Processing Agreement Aristotle Technologies B.V.

Data Processing, Secrecy, Hosting

Version 2.1, August 24, 2023

This Processing Agreement applies to all forms of data processing, in particular (personal) data, that Aristotle Technologies B.V., registered with the Chamber of Commerce under number 84657111 (hereinafter: Processor) carries out for the benefit of a counterparty to whom it provides services. (hereinafter: Controller), and for which Processor and Controller have entered into an *Agreement for the provision of services*, of which the (i) *ARISTOTLE END USER LICENSE AGREEMENT* and (ii) *SOFTWARE SUPPORT & MAINTENANCE TERMS & CONDITIONS* (hereinafter: the **Terms and Conditions**) are part of.

A. Processing of data

Article 1. Purposes and subject of the processing

1.1 Under the terms of this processing agreement (hereinafter: the **Processing Agreement**), the Processor undertakes to process data, possibly including personal data, on the instructions of the Controller.
Processing will only take place in the context of providing web-based services, managed by the Processor (hereinafter: **Platform**), and furthermore those purposes that are reasonably related thereto or that are determined with further consent.
The Platform is offered either on servers under the management of or on behalf of the Controller, or on servers under the management of the Processor, which includes the storage of data of the Controller (hereinafter: ***Hosted Platform***).

1.2 The Processor will not process the (personal) data made available for any purpose other than as determined by the Controller. The Controller will inform the Processor of the processing purposes insofar as they have not already been mentioned in this Processing Agreement. The activities and processing to be carried out by the Processor are exhaustively listed in *Appendix A*.

1.3 Processing of data is carried out in accordance with generally accepted guidelines in the Netherlands and with due observance of the provisions of this Processing Agreement. The Processor carries out limited checks on (personal) data provided by the Controller; statistical tests are only performed where appropriate for substantive considerations. Processor takes all possible care in the processing of (personal) data, but cannot give any guarantees with regard to the processing of (personal) data, any incompleteness or errors in processing. Processor is in no way liable for errors that arise as a result of any interpretation of (personal) data presented in the Platform.

1.4 The controller guarantees that the processing of (personal) data falls under one of the exemptions under the GDPR, and that no notification to the Dutch Data Protection Authority is therefore required.

Article 2. Obligations Processor

2.1 With regard to the processing operations referred to in Article 1, the Processor will ensure compliance with the applicable laws and regulations, including in any case the laws and regulations in the field of the protection of (personal) data, such as the General Regulation Data Protection (GDPR).

2.2 The Processor will inform the Controller, at its first request, about the measures it has taken regarding its obligations under this Processing Agreement.

2.3 The Processor is expressly not permitted to use personal data for its own purposes. The Processor ensures that these obligations are also fulfilled by the personnel it engages.

2.4 The obligations of the Processor arising from this Processing Agreement also apply to those who process (personal) data under the authority of the Processor, including but not limited to employees, in the broadest sense of the word.

2.5 The Processor will immediately notify the Controller if, in its opinion, an instruction from the Controller constitutes a breach of privacy laws and regulations or may lead to this. The Processor accompanies this notification of the motivated reasons why the Processor believes that the instruction constitutes or may constitute an infringement of privacy laws and regulations.

Article 3. Transfer of (personal) data

3.1 Processor may process the (personal) data in countries within the European Union. Transfer to countries outside the European Union is prohibited.

3.2 The Processor will inform the Controller of the country or countries involved.

Article 4. Division of Responsibility

4.1 The permitted processing is carried out by fully automated means under the control of the Processor.

4.2 The Processor is responsible for the processing of the (personal) data under this Processing Agreement, in accordance with the instructions of the Controller. For the other processing of (personal) data, including in any case but not limited to the collection of the (personal) data by the Controller, processing for purposes that have not been reported to the Processor by the Controller, processing by third parties and/or for other purposes, the Processor is expressly not responsible. Part of these other processing operations is also the use of data that is exported from the Platform, in any way whatsoever.

4.3 The Controller guarantees that the content, use and order to process the (personal) data as referred to in this Processing Agreement is not unlawful and does not infringe any right of third parties.

4.4. With the Platform, (personal) data can be processed with regard to the use of the Platform. Here too, the Controller is the Controller, and the Processor is the Processor. When using this data by the Controller, it undertakes to inform the Data Subjects about this and/or to request permission.

Article 5. Security

5.1 Processor will take all appropriate technical and organizational measures in accordance with Article 32 of the GDPR legislation to protect personal data against loss or any form of unlawful processing (hereinafter: the **Security Measures**). These Security Measures guarantee an appropriate level of security in view of the state of the art, the implementation costs, as well as in view of the nature, scope, context and processing purposes and the varying likelihood and severity of the risks that the processing of the personal data processed by the Processor entails for the rights and freedoms of data subjects.

