DATA PROCESSING AGREEMENT

Standard Contractual Clauses

Pursuant to Article 28(3) of Regulation 2016/679 (the General Data Protection Regulation – "GDPR") for the purpose of the data processor's processing of personal data.

Between

Name
Cvr no
Address
ZIP code and city
Country

(hereinafter 'the data controller')

and

Name
CVR No:
Address
ZIP code and city
Country

(hereinafter 'the data processor')

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

2.1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor when processing personal data on behalf of the data controller.

2.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

2.3. In the context of the provision of the services to which the data controller subscribes, as described in the applicable commercial agreement, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

2.8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

2.9. Appendix D contains provisions for other activities which are not covered by the Clauses.

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

2.11. These Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

3.1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 of the GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

3.2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3. The data controller shall be responsible, among others, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

4.1. The data processor shall process personal data only on documented instructions from the data controller unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

5.2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1. Article 32 of the GDPR stipulates that taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. pseudonymisation and encryption of personal data;
b. the ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2. According to Article 32 of the GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

6.3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 of the GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 of the GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 of the GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 of the GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1. The data processor shall meet the requirements specified in Article 28(2) and (4) of the GDPR in order to engage another processor (a sub-processor).

7.2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

7.3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 6 weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

7.5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business-related issues that do not affect the legal

data protection content of the sub-processor agreement shall not require submission to the data controller.

If the sub-processor does not fulfil its data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular, those foreseen in Articles 79 and 82 of the GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V of the GDPR.

8.2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3. Without documented instructions from the data controller, the data processor, therefore, cannot within the framework of the Clauses:

8.3.1. transfer personal data to a data controller or a data processor in a third country or in an international organisation

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

8.3.3. have the personal data processed in by the data processor in a third country

8.4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V of the GDPR on which they are based, shall be set out in Appendix C.6.

8.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) of the GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V of the GDPR.

9. Assistance to the data controller

9.1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

9.2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.4., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

9.2.1. the data controller's obligation to without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority in the country where the controller is based unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

9.2.2. the data controller's obligation to without undue delay communicate the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

9.2.3. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

9.2.4. the data controller's obligation to consult the competent supervisory authority in the country where the controller is based, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

9.3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

10.1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

10.2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the GDPR.

10.3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

10.3.1. 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;

10.3.2. the likely consequences of the personal data breach;

10.3.3. 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.

10.4. The parties shall define in Appendix D all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

11.1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so cf. Appendix A. unless Union or Member State law requires the storage of personal data.

12. Audit and inspection

12.1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

12.2. Procedures applicable to the data controller's audits, including inspections of the data processor and sub-processors, are specified in appendices C.7. and C.8.

12.3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

13.1. The parties may agree on other clauses concerning the provision of the personal data processing service specifying, e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

14.1. The Clauses shall become effective on the date of both parties' signature.

14.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendices A.5 and C.4., the Clauses may be terminated by written notice by either party.

15. Data controller and data processor contacts:

15.1. The parties may contact each other using the following contacts/contact points:

With the data controller:

Name

Position

Telephone

Email

With the data processor:

Name

Position

Telephone

Email

15.2. The parties shall be under obligation continuously to inform each other of changes to contracts/contact points

16. Signatures

On behalf of the data controller

Name

Position

Telephone

Email

Signature

On behalf of the data processor

Name

Position

Telephone

Email

Signature

17. Appendix A - Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

Delivering digital performance marketing and related advisory services via Ai Marketing Hub and Ai - based Optimisation services. This includes:

a. Managing and optimising websites and digital platforms
b. Monitoring and analysing website traffic and user behaviour
c. Search engine optimisation (SEO) and performance analysis
d. Managing marketing campaigns across digital channels
e. Lead generation and customer relationship management
f. Email marketing, newsletter distribution, and marketing automation
g. Social media management and online advertising
h. eCommerce analytics
i. Workflow automation
j. Use of AI-based tools to generate, analyse, or process content and communications

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

a. AI Marketing Hub (SaaS Platform)

Processing carried out through an AI-enabled SaaS-based marketing and analytics platform made available to the data controller and its authorised users via individual user IDs and login credentials.

The platform supports AI-assisted marketing analytics, optimisation, and automation. Processing includes the hosting and provision of the platform; user account administration; configuration and operation of marketing, analytics, tracking, targeting, and AI-powered optimisation functionalities; collection, structuring, and analysis of user interaction, behavioural, transactional, and performance data; and the generation of AI-assisted insights, predictions, recommendations, and performance reports.

The platform incorporates artificial intelligence and machine learning technologies to perform automated data analysis and modelling, including behavioural analysis, segmentation, profiling, predictive analytics, and the generation of marketing recommendations, optimisation suggestions, and content variations. AI functionalities may also support automated campaign optimisation, targeting improvements, performance forecasting, and the orchestration of marketing activities.

