agreement and are familiar with the data protection provisions relevant for them before processing said data pursuant to Articles 28(3) sentence 2 letter b, 29, 32(4) GDPR. The Asendia Company and all persons reporting to the Asendia Company with access to Personal Data must process the data exclusively in accordance with the Customer's Instructions, including the authorisations granted in this Data Protection Agreement, unless they are legally obliged to process said data. This obligation to maintain confidentiality extends beyond the end of the processing activities.

7.9. The fulfilment of the aforementioned duties must be inspected by the Asendia Company or third parties obligated by the Asendia Company to perform such inspection and documented in a suitable manner.

7.10. Furthermore, the Asendia Company undertakes to support the Customer pursuant to Art. 28(3) letter f GDPR to ensure compliance with the obligations stipulated in Articles 34 - 36 GDPR:

7.10.1 To provide all relevant information in this connection without delay as part of its duty of disclosure with regard to the Data Subjects and the Customer.

7.10.2 In the performance of the data protection impact assessment.

7.10.3 During a previous consultation with the supervisory authority.

7.11. Upon request, the Customer and the Asendia Company will cooperate with the supervisory authority regarding the fulfilment of their responsibilities.

7.12. If the Customer is also subject to an inspection by the supervisory authority, involved in infringement or criminal proceedings, affected by a liability claim of a Data Subject or a third party or by another claim in connection with the Asendia Company's Order processing, the Asendia Company shall support the Customer to the best of its abilities.

7.13. The Asendia Company will regularly inspect its internal processes as well as technical and organisational measures in order to ensure that the data processing within its sphere of responsibility is carried out in compliance with applicable data protection laws and that the rights of the Data Subject are protected.

8. Rights and duties of the Customer

8.1. The Customer's instructions are initially determined by this Data Protection Agreement and can then be changed, supplemented or replaced by the Customer in writing or in text form by individual instructions. The Customer shall issue Instructions in writing or in text form.

8.2. All issued Instructions are to be documented by both the Customer and the Asendia Company.

8.3. The Customer shall notify the Asendia Company in full and without delay if it detects errors or irregularities concerning data protection provisions during the inspection of Order results.

8.4. The Customer is obliged to comply with the reporting obligation stipulated in Art. 33(1) GDPR.
8.5. If the Customer issues individual Instructions that go beyond the scope agreed in this Data Protection Agreement or the Contract, the costs in connection with the fulfilment of these Instructions shall be borne by the Customer.

9. Guaranteeing the rights of the Data Subject

9.1. The Customer is responsible for protecting the rights of the Data Subject.
9.2. If the Asendia Company is required to cooperate in protecting the rights of the Data Subject, particularly regarding the right to access, rectification, restriction, data portability or deletion carried out by the Customer, the Asendia Company shall take the required measures in each case as instructed by the Customer.
9.3. If a Data Subject contacts the Asendia Company directly to request rectification, deletion or restriction or portability of its data, the Asendia Company shall forward this request to the Customer without delay.
9.4. This shall not affect any agreements concerning possible compensation for additional costs incurred by the Asendia Company through provision of cooperation services in connection with the assertion of the rights of Data Subjects vis-a-vis the Customer.