5.2 The Processor has in any case taken the following Security Measures:

Company culture

- Data security is a regular subject that receives attention within the Processor's organization.

Technology

- A secure internal network within the Processor's organization. This has been set up on the basis of proven products Office365 and Azure from Microsoft.
- This means that hosting of servers is outsourced to third parties that are at least certified for ISO 9001, 22301, 20000-1, 27018, 27017, 27001.
- This enables encryption (encryption) of digital files with (personal) data. No storage of personal data on computers other than servers such as laptops.
- Logical access control, using personal passwords. The use of strong passwords is enforced.
- Automatic logs of the use of the Platform.
- Security of network connections via Secure Socket Layer (SSL) technology.

Organization

- Physical measures for access security.
- General organizational measures for access security.
- Random check for policy compliance.
- Purpose-bound access restrictions to collections of (personal) data that are processed.
- Aristotle Technologies B.V. has commissioned experts in the field of data processing for the implementation of the security of (personal data in) the Platform in order to comply with GDPR legislation, and follows the advice given by these experts.

5.3 The Processor hereby guarantees that the implemented measures, as referred to in Article 5.2, at least comply with what is stipulated in the privacy laws and regulations and in particular with Article 32 of the GDPR legislation.

5.4 The Processor hereby also guarantees that it will comply with the instructions of the Controller in the context of the security of personal data processed by the Processor on behalf of the Controller

(if this can reasonably be required of the Processor). The Processor does not guarantee that the security is effective under all circumstances.

5.5 Processor will regularly evaluate the measures referred to in Article 5.2 and supplement and change them where necessary to comply with privacy laws and regulations. The Processor always informs the Controller prior to any addition or change of the measures by means of a notification.

5.6 In the case of *Hosted* Platform, that which is in *Appendix B Hosted Platform* is applicable.

5.7 The Controller will only make (personal) data available to the Processor for processing if it has ensured that the required security measures have been taken.

5.8 When developing and managing the Platform, developers of the Processor need temporary access to (personal) data of the Controller, or parts thereof, on systems under the management of the Processor.

5.9 In the context of development, the Processor can use the logs of the use of the Platform. The purpose of this is to optimize the use for the benefit of the users, both in the Platform and by means of advice to users where necessary.

5.10 If the Controller, for whatever reason, judges that the security of personal data by the Processor no longer meets the requirements of the Controller, then the Controller is entitled to dissolve this Processing Agreement without judicial intervention and immediately by sending a written message. to Processor. If this situation arises, the Processor will immediately cooperate in carrying out the exit procedure as described in Article 14 of this Processing Agreement.

Article 6. Reporting obligation

6.1 In the event that a security leak and/or a data leak is detected by the Processor or the Controller, the Processor and the Controller, respectively, will immediately inform the other party about this (but in any case within twelve (12) hours). The Controller assesses whether it will inform the data subject or not, and is responsible for that choice.

6.2 The obligation to report referred to in Article 6.1 includes in any case a description of the following:

- What is the (alleged) cause of the vulnerability and/or data breach;
- The nature of the security breach and/or data breach, including where possible the categories of data subjects and personal data affected and, approximately, the number of data subjects and personal data affected;
- What are the (as yet known and/or expected) consequences of the vulnerability and/or a data leak;
- The measures proposed by the Processor to address the security breach and/or the data breach, including, where appropriate, the measures to limit any adverse consequences thereof;
- Contact details for following up on the report.

6.3 Taking into account the nature of the processing and the information available to it, the Processor will assist the Controller in complying with the obligations under Articles 33 and 34 of the GDPR

legislation, more specifically, the Processor will assist the Controller in reporting a security breach and/or a data breach or a similar incident to the supervisory authority and/or the data subject(s).

6.4 Processor hereby undertakes to implement an appropriate policy with regard to security leaks and/or data leaks, such as but not limited to protocols that comply with privacy laws and regulations. The Controller is entitled to inspect these protocols on first request and is entitled to obtain a copy of them from the Processor, also on the first request of the Controller.

6.5 If a situation as referred to in Article 6.1 arises, the parties hereby undertake to maintain the confidentiality of any information in connection with the security leak and/or data leak. The parties will not disclose information about this under any circumstances without the prior written consent of the other party.

6.6 If the report is made as stipulated in Article 6.1, the parties will remain available and reachable for consultation with the other party. The parties also ensure that the personnel involved in determining or resolving the security breach and/or the data breach is available to the other party.