Processing further includes the operation, monitoring, testing, validation, and refinement of AI-enabled functionalities, as well as ongoing technical maintenance, support, optimisation, and security of the platform.
All processing, including AI-based processing, is carried out solely on behalf of and in accordance with the documented instructions of the data controller.

b. AI-Based Optimisation Services

Processing carried out in connection with the design, configuration, implementation, and operation of AI-driven and automated optimisation solutions aimed at improving lead generation, SEO performance, digital marketing effectiveness, and customer support flows.

Such processing involves the application of artificial intelligence, machine learning models, predictive analytics, and automated decision-support tools to analyse data and generate optimisation insights.

This includes:
• analysis of website, behavioural, transactional, and performance data using AI-assisted analytical models;
• AI-driven profiling, segmentation, and audience modelling for marketing optimisation;
• predictive modelling and optimisation of content, conversion paths, and customer journeys;
• automation of marketing communications and customer support interactions using AI-enabled workflows;
• integration with relevant systems (e.g., CRM, marketing automation, analytics, and e-commerce tools); and
• testing, training, validation, calibration, and refinement of AI models and automated workflows within the scope of the agreed services.

AI systems generate automated insights, predictions, recommendations, or suggested actions to support the data controller’s marketing and operational decision-making.

c. AI Processing Safeguards

Where the Services involve the use of artificial intelligence or machine learning systems, such processing shall be carried out solely for the purpose of providing and improving the Services to the data controller.

The data processor shall not:

• use personal data processed under this Agreement to train general-purpose or cross-customer AI models, or
• use such personal data for the data processor's own independent purposes,
unless expressly authorised in writing by the Data Controller.

Personal data processed within AI functionalities shall not be used to improve services for other customers unless the data has been irreversibly anonymised and aggregated, such that it can no longer be linked to an identified or identifiable individual.

AI-generated outputs are intended to support and augment decision-making by the data controller and its authorised users.

See also A.5.

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

CATEGORIES OF DATA SUBJECTS	PERSONAL DATA
Persons who visit the data controller's e-commerce platform: Customers and potential customers with an interest in the data controller's products and services.	Name Email addresses, Phone number, Address Purchase and order data (order history, purchased products, order value and frequency, fulfilment status – not payment card or account credentials) Company name Job title Marketing preferences Consent records Engagement and campaign interaction data Subscription preferences Profile identifiers Advertising and tracking identifiers
Where applicable: data subjects whose purchase, behavioural, or interaction data may reveal special categories of personal data (Article 9 GDPR)	Data from which special categories of personal data within the meaning of Article 9 GDPR may be inferred – including potentially health-related data – where applicable to the data controller's specific product range, service context, or customer base. Whether this category applies to a specific customer is specified in Appendix B.

A.4. Processing includes the following categories of data subject:

See the overview in section A.3.
Note: Only the categories of personal data that the data controller actually shares with the data processor are in scope for the specific customer relationship governed by this Agreement. The enumeration of categories in Section A.3 reflects the full range of data types that may be processed across all customer configurations. Each data controller is solely responsible for ensuring that only data categories relevant to its specific use of the Services are shared with the data processor. Where the data controller's product range, service context, or customer base is such that purchase, order, behavioural, segmentation, or interaction data may allow inference of special categories of personal data within the meaning of Article 9 GDPR (including but not limited to health-related data), this shall be specified by the data controller in Appendix B. Processing of data from which special categories may be inferred shall be subject to the elevated protection measures set out in Section C.2.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The data controller determines the duration of the processing of the personal data.

The Data Processor's processing of personal data on behalf of the Data Controller continues as long as the Data Controller makes use of the Services provided by the Data Processor to which the Data Controller subscribes, as described or referenced in the applicable commercial agreement,

If the data controller's deletion policies dictate that personal data must be deleted during the agreement period, the data processor complies with this request, including by setting the underlying systems to delete personal data automatically.

See also C.4

18. Appendix B - Sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors. The list is specific to the data controller's service configuration and forms an integral part of this Data Processing Agreement. The data processor shall notify the data controller in writing of any intended addition or replacement of sub-processors at least 6 weeks in advance, in accordance with Clause 7.3.

Sub-processor table example (See Appendix B below as attachment):

Sub-processor	Purpose	Data categories processed	Special categories may be inferred (Art. 9 GDPR)	Location	Transfer basis	DPF verified (date)	Active for this customer

The data processor shall update this annex and provide written notice to the data controller before any sub-processor is added, replaced, or deactivated for this customer's service configuration.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

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

See Clause 7.3.

