Agreement on Processing

(data protection pursuant to Art. 28 GDPR)

between

.....

.....

(if applicable: Authorized Representative pursuant to Art. 27 GDPR:

.....)

–Controller – hereinafter “Client” –

and

AEB SE

Sigmaringer Strasse 109

70567 Stuttgart

Germany

–Processor – hereinafter “Supplier” or “AEB” –

Contents

1 Recitals

1.1 Data Protection Legislation

Data Protection Legislation means, as applicable, the Data Protection Act 2018, the EU General Data Protection Regulation (2016/679) (GDPR), and the Privacy and Electronic Communications (EC Directive) Regulations 2000 and any applicable replacement legislation governing the use and security of personal data.

Controller, processor, data subject, personal data, personal data breach, processing and appropriate technical measures: shall all have the meanings given in the GDPR.

2 Subject matter, duration, and details of processing

2.1 Subject matter and duration of this agreement

(1) Subject matter

The subject matter of this agreement arises from and/or in connection with the service agreement ("Service Agreement").

The Service Agreement arises from the Supplier's individual confirmations of orders for the Supplier's services. The services typically include:

- the licensed use software solutions provided by AEB (Cloud or On-Premise model); and
- services (such as implementation, training, support and hosting).

(2) Duration

The duration (term) of this agreement corresponds to the term of the Service Agreement.

This agreement takes effect on the date of the last signature (including electronic confirmation).

Any earlier data protection agreements governing processing that may have been in effect are superseded by this agreement when it takes effect.

2.2 Specification of this agreement (details)

(1) Nature and purpose of the intended processing of personal data

The precise nature and purpose of the processing of personal data by the Supplier for the Client is set forth in the Service Agreement.

Unless otherwise specified, personal data is used to record the persons (name, contact information) responsible for transactions in the software solutions – so that such persons can be consulted if necessary, for example.

The objective in using the Compliance application for screening business contacts against the stored restricted party lists is to achieve compliance with EU prohibitions on the provision of goods and services and with the laws and regulations of other countries.

The contractually agreed processing of data shall be undertaken exclusively within a member state of the European Union or another signatory state of the European Economic Area Agreement. Any transfer to a state outside the European Union or European Economic Area requires the prior consent of the Client and must satisfy the specific requirements of Art. 44 et seqq. GDPR.

AEB may only provide services outside the area described above (such as in Switzerland) if an adequate level of protection can be assured.

(2) Type of personal data

The subject of the processing of personal data comprises the following data types/categories(list/description of data categories):

- [x] Personal master data (“prename”, “surname”; when using compliance screening at the choice of the Client optionally further data like “date of birth”)
- [x] Contact data (phone, email, etc.)
- [ ] Customer history
- [ ] Contract billing and payment data
- [ ] Disclosed information (from third parties such as credit reference agencies or from public directories)

(3) Categories of data subjects

The categories of data subjects comprise:

- [x] Customers
- [ ] Prospects
- [ ] Subscribers
- [x] Employees
- [x] Suppliers
- [ ] Authorized agents
- [x] Contacts

3 Scope and responsibility

(1) Supplier processes personal data on behalf of Client. This includes activities set forth in detail in the Service Agreement. Within the scope of this agreement, Client is solely responsible for the legality of its initial transmission of data to the Supplier. Both parties are responsible to comply with all applicable data protection laws in their roles defined in GDPR.

(2) The instructions are initially established by the Service Agreement and can then be modified, expanded,or replaced through individual instructions in written form or in an electronic format (text form) from Client to the contact designated by Supplier (individual instruction). Instructions not provided for in the contractshall be regarded as a request to modify the service. Oral instructions must be confirmed and documented in written or text form without undue delay.

4 Obligations of Supplier

4.1 Obligations to follow instructions

(1) Supplier may process the Data of data subjects only within the scope of the order and Client's instructions unless an exception as set forth in Art. 28(3) a) GDPR is present. Supplier shall notify Client without undue delay if Supplier believes that an instruction violates applicable laws. Supplier is entitled to delay carrying out the instruction until it is confirmed or modified by Client.

(2) Supplier assures that the employee entrusted with processing Client's Data and other persons working for Supplier are prohibited from processing the Data beyond the scope of Client's instruction. Supplier furthermore assures that the persons authorized to process personal data have promised to maintain confidentiality or are subject to an appropriate legal obligation of secrecy. This obligation of confidentiality/secrecy continues even after the termination of the order.