6.7 In connection with, among other things, the reputation to be maintained by the Controller in its industry and/or in general, the Controller is exclusively responsible for any notification to the Dutch Data Protection Authority or Data Subjects. The Processor will never independently report to the Dutch Data Protection Authority or Data Subjects, unless the Processor is obliged to do so on the basis of applicable laws and regulations.

6.8 The parties acknowledge that under certain circumstances they are legally obliged to report a breach of security (of whatever nature) that (partly) relates or may relate to the personal data processed by the Processor to data subjects and/or authorities. Such a report by a party will never be regarded as a failure to comply with this Processing Agreement or otherwise as an unlawful act. Parties will take all measures necessary to limit the (possible) damage of a security breach and will support the other party in reporting to data subjects and/or authorities.

Article 7. Handling requests from data subjects

7.1 In the event that a data subject submits a request to the Processor to exercise his rights set out in Chapter III of the GDPR legislation (including, but not limited to, inspection, improvement, addition, amendment or shielding), the Processor will forward the request to the Controller , and the Controller will further process the request.
The Processor only extracts (personal) data from systems of the Controller and improvement, addition or change must therefore first take place in these systems, and the Controller must make adjustments thereof in the Platform.

7.2 Processor will, taking into account the nature of the processing, assist the Controller by means of appropriate technical and organizational measures, insofar as possible, in fulfilling its duty to answer the request of the data subject's rights set out in Chapter III of the GDPR legislation.

7.3 Processor will, insofar as permitted by law, promptly inform the Controller if the Processor receives a request from a data subject in connection with the rights that the privacy laws and regulations offer the data subject. Processor will not meet any request from a data subject.

Article 8 Audit

8.1 The controller has the right to have audits carried out by an independent third party who is bound by confidentiality to verify compliance with the general rules regarding the processing of (personal) data, and everything that is directly related to this. Processor will cooperate in this.

8.2 The Processor will cooperate with the audit and provide all information relevant to the audit, including supporting data such as system logs, and employees as soon as possible.

8.3 The findings resulting from the audit performed will be assessed by the Parties in mutual consultation and, as a result thereof, whether or not implemented by one of the Parties or by both Parties jointly.

8.4 The costs of the audit are borne by the Controller if the audit takes place at the request of the Controller.

B. confidentiality

Article 9. Confidentiality and confidentiality of data

9.1 All (personal) data that the Processor receives from the Controller and/or collects itself in the context of this Processing Agreement is subject to a duty of confidentiality towards third parties. Processor (and employees authorized to process personal data) will not use this information for any other purpose than for which it was obtained.

9.2 Processor guarantees that the persons authorized to process personal data have committed themselves to observe confidentiality, by means of written confidentiality agreements. The Processor hereby assures that the provisions of these confidentiality agreements that ensure the confidentiality of personal data will survive the termination of the agreements that form the basis of the relationship between the employee and the Processor.

9.3 This confidentiality obligation does not apply insofar as the Controller has given explicit permission to provide the information to third parties, if the provision of the information to third parties is logically necessary in view of the nature of the assignment given and the implementation of this Processing Agreement, or if there is there is a legal obligation to provide the information to a third party, as further specified in Article 11.

9.4 Both during and after termination of this Processing Agreement, the parties undertake to observe complete confidentiality towards third parties with regard to all data and information regarding matters of the other Party - in the broadest sense of the word - of which one Party knows the confidential nature, or ought to know, as well as of all matters in respect of which secrecy has been imposed. This is without prejudice to informing third parties that the Processor is carrying out an assignment from the Controller, as well as providing information to third parties that is necessary for the performance of the agreed activities.

C. Hosted Platform

Article 10. (Personal) data in case of Hosted Platform

10.1 (Personal) data made available by the Controller remains the property of the Controller or the Data Subject at all times.

10.2 The following applies to the storage and destruction of (personal) data. Hosted Platform works with (personal) data from the primary information systems of the Controller , and only records limited additional data, i.e. data about the performance of tasks and tests. Storing and destroying data originating from primary information systems is the responsibility of the Controller, and not of the Processor.

10.3 The retention periods of the additional data are equal to the periods used for the back-up solution used for Hosted Platform.

Article 11. Provision to third parties

11.1 The (personal) data provided processed in the Hosted Platform will not be made available to third parties by the Processor without the prior consent of the Controller, unless the Processor is obliged to do so under any legal provision, regulation or other regulation, or if the disclosure and/or provision in the context of services is necessary.

