

Schedule III. Data Processing Agreement

Reference: ARST-DPA-2026-10 · version 1.0 · October 2026

Agreement entered into pursuant to Article 28 of Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR"), and Article 33 of Spanish Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights ("LOPDGDD").

Controller: the Customer identified in the Master Agreement or, if no Master Agreement has been signed, the professional user who accepts this Agreement when uploading a portfolio to the Platform (the "Controller").

Processor: ARSTDATA LABS SL, NIF B88701362, with the registered office stated in the [legal notice of the Site](#) and data protection contact at info@arstdata.com ("ARST Data" or the "Processor").

This Agreement forms part of the Master Licence and Services Agreement ARST-CM-2026-10 (the "Master Agreement") or, failing that, of the [General Terms of Use and Sale of arstdata.com](#). It prevails over any other provision as regards the processing of personal data.

1. Subject matter

1.1. This Agreement governs the processing of personal data that ARST Data carries out on behalf of the Controller when providing the Services, in particular the portfolio monitor, retrospective back-testing and the professional services that require uploading portfolio or contract data of the Controller.

1.2. The details of the processing (purpose, categories of data and data subjects, duration) are set out in Appendix 1.

2. Instructions

2.1. ARST Data shall process personal data only on the documented instructions of the Controller. The Master Agreement, the Service Order, this Agreement and the configuration of the Services that the Controller makes on the Platform constitute its complete instructions. Additional instructions must be given in writing and, if they involve a cost or a change to the Service, shall be processed as an amendment to the Service Order.

2.2. ARST Data shall inform the Controller immediately if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions, and may suspend its execution until the Controller confirms or amends it.

2.3. If Union or Member State law requires ARST Data to process the data for another purpose, ARST Data shall inform the Controller of that legal requirement before the processing, unless that law prohibits such information on important grounds of public interest.

3. Minimisation of the data provided

3.1. The Services operate with vehicle and contract data that do not directly identify individuals. The Controller shall provide pseudonymised contract references and shall not provide names, identity documents, contact details, registration plates or VINs, unless the Service Order expressly authorises it for a specific purpose.

3.2. The Platform may reject files that contain columns identified as direct identifiers. This check is a supporting measure and does not release the Controller from its minimisation obligation.

3.3. The Controller retains the information that allows the pseudonymised references to be linked to the data subjects. ARST Data shall not attempt to re-identify the data subjects.

4. Obligations of the Controller

The Controller warrants that: (a) it has a valid legal basis for the processing and for entrusting it to ARST Data; (b) it has informed the data subjects in accordance with Articles 13 and 14 of the GDPR; (c) the data it provides are adequate, relevant and limited to what is necessary; and (d) it will comply with its own obligations as controller, including, where applicable, those relating to automated decision-making and data protection impact assessments.

5. Obligations of ARST Data

ARST Data undertakes to:

- a) process the personal data only for the purpose set out in Appendix 1 and in accordance with the Controller's instructions;
- b) not use the personal data for its own purposes, not disclose them to third parties other than the sub-processors authorised under clause 7, and not incorporate them into the Market Data or

- use them to train or calibrate models offered to other customers;
- c) ensure that the persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they access the data only to the extent necessary to provide the Services;
 - d) implement the technical and organisational measures set out in Appendix 2, in accordance with Article 32 of the GDPR;
 - e) maintain a written record of the processing activities carried out on behalf of the Controller, in accordance with Article 30(2) of the GDPR;
 - f) assist the Controller as set out in clauses 8 and 9;
 - g) not use third-party artificial intelligence tools to process the personal data contained in the Controller's portfolios.
-

6. Security

6.1. ARST Data shall implement the measures set out in Appendix 2 and shall review them periodically in light of the state of the art, the costs of implementation and the risks of the processing.

6.2. ARST Data may modify those measures provided that it does not reduce the overall level of security. It shall inform the Controller of any substantial changes.

7. Sub-processors

7.1. **General authorisation.** The Controller grants ARST Data a general authorisation to engage the sub-processors listed in Appendix 3.

7.2. **Changes.** ARST Data shall inform the Controller, at least 30 days in advance, of any addition or replacement of a sub-processor, by email to the data protection contact address given in the Service Order. The Controller may object in writing, giving reasons relating to data protection, within that period. If the objection is not resolved in good faith within 30 days, the Controller may terminate, without penalty, the part of the Service Order that cannot be provided without the new sub-processor, with a refund of the prepaid price corresponding to the period for which the Services are not provided.

7.3. **Conditions.** ARST Data shall impose on each sub-processor, by contract, data protection obligations substantially equivalent to those of this Agreement, in particular as regards security.

ARST Data shall remain fully liable to the Controller for the performance of the sub-processor's obligations.

7.4. Urgency. If a sub-processor has to be replaced urgently for reasons beyond ARST Data's control, for example because it ceases its activity or following a security incident, ARST Data may do so and shall inform the Controller without delay, and clause 7.2 shall apply from then on.

8. Rights of data subjects

8.1. If a data subject sends ARST Data a request to exercise their rights in respect of data processed on behalf of the Controller, ARST Data shall forward it to the Controller within five Business Days and shall not respond directly to the data subject unless instructed to do so by the Controller.

8.2. ARST Data shall assist the Controller, by appropriate technical and organisational measures and insofar as this is possible, so that the Controller can respond to requests for access, rectification, erasure, restriction, portability and objection. The Platform allows the Controller to view, modify, download and delete the portfolios it has uploaded.

9. Assistance with security, breaches and impact assessments

9.1. **Security breaches.** ARST Data