4.2 Technical and organizational measures

(1) Supplier shall organize internal operations within its area of responsibility to satisfy the specific requirements of the Data Protection Legislation. To provide appropriate protection of the personal data, Supplier shall implement appropriate technical and organizational measures necessary to protect the personal data against unauthorized and unlawful processing and against accidental loss, destruction, disclosure, damage or alteration satisfying the requirements of the General Data Protection Regulation (Art. 32 GDPR). Client is aware of these technical and organizational measures. Client has assessed the level of security appropriate to the processing in the context of the Data Protection Legislation and agrees that the measures adopted by Supplier are consistent with the requirements for the personal data to be processed.

(2) This must take into account the state of the art, the costs of implementation, and the nature, scope, and purposes of processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects as defined in Art. 32(1) GDPR [details in Annex 1].

(3) Before the processing commences, Supplier shall document the execution of the necessary technical and organizational measures set out before the order was issued, specifically with regard to the detailed execution of the order, and shall present these documented measures to Client for inspection. Upon acceptance by Client, the documented measures become the basis of the order. Insofar as the inspection/audit by Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(4) The technical and organizational measures are subject to technical progress and further development. Supplier is therefore permitted to implement alternative adequate measures as long as this does not reduce the security level of the established measures. Substantial changes must be documented.

(5) Supplier promises to comply with its obligations under Art. 32(1) d) GDPR and to implement a process for a regular efficacy review of the technical and organizational measures to ensure the security of the processing.

(6) For compliance with the agreed protective measures and their verified efficacy, reference is made to the current certifications (and any other applicable certificates) relating to data protection or information security, which can be presented to document appropriate assurances.

4.3 Rectification, restriction and deletion of data

(1) Supplier may only rectify, erase or restrict the processing of Data processed on behalf of Client in response to Client's documented instructions, not on Supplier's own authority. If a data subject contacts Supplier directly concerning a rectification, erasure or restriction of processing, Supplier shall forward the data subject's request to Client without undue delay.

(2) In special cases to be determined by Client, such data storage media and other materials are stored or handed over. The associated compensation and protective measures shall be negotiated separately if not already specified in other contracts.

4.4 Other support obligations

(1) Supplier shall support Client to the best of its abilities in satisfying the requests and demands of data subjects pursuant to Chapter III GDPR and in complying with its obligations set forth in Articles 32–36 GDPR.

(2) Supplier shall notify Client without undue delay if it becomes aware of violations of the protection of Client's personal data.

Supplier shall take the necessary measures to protect the Data and mitigate any possible negative consequences for the data subjects and consult with Client on such measures without undue delay.

(3) Supplier shall designate a Data Protection Officer for Client. The Data Protection Officer serves as a liaison for all data protection questions under the contract and can be reached at:

mailto:dataprotectionofficer@aeb.com. The current contact information is easily accessible on Supplier's website.

(4) Data, data storage media, and all other materials must be surrendered or deleted after the end of the order if requested by Client, unless Supplier is required to retain such personal data under applicable laws.

Any additional costs incurred through differing or not yet defined specifications during the surrender or deletion of the data shall be borne by Client.

(5) Supplier shall support the Client in keeping records of processing activities as defined by Art. 30 GDPR.

(6) Supplier shall undertake appropriate measures to assist the Client in regard to any required assessment of the impact of data protection pursuant to Art. 35 GDPR. Supplier shall provide Client with the relevant information, especially on the results of the assessment, if it affects the processing that is the subject of this agreement.

(7) Client and Supplier shall work upon request with the regulatory authority to complete their tasks.

(8) If permitted to do so by the regulatory authority, Supplier shall notify Client without undue delay of any controls and measures undertaken by the regulatory authority if they relate to this order. This applies even if a responsible authority in administrative or criminal proceedings relating to the processing of personal data investigates Supplier's processing activities.

(9) If Client itself is subjected to a check by the regulatory authority, administrative or criminal proceedings, liability claims by a data subject or third party, or any other claim relating to Supplier's processing, Supplier must support Client to the best of its abilities.

5 Obligations of Client

(1) Client shall comply with the Data Protection Legislation and ensure that all instructions it gives to Supplier in respect of the personal data are and shall be lawful and in compliance with the Data Protection Legislation.

(2) Client must provide Supplier with prompt and complete information of any errors or irregularities with regard to data protection provisions set out in this agreement that Client identifies.

(3) Client shall promptly notify Supplier in writing (email is sufficient) of the contact person responsible for all questions relating to data protection under this contract and shall also promptly notify Supplier whenever this information changes. The contact information at the time the contract is signed (generic information is sufficient) is as follows:

.....

(4) Client shall consider the impact that changes to its usage or extensions may have on this Agreement on Processing and notify the Supplier of such changes without undue delay. This can trigger changes in section 2.2.