19. Appendix C - Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Provision of the Services
Processing personal data as necessary to deliver the services described in Sections A.1 and A.2, within the categories of personal data and data subjects set out in Section A.3. This includes operation of the AI Marketing Hub (SaaS platform) and the AI-based optimisation services relating to lead generation, SEO, digital marketing, and customer support flows.

Operation and Technical Management
Hosting, storing, organising, analysing, retrieving, and otherwise processing personal data within the SaaS and supporting systems; administering user accounts and login-based access; configuring integrations with advertising, analytics, e-commerce, CRM, and marketing systems; and ensuring ongoing technical maintenance, support, validation, optimisation, and security of the Services.

AI and Optimisation Activities
Implementing, configuring, testing, training, refining, and optimising AI-driven models, automation workflows, targeting mechanisms, segmentation, tracking technologies, reporting tools, and performance optimisation features, insofar as such activities are necessary to provide and improve the Services within the agreed purpose.

Service Improvement and Security
Processing personal data as necessary to maintain, secure, troubleshoot, and improve the functionality, stability, and performance of the Services, provided that such processing remains within the purpose defined in Section A.1..

Sub-processors and Infrastructure
Engaging approved sub-processors and using appropriate technical infrastructure in accordance with the Agreement.

The Agreement, including Sections A.1–A.3 and A.5 (where applicable), as well as the Data Controller’s use and configuration of the Services, constitutes the Data Controller’s documented instructions.

No Zebra anonymises the information specified in A.3. for statistical purposes,product and services improvements including fine tuning of models and process the information as required by law,

including in connection with a legal decision, regulatory requirements, the bankruptcy of the data controller, death or the like.

The data processor shall not use personal data processed under this Agreement to train general-purpose or cross-customer AI models, or use such personal data for the data processor's own independent purposes, unless expressly authorised in writing by the data controller. This restriction does not apply to data that has been irreversibly anonymised and aggregated such that it can no longer be linked to an identified or identifiable individual, as such data falls outside the scope of the GDPR.

C.2. Security of processing

The level of security shall take into account:

The processing of data includes personal data covered by Article 9 of the General Data Protection Regulation on specific categories of personal data, which is why a high level of security has been established.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

However, the data processor shall – in any event, and at a minimum – implement the following measures that have been agreed with the data controller:

The implemented technical and organisational measures reflect that the overall risk to the rights and freedoms of data subjects is assessed as moderate, regardless of the risk assessment methodology applied. Where the data controller has specified in Appendix B that the processing may involve data from which special categories of personal data within the meaning of Article 9 GDPR can be inferred, the risk level for that customer configuration shall be assessed as elevated, and the data processor shall apply a correspondingly higher level of technical and organisational protection.

Encryption and Secure Transmission

Personal data is protected during transmission through the use of industry-standard encryption protocols (e.g., SSL/TLS).

External connections to the Data Processor's systems are secured using encrypted communication channels

Integrity, Availability and Resilience
The Data Processor maintains appropriate technical safeguards designed to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
Systems are in place to detect, manage, and respond to security incidents affecting personal data.

Backup and Restoration
Personal data is hosted in secure environments with backup mechanisms designed to enable restoration of data in a timely manner in the event of a physical or technical incident

Confidentiality and Access Control

Access to personal data is restricted to authorised personnel with a legitimate business need.

Access requires individual user authentication (unique username and password), and access rights are granted and reviewed based on role and necessity.

Logging and Monitoring

Access to personal data is logged. Logs may include information on user identity, time of access, and activity performed. Monitoring mechanisms are implemented to detect unauthorised access.

Data Retention and Deletion

Personal data is retained only for as long as necessary in accordance with the Data Controller's documented instructions and is deleted or returned upon termination of the Agreement, unless otherwise required by law..

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing such technical and organisational measures, which may contribute to the data controller's ability to respond to requests for the exercise of the rights of data subjects.

C.4. Storage period/erasure procedures

Personal data is retained only for as long as necessary to fulfil the purposes described in Appendix A and in accordance with the data controller's documented instructions.

Upon termination of the Agreement for any reason, the data processor shall delete all personal data processed on behalf of the data controller within 30 days of the termination date, unless EU law or the national law of the Member States requires that the personal data be stored for a longer period. The data processor shall provide the data controller with written confirmation that deletion has been completed. Until deletion is confirmed, the data processor must continue to ensure that these provisions are complied with.

C.5. Processing location

Processing of the personal data covered by the Regulations, with the data controller's prior general approval cf. C.1 and C.6, as well as prior notice to the data controller cf. 7.3, may take place in locations other than the following:

See B.1. Approved Sub-processors.
See C.2. Processing Security - Service and Database Security.

C.6. Instruction on the transfer of personal data to third countries

The data controller is aware of – and is obligated to make its customers aware – that the data processor's Services are made available through a cloud-based solution where the data processor makes use of software and IT systems, among other things, including servers provided by third parties.