10. Monitoring rights

10.1. The Customer has the right to monitor compliance with legal data protection regulations and the technical and organizational measures of the Asendia Company as well as compliance with the Customer's Instructions by the Asendia Company in the respectively required scope once annually.
10.2. Customer may carry out such monitoring either directly or through a neutral third party, provided however, that any such third party is on competitor.
10.3. Customer shall give the Asendia Company one-month prior notice of the monitoring in writing, providing further details regarding the party performing the audit. The Asendia Company may refuse for legitimate reasons the party designated to carry out the monitoring. In case of such refusal, the parties shall mutually agree on the designation of the monitor.
10.4. The audit may be carried out during the regular opening hours of the respective Asendia Company, only to the extent necessary and without disproportionately disturbing the operations of the Asendia Company.
10.5. The Customer shall document the result of the monitoring and inform the Asendia Company thereof without undue delay. If any circumstances are identified during the inspection, which are to be avoided in the future and which require changes to the Asendia Company's processes regarding data protection, the Customer shall notify the Asendia Company of any such changes without undue delay.
10.6. The Asendia Company shall provide any requested information to the Customer insofar as this is necessary to carry out the monitoring within the meaning of paragraph 1.
10.7. The Asendia Company shall provide the required information to the Customer in the event of measures taken by the supervisory authority with regard to the Customer within the meaning of Art. 58 GDPR in particular with regard to the obligations to provide information and carry out inspections.
10.8. The Asendia Company will provide evidence for technical and organisational measures that refer not only to the Order as set forth in Attachment A (Job Details) to this Data Protection Agreement. This may be carried out by:
  10.8.1. Compliance with authorised rules of conduct pursuant to Art. 40 GDPR;
  10.8.2. Certification in accordance with an authorised certification process pursuant to Art. 42 GDPR;
  10.8.3. Up-to-date test certifications, reports or extracts from reports by independent bodies (e.g. auditors, internal audit department, data protection officer, IT security officer, data protection auditors);
  10.8.4. A suitable certification by the IT security and data protection audit (e.g. according to ISO 27001 or BSI basic protection).
10.9. The costs of carrying out an inspection of the Asendia Company's may be charged to the Customer.

11. Sub-Contracting relationships

11.1. The Customer agrees that the Asendia Company may commission or sub-contract external companies for the performance of the Contract. A list of the currently authorised sub-processors will be provided as Attachment A (section 3) to this Data Protection Agreement.
11.2. Asendia Company must either directly or by appropriate contractual provisions ensure that the sub-processor is carefully selected. The Asendia Company shall check or obligate a third party by appropriate contractual provisions to check before commissioning that the sub-processor in question is capable of fulfilling the provisions of the Data Protection Agreement between the Customer and the Asendia Company. In particular, prior to the start of any sub-commissioning and also regularly during the term of the Contract and/or this Data Protection Agreement, the Asendia Company must check or obligate a third party by appropriate contractual

provisions to check, that the sub-Contractor has taken the required technical and organisational measures pursuant to Art. 28(3) letter c, Art. 32 GDPR in conjunction with Art. 5(1) and (2) GDPR for the protection of Personal Data. The Asendia Company must document the monitoring results and provide these to the Customer upon request. The Asendia Company is obliged to obtain confirmation from the sub-processor that it has appointed an internal data protection officer within the meaning of 37-39 GDPR.

11.3. The Asendia Company must ensure that the provisions regulated in this Data Protection Agreement and potential additional Instructions by the Customer also apply to sub-processors. The Asendia Company shall regularly check or obligate a third party by appropriate contractual provisions to check compliance with these obligations.

11.4. The sub-processor must sign an undertaking to this effect. The Asendia Company must provide to the Customer a copy of this written undertaking upon request.

11.5. The Asendia Company shall specifically ensure through contractual provisions that the monitoring powers of the Customer and the supervisory authorities also apply to the sub-processor and that the respective rights of the Customer and the supervisory authorities to carry out monitoring inspections are agreed. Moreover, it must be contractually agreed that the sub-processor is obliged to accept these monitoring measures and any on-site inspections.

11.6. In the event that the Asendia Company performs all or part of the processing of Personal Data outside the territory of a member country of the European Union, the European Economic Area (EEA) or a country recognized as adequate by the European Union - including accommodation - it undertakes to regulate the transfer of Personal Data by appropriate safeguards, including standard clauses adopted by the European Commission.

12. Data secrecy and obligations to maintain confidentiality

12.1. The Asendia Company undertakes to comply with the same confidentiality laws that apply to the Customer. The Customer is obliged to inform the Asendia Company of any special confidentiality laws.

12.2. Upon the Customer's request in writing or in text form, the Asendia Company shall provide an assurance that it is aware of the currently applicable data protection regulations and that it is familiar with their application.

12.3. Both parties undertake to treat all information confidentially that they receive in connection with the performance of this Data Protection Agreement for an unlimited time and to only use them for the performance of the Services. The parties are not permitted to use this information in part or in full for any other than the aforementioned purposes or to make the information available to third parties, exclusive of any affiliates of the Customer or the Asendia Company to the extent necessary for the performance of the Contract.