11.2 If the Processor receives a request or an order from a Dutch or foreign supervisor or an investigative, criminal investigation or national security authority to provide (access to) (personal) data, including but not limited to a request based on the USA Patriot Act, the Processor will immediately inform the Controller. When handling the request or order, the Processor will comply with all instructions from the Controller (including the instruction to leave the handling of the request or order in whole or in part to the Controller) and provide all reasonably necessary cooperation. In the event that legal privilege applies, the Processor will act as described in Appendix *A*.

D. General

Article 12. Liability

12.1 The parties expressly agree that with regard to liability that which is included in the Terms and Conditions applies.

Article 13. Duration, Termination and exit procedure

13.1 This Processing Agreement is concluded by entering into an Agreement for the provision of services between the parties and on the date of entering into that Agreement for the provision of services.

13.2 This Processing Agreement is entered into for the duration of the Agreement for the provision of services.

13.3 As soon as the Processing Agreement has been terminated, for whatever reason and in whatever way, the Processor will remove and/or destroy all (personal) data that it has. The Processor is entitled to retain anonymized data that (i) cannot be traced back to identifiable persons in any way and (ii)

cannot be traced back to the Controller and data subjects, as these are used to further optimize the Platform.

13.4 Processor is entitled to revise this agreement from time to time. It will notify the Controller of the changes at least one month in advance.

13.5 If the Processor, for whatever reason, but contrary to the wishes of the Controller, is unable to destroy or remove the Personal Data on the basis of this article, the Processor will immediately inform the Controller of this in writing. In that case, the Processor will, until otherwise instructed by the Controller, take all necessary measures to:

13.5.1 get as close as possible to complete destruction or deletion of the personal data, and make the personal data unsuitable for further processing;

13.5.2 the risk that the personal data will not be returned, destroyed or removed remains with the Processor and the Processor remains bound by those articles of this Processing Agreement which, given their nature, are intended to continue to apply after the expiry or termination of this Processing Agreement.

13.6 In the event of the destruction or removal of (personal) data, the functionalities of the platform may be limited with regard to the destroyed or deleted data. Controller accepts these consequences.

13.7 Article 9 (Confidentiality), Article 12 (Liability) and Article 14 (Applicable law and choice of forum) will continue indefinitely between the Parties after the termination or dissolution of this Processing Agreement, for whatever reason.

Article 14. Applicable law and dispute resolution

14.1 If one or more provisions of this Processing Agreement prove to be invalid, the Processing Agreement will otherwise remain in force. The parties will consult about the provisions that are not legally valid, in order to make a replacement regulation that is legally valid and that corresponds as much as possible with the purport of the regulation to be replaced.

14.2 The Processing Agreement and its implementation are governed by Dutch law.

14.3 All disputes that may arise between the Parties in connection with the Processing Agreement will be submitted to the competent court for the district in which the Processor is located.

Appendix A Explanation

Ad. Application

Prior to processing, an *agreement for the provision of services is* concluded between the Controller and the Processor, of which this Processing Agreement forms an integral part. This can be a quote, offer, letter of intent, partner agreement or similar.

The Processor also applies this Processing Agreement if it concerns (personal) data that has been made available to the Processor in the context of a pilot, preliminary phase, or any other contact with potential customers. Making (personal) data available to the Processor implies application of this Processing Agreement.

Ad. Article 1.2. Edits

The operations that the Processor performs on the (personal) data are as follows. Processes other than those listed below will not be carried out without explicit agreement with the Controller.

1. Limited control of the correct use of (personal) data and data fields.
2. Capturing task and test data during the execution of tasks and tests by individual users.
3. Enabling supervisors to monitor and analyze the task and test performance of both individual users and groups of users for which the supervisor is responsible.
4. Use of this data in anonymized form, with the aim of optimizing effectiveness for each individual user through AI.
5. Use of this data in anonymized form, with the aim of optimizing the effectiveness for all users of the Platform through AI.
6. Use of anonymized personal data for conducting scientific research in order to investigate and further improve the effectiveness of the Platform.
7. Derivation of anonymized personal data for demonstrations of the Platform to third parties, in such a way that neither the Controller nor the data subjects can be identified in any way.

Ad. Article 11. Third parties - legal privilege

If there is a professional duty of confidentiality and the associated right of non-disclosure on the part of the Controller, and officials on behalf of the Ministry of Justice inform the Processor that they wish to conduct a house search and/or seize evidence at the offices of the Processor, the Processor and its employees will act as follows.