To the extent that the data processor's Services make use of or are based on services provided by sub-processors in third countries, the data controller hereby instructs and authorises the data processor to transfer personal data to the data processor's sub-processors in such third countries for the purpose of the provision of services to which the data controller subscribes , as specified in the applicable commercial agreement.

The use of sub-processors in third countries must be subject to similar provisions to the provisions agreed between the data controller and the data processor, and the data processor is obliged to ensure that the transfer and data processing is carried out in accordance with applicable EU standard clauses for the transfer of personal data (EU standard contractual clauses).

In its agreement with sub-processors, the data processor shall include the data controller as a third-party beneficiary in the event of the data processor's bankruptcy, so that the data controller can enter into the data processor's rights and assert them against sub-processors, cf. Clause 7.6.

The transfer to third countries is done according to (i) EU-U.S. Data Privacy Framework, (ii) EU Commission standard regulation for data protection or (iii) the data protection regulation article 47, where transfer is done to one or several members of a corporate group subject to Binding Corporate Rules.
The applicable transfer basis for each sub-processor is specified in Appendix B. For sub-processors certified under the EU-U.S. Data Privacy Framework, the date of verification of the certification is indicated in Appendix B. The data processor shall maintain up-to-date records of the applicable transfer basis and shall update Appendix B accordingly when changes occur.

EU Standard Contract Clauses (Module 3)

Overview of companies with approved Binding Corporate Rules (pre-GDPR)

Overview of companies with approved Binding Corporate Rules (pre-GDPR)

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall give the data controller or a representative of the data controller access to carry out an inspection, including physical inspection, of the sites from which the data processor processes personal data, including physical sites and systems used for or in connection with the processing. Such an inspection is carried out annually when the data controller convenes for the possibility of inspection and must, where relevant, be carried out with a reasonable notice.

When the data controller decides on a review or audit, this may take into account relevant certifications held by the data processor.

The data controller's and the data processor's costs, if applicable, relating to an inspection shall be borne by the data controller.

The data processor shall be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

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

The data processor or the data processor's representative shall have access to an annual physical inspection of the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing to ascertain the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data processor may perform an inspection of the sub-processor when the data processor deems it required.

Documentation for such inspections shall without undue delay be submitted to the data controller for information.

The data controller may contest the scope and/or methodology of the report and may in such cases at its own expense and risk request a new inspection under a revised scope and/or different methodology.

Based on the results of such an inspection, the data controller may its own expense and risk request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller may at its own expense and risk elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor's and the sub-processor's costs related to a physical inspection at the sub-processor's facilities shall not concern the data controller unless the inspection is initiated by the data controller.

20. Appendix D - The Parties' agreement on other matters

The Parties have agreed on the following supplements for the Clauses:

For Clause 4.2

Notwithstanding Section 4.2, the data processor is not obliged actively to verify or investigate the legality of the data controller's instructions.

The data controller is aware that the data processor is dependent on the data controller's instructions on the extent to which the data processor is entitled to use and process the personal data on behalf of the data controller.

The data processor is therefore not liable for claims arising from the data processor's actions or omissions, to the extent that these actions or omissions are a direct data processing activity carried out in accordance with the data controller's instructions.

For Clause 7.3

The data controller acknowledges that the data processor's Services are standardised, cloud-based subscription services made available to a large number of customers and that the data processor is therefore not able to design the systems offered in such a way that each customer may require the data processor not to make use of specific sub-processors approved by the data processor.

Thus, the data controller acknowledges that if the data controller objects to the data processor's change or choice of new sub-processors and the data processor does not accommodate such an objection, the data controller's sole remedy is to terminate the subscription agreement with the data processor. The termination may take place with immediate effect, and neither party shall have any claim against each other in this connection.

For Clause 9.2

To the extent that the data controller wishes the data processor assistance to the services described in Clauses 9.2, (c) and (d), the data controller is obliged to remunerate the data processor for the time spent with the hourly rates used by the data processor at all times, as shown on the data processor's website.

For Clause 12.1

The data processor is obliged to allocate the resources necessary for the data controller or its adviser/representative to carry out its inspection and/or audit by the data processor or its sub-processors. "The costs incurred by the data processor in connection with a physical inspection and/or an audit carried out by the data processor or its sub-processors shall be borne by the data controller.

The time of the data processor and/or its sub-processors shall be reimbursed with the hourly rates used by the data processor at all times."

For Clause 13.1

The data processor's liability to the data controller is limited to what is set out in the commercial agreement. The liability limitation does not apply to the extent that such limitation is excluded under mandatory legislation, including the General Data Protection Regulation.

21. Version history:

Version 1.0 – First version - 27. May 2026