6 Requests from data subjects

(1) If a data subject turns to Supplier with demands to rectify, delete, or provide data, Supplier shall refer the data subject to Client if a referral to Client is possible based on the information provided by the data subject. Supplier shall forward the data subject's request to Client without undue delay. Supplier shall support Client to the best of its abilities when instructed if so agreed.

7 Controls and documentation options

(1) Supplier shall use appropriate means to provide the Client with documentation of compliance with the obligations set forth herein.

(2) To document compliance with the agreed obligations, Supplier can provide the Client with the following information:

- Performance of a self-audit
- Data protection and/or information security certificate (such as ISO 27001)
- Current attestations, reports, or report excerpts from independent authorities (internal or external auditors, data protection official, IT security department, data protection auditors, quality auditors)
- Approved codes of conduct as defined by Art. 40 GDPR
- Certifications as defined by Art. 42 GDPR

(3) Supplier shall ensure that Client can verify Supplier's compliance with its obligations as defined by Art. 28 GDPR. Supplier commits to provide the Client with the necessary information upon request and in particular to document implementation of the technical and organizational measures.

(4) Any audit (including inspection) of Supplier's premises by Client or an auditor engaged by Client that might prove necessary in a particular instance shall be conducted during normal business hours without disrupting business operations and only after giving adequate advance notice. Supplier may make such audits contingent on adequate advance notice and the signing of a statement of confidentiality regarding the data of other customers and the technical and organizational measures that have been put in place. Supplier is entitled to veto the Client's appointment of an auditor who is in competition with Supplier.

(5) Should the inspection be undertaken by a data protection authority or any other sovereign regulatory authority of Client, subsection 4 shall always apply accordingly. No statement of confidentiality is required if this regulatory authority is subject to a professional or legal confidentiality whose violation is punishable under the German Criminal Code.

8 Subcontractor (other processors)

(1) Subcontractor relationships as defined here are services relating directly to the provision of the primary service. This does not include incidental services of which Supplier avails itself, such as telecommunications services, postal or transport services, maintenance and user services, or any other measures undertaken to ensure the confidentiality, availability, integrity, and resilience of the hardware and software of data processing systems. Even in the case of outsourced services, however, Supplier shall ensure that all subcontractors are subject to contractual obligations which are reasonably equivalent to those imposed on the Supplier under this agreement. Supplier shall remain fully liable to Client for the performance of any subcontractor's obligations under the Data Protection Legislation.

(2) A subcontracting relationship requiring approval is present when Supplier hires other contractors to perform, in whole or in part, a contractually defined service. Supplier shall enter into agreements of an appropriate scope with these third parties to ensure that appropriate data protection and information security measures are taken.

(3) The use of subcontractors as additional processors is permissible only with the prior consent of Client.

Client hereby issues a "general written authorization" pursuant to Art. 28(2) GDPR for the Supplier to engage subcontractors.

The contractually agreed services or the partial services are to be carried out with the assistance of subcontractors. The current list of these subcontractors can be found on AEB's website at www.aeb.com/subcontractors. By signing this agreement, Client agrees to the use of these subcontractors.

AEB shall notify Client through Client's contact designated under section 5(3) herein before making any changes involving the addition of subcontractors or the replacement of currently listed subcontractors.

Such notification shall include the following:

- Name, address, contact of subcontractor
- Subcontracted service of subcontractor
- Client's options in response to this change

(4) Client may object to the change – for cause – to Supplier's designated contact within an appropriate period (of 6 weeks after receipt of the information). If no objection is raised within this period, the consent to the change shall be regarded as granted. If an objection is raised in due time, and if there is

cause, and if the parties cannot agree on a solution within 4 weeks of receipt of the objection, both parties shall have a special right of termination for this and the part of the Service Agreement affected by this processing.

(5) If Supplier assigns orders to subcontractors, it is the responsibility of Supplier to transfer its data protection obligations under this agreement to the subcontractor.

(6) Client's personal data may not be shared with the subcontractor and the subcontractor may not commence its activities until all the conditions for subcontracting defined herein for have been met.

9 Use of AEB subsidiaries outside of EU

9.1 Introduction

Unless otherwise regulated, it is not excluded that the AEB subsidiaries mentioned below may provide services (such as support or project services) within the scope of the present order processing and may also gain access to personal data.