To the relevant official(s) on behalf of the Ministry of Justice:

- information is provided about the places, both physical and virtual, where data subject to confidentiality is located;
- is informed that the relevant Controller must be notified immediately of the search and/or seizure, in order to allow the Controller to be present as a witness, or to have it assessed during a house search whether the requested information has been entrusted to the Controller in the capacity to which the waiver applies, and should be regarded as the object of the waiver ;

- is informed that employees of the Processor will not cooperate with access to data until the Controller in question is present on site;
- is informed that the Processor and its employees will refrain from any cooperation in obtaining access to data until the Controller in question is present on site.

Appendix B Hosted Platform

This appendix does not apply if the Controller provides its own hosting provider for the Platform, or takes care of servers in its own server park. In that case, what is stated below with regard to certification, applicable law, Disaster Recovery and Availability, security of connections, authorization, is the responsibility of the Controller and not of the Processor.

1. Hosting provider

Server Hosting for Hosted Platform involves Processor from Microsoft Azure.

Microsoft Azure was chosen as hosting provider because Microsoft Azure is ISO 9001, 22301, 20000-1, 27018, 27017 and 27001 certified.

Hosted Platform uses one Microsoft Azure data center

Controller agrees that Disaster Recovery and Availability are adequately covered by this.

2. Hosting provider in Europe for applicable law

The data centers of Microsoft Azure are located on European territory, and therefore not outside Europe. This ensures clarity about applicable law.

The controller agrees that matters with regard to applicable law are adequately covered by this.

3. Connection Controller – Microsoft Azure for security access

Only HTTPS connections are used to access the Platform.

Dedicated data connections are possible, but only on request, and they are not a standard part of the Hosted Platform.

4. Authorization Controller for security access

The Controller and the Processor undertake to take common measures for the security of the systems involved. The Controller is aware of the fact that security also includes taking organizational measures and will also impose this on staff, users and third parties.

The Controller ensures that all users and/or other third parties attributable to it who have access to the Platform in any way will also use and observe the necessary security measures.

In addition to the authorization set up by the Controller, the Platform itself also records, by or on behalf of the Controller, which users have access on behalf of the Controller. Checks are carried out on requests for access to the Platform. The Platform enforces the use of strong passwords. Passwords for admin users are created by representatives of Aristotle Technologies BV. A strong password is required.

The Processor does not apply additional multi-factor authentication, to which the Controller agrees.

5. Shared use

With Hosted Platform, Controllers share the use of infrastructure and the layout of the Platform. After all, one of the intended benefits of Hosted Platform is that sharing leads to faster availability, and this is important for that.

For a Hosted Platform, one or more (virtual) servers are set up that only Dutch users of the same Hosted Platform use. This means that only Dutch Data Controllers and only users of the same Platform have access to the same server.

Processor takes appropriate technical and organizational measures to ensure that users only see (personal) data from their own organization.

Exceptions to this, if explicitly agreed, may relate to benchmarking and/or regional cooperation. In such cases, further agreements are always made in advance and laid down in the relevant agreement for the provision of services.

A Dedicated server, one physical or virtual server per Controller, is possible, but only on request, at the applicable cost, and is not a standard part of Hosted Platform. Consent to a Hosted Platform agreement implies consent of the Controller to the shared use described.

6. Fair use

The Processor offers the Hosted Platform on the basis of a fair use principle, which means that the Processor does not, in principle, impose any restrictions on the system and network load by or on behalf of an individual Controller. The Processor reserves the right to take measures if an individual Controller generates such a load that other users are hindered in their use. If, in the reasonable opinion of the Processor, a danger arises or threatens to arise for the functioning of the infrastructure, being the technical platform with which the Hosted Platform is realized for the Controller, and/or the service, the Processor may require the Controller to take measures to prevent such a danger.
The Controller and/or user(s) are not permitted to use the Hosted Platform in such a way that damage may occur to the Hosted Platform, to the Processor or to a third party, and/or as a result of which malfunctions may occur in the Hosted Platform.

The Controller will follow the instructions of the Processor when using the Hosted Platform.

7. Exit control

Upon termination of the agreement for Hosted Platform, the Processor will, at the first request of the Controller and for an agreed fee, cooperate in the transition of additional data to the Controller or to a third party to be designated by the Controller. This means that the Processor makes relevant data files available in CSV format. The (personal) data that has been made available from the systems of the Controller will not be returned because it is already in the possession of the Controller - the above with regard to destruction applies to this.

A request as referred to in this article may be refused in the event of payment arrears. Partly due to the protection of (personal) data, the Controller cannot under any circumstances require the Processor to run third-party computer software on the Processor's equipment or to allow third parties to otherwise gain access to the Processor's equipment.