12.4. The above mentioned obligation does not extend to information that one of the parties has demonstrably received from third parties without being subject to a non-disclosure agreement in this respect or that is already in the public domain.

13 Customer's obligations

12.5. The Customer warrants that he has complied with all the applicable laws and regulations relating to the protection of privacy and that said laws and regulations permit the provision of this Personal Data to the Asendia Company and the processing of this Personal Data by the Asendia Company for the performance of the Services. The Customer warrants that all appropriate consents have been obtained from persons whose data is to be processed by the Asendia Company. The Customer commits himself to indemnify and hold the Asendia Company harmless from any claims made against the latter by Third Parties that arise from the non-compliance with these laws and regulations.

12.6. The Customer gives its explicit consent to the Asendia Company to process, store and use within Asendia Group the disclosed Personal Data in order to fulfill its contractual and legal obligations, to ensure a high quality of service and to maintain the customer relationship. The Customer undertakes to enter into more specific data protection agreements with the respective Asendia Company with undue delay upon the Asendia Company's request to this regard in writing or text form.

14 Duties of disclosure, written form requirement, choice of law

13.1. The Asendia Company must notify the Customer without delay if the safety of the Customer's Personal Data is threatened by a levy of execution, confiscation or insolvency or settlement proceedings or other events or measures enacted by third parties. The Asendia Company will notify all responsible parties in this respect without delay that the Customer is the exclusive owner of the Personal Data as the Controller within the meaning of the GDPR.

13.2. Any modifications and amendments of this Data Protection Agreement and of all of its constituent parts - including any assurances by the Asendia Company - require a written agreement and an explicit note stating

that these are modifications and/or amendment of these terms. This also applies to the waiver of this written form requirement.

13.3. If any provision in this Data Protection Agreement is invalid, the remaining provisions shall remain unaffected thereby. The contractual parties shall undertake in good faith to replace the invalid provision or any unintended missing provision in the Data Protection Agreement with a provision coming as close as possible to the mutually intended purpose of both Contractual parties.

© Asendia, July 2021

© Asendia Nordic AB, Registered at the Chamber of Commerce of Stockholm under number 556670-2253, Share capital of SEK 104'512; Registered address and main place of business: Kanalvägen 10C, 194 61 Upplands Väsby, Sweden.

Attachment A: Job details

1. Subject of the Controller
The Order placed by the Customer comprises the Services performed on basis of the Contract.

2. Scope, nature and purpose of processing
The scope of processing and thus the quantity of Personal Data used is variable and is based on the Services requested by the Customer.

3. Type of data and Subcontractors
The type of Personal Data processed depends on the Services which are subject to the Contract.

Asendia Offers	Personal Data Processed	Retention period	Person having access to the Personal Data
Business Mail	Name, Surname, Title, Address	Distribution duration	Asendia Company and/or Subcontractors handling distribution process (Postal Operators, Carriers, Partners)
Customs Clearance	Name, Surname, Title, Address, Customs information	Duration required by law (3 years)	Subcontractors in charge of the Service (Local Partners)
Direct Mail	Name, Surname, Title, Address	Distribution duration	Asendia Company and/or Subcontractors handling distribution process (Postal Operators, Carriers, Partners)
Goods	Name, Surname, Title, Address, Telephone, email, Customs information	Distribution duration	Asendia Company and/or Subcontractors handling distribution process. (Postal Operators, Carriers, Partners)
Press	Name, Surname, Title, Address	Distribution duration	Asendia Company and/or Subcontractors handling distribution process. (Postal Operators, Carriers, Partners)
Registered items	Name, Surname, Title, Address, tracked number	Duration of the Service + 6 months after sale management	Asendia Company and/or Subcontractors handling distribution process. (Postal Operators, Carriers, Partners)
Response mail	Name, Surname, Title, Address	Duration of the Service	Asendia Company and/or Subcontractors handling distribution process. (Postal Operators, Carriers, Partners)
Returns	Name, Surname, Title, Address, Customs information on goods carried	Duration of the Service + 6 months for after sale management	Asendia Company and/or Subcontractors handling distribution process. (Postal Operators, Carriers, Partners)
Tracked items	Name, Surname, Title, Address, tracked number	Duration of the Service + 6 months for after sale management	Asendia Company and/or Subcontractors handling distribution process. (Postal Operators, Carriers, Partners)
Undeliverable items management	Name, Surname, Title, Address	Duration of the Service	Asendia Company and/or Subcontractors handling distribution process. (Postal Operators, Carriers, Partners)

4. Data subject categories
Customer's clients.

© Asendia, July 2021

© Asendia Nordic AB, Registered at the Chamber of Commerce of Stockholm under number 556670-2253, Share capital of SEK 104'512; Registered address and main place of business: Kanalvägen 10C, 194 61 Upplands Väsby, Sweden.

Attachment B: Technical and organisational data protection measures

1. Confidentiality

1.1 Physical Access Control

Unauthorised persons must be prevented from obtaining physical access to the technical facilities used by the Asendia Company for the provision of the hosting service.

Measures implemented on the Asendia Company's side:

- Locking system for offices and server room
- Key administration / documentation of keys issued
- Careful selection of cleaning staff
- Compulsory regulations for dealing with visitors

1.2 Access Control

Measures must be put in place to prevent unauthorised persons from using the facilities (hardware, operating systems and software) required to provide the specified IT service.

Measures implemented on the Asendia Company's side:

- Personal and individual user log-in for logging onto the system and/or company network
- Password procedure (specifying password parameters relating to complexity and update frequency)
- Blocking clients after particular period of time has elapsed with no user activity (including password-protected screensavers or automatic pausing)

1.3 Data Access Control

Measures must be put in place to ensure that the persons authorised to use a data processing system only have access to the data covered by their access authorisation, and that Personal Data cannot be read, copied or altered in an unauthorised manner during processing, utilisation and after storage.

Measures implemented on the Asendia Company's side:

- Administration of access authorizations by system administrators
- Highest possible level of automation when setting up systems and authorizations to prevent errors
- Differentiated access authorizations
- Profile and role concept

1.4 Transfer Control

Measures must be put in place to ensure that Personal Data cannot be read, copied, altered or removed in an unauthorised manner during electronic transmission or during transport or while being loaded onto data carriers, and that it is possible to check and ascertain where the transmission of Personal Data by data transmission systems should take place in the normal course of operation.

Measures implemented on the Asendia Company's side:

- Tunnelled remote data connections (VPN=Virtual Private Network)
- Secure data transmission over the internet through SSL encryption (https)

1.5 Separation Control

Measures must be put in place to ensure that data collected for different purposes can be processed separately.

Measures implemented on the Asendia Company's side:

- Separate systems (logical client separation)
- Access authorizations
- Separation of production and testing systems

1.6 Encryption

The processing of Personal Data should be performed in a manner that prevents its unintended or unlawful or unauthorised disclosure. This is to be ensured by state-of-the-art encryption mechanisms that are deemed to be reliable.

Measures implemented on the Asendia Company's side:

- Encrypted data transmission (VPN, SSL / TLS encrypted internet connections)

2. Integrity

2.1 Data Input Control

It must be possible to retrospectively check and ascertain whether and by whom Personal Data has been entered into data processing systems, altered or removed.

Measures implemented on the Asendia Company's side:

- Access rights
- System-based logging (access logs in the individual applications)

2.2 Transfer Control

The measures for transfer control pursuant to 1.4 are also intended to ensure data integrity.

3. Availability and reliability

Care must be taken to ensure that Personal Data is protected against accidental destruction or loss.
Measures implemented on the Asendia Company's side:

- Continuous server monitoring using monitoring software
- Backup and data backup procedures
- Anti-virus protection / Firewall

4. Other Areas Subject to Control

There must be a system in place for the regular checking, assessment and evaluation of the data protection and the effectiveness of the implemented technical and organisational measures.
Measures implemented on the Asendia Company's side:

- Information security management (based on ISO 27001)
- Incident Response System to verify security breaches and problems
- Conducting regular audits

© Asendia, July 2021

© Asendia Nordic AB, Registered at the Chamber of Commerce of Stockholm under number 556670-2253, Share capital of SEK 104'512; Registered address and main place of business: Kanalvägen 10C, 194 61 Upplands Väsby, Sweden.