Name of subcontractor	Address, seat	Description of Service	Legal basis
AEB (International) Ltd	3 Olympus Court, Olympus Avenue, Tachbrook Park, Warwick CV34 6RZ, UK	Project- and support-Services (direct contact with controller possible)	Art. 45 GDPR
AEB (Asia Pacific) Pte Ltd	70 Shenton Way, #20-15 EON Shenton, Singapore 079118	Project- and support-Services (direct contact with controller possible)	Art. 46 Sect. 2 c) GDPR (SCC, using MODULE THREE)
AEB Schweiz AG	Sihlquai 131, 8005 Zürich, Schweiz	Project- and support-Services (direct contact with controller possible)	Art. 45 GDPR

These above-mentioned majority controlled AEB company subsidiaries are each based in a third country.

9.2 Information on integration within the corporate group

AEB SE warrants that the AEB subsidiaries

- are integrated via an internal, legally compliant agreement on personal data processing.
- participate in the necessary training and further training measures, e.g. on IT security and data protection, and be instructed in the obligations of the GDPR.
- the employees sign appropriate agreements on confidentiality.

- provide data protection coordinators who are in direct and regular contact with the data protection officer of AEB SE.
- fulfil the same level of protection of the common security concept within the AEB group of companies.

AEB regularly reviews whether there are indications in the above countries to introduce additional security measures in accordance with the recommendations of the EDPB.

10 Deletion and return of personal data

(1) No copies or duplicates of the Data shall be created without the knowledge of Client except for backup copies that may be needed to ensure proper data processing and data required to comply with data retention laws.

(2) Upon completion of the contractually stipulated work, or earlier if requested by Client – but no later than upon termination of the Service Agreement – all documents, all results derived from the processing and use of the data, and all data records relating to the contractual relationship that Supplier has acquired must be surrendered to Client or, after prior consent, destroyed in compliance with data protection laws. The same applies to testing and scrap material. Documentation of this deletion must be presented upon request.

(3) Documentation whose purpose is to demonstrate that data was processed properly and as requested must be retained by Supplier in keeping with the appropriate data retention periods beyond the end of the contract term. Supplier may hand over such data to Client at the end of the contract term in discharge of its obligations.

11 Notification requirements, written form, choice of law

(1) Supplier must notify the Client without undue delay if Client's Data held by Supplier is in danger of being seized or confiscated or is threatened by insolvency or receivership proceedings or other events or measures of third parties. Supplier shall promptly notify all persons responsible in such circumstances that the ownership of and sovereignty over the Data rests solely with the Client, who is the "controller" as defined the by General Data Protection Regulation.

(2) Any amendment or addition to this Agreement on Processing and all its components – including any assurances of Supplier – must be agreed to in writing, which may include electronic formats (text form), with an express reference indicating that it is an amendment or addition to these terms. This applies as well to any waiver of this requirement of written form.

(3) Should any contradictions arise, the terms of this Agreement on Processing take precedence over any Service Agreement. Should individual parts of this Agreement on Processing be found invalid, this shall not affect the validity of the rest of the Agreement on Processing.

(4) These terms are subject to the laws of the Federal Republic of Germany.

12 Business terms

This agreement is subject to the obligations of collaboration and support agreed between the parties and set forth in law.

Supplier shall support Client in the following situations:

- Supplier shall support Client to the best of its abilities in satisfying the requests and demands of data subjects pursuant to Chapter III GDPR and in complying with its obligations set forth in Articles 32–36 GDPR.
- Supplier commits to provide the Client with the necessary information upon request and in particular to document implementation of the technical and organizational measures. Supplier shall support Client in conducting inspections/audits.

Unless Supplier is culpable for causing the costs incurred Client is under the obligation to compensate Supplier's efforts. A contingent of eight (8) person hours per year will not be invoiced by Supplier. Once this contingent has been exhausted, Client shall pay the Supplier's further costs for support described above at the Supplier's hourly rate in effect at that time.

13 Annexes

13.1 Technical and organizational measures (Annex 1)

13.1.1 Description

List of technical and organizational measures; collaborative document on the current status entitled: "Data Security at AEB SE."

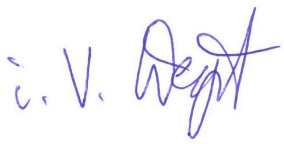
The measures may and should be updated in keeping with the state of the art in such a way that the previously attained level of data protection is not reduced.

13.1.2 About this document

The document on the technical and organizational measures in its current form is attached to this agreement as Annex 1 and can be provided in the future upon request in its current version at the time by the data protection officer.

Until further notice, it is also available on AEB's website at www.aeb.com/security-concept under the name Security Concept

Supplier AEB SE

City	Stuttgart
Date	August 09, 2021
Name / position	Volkher Wegst / Data Protection Officer
Signature	

Client

City	
Date	
Name / position	
Signature	

City	
Date	
Name / position	
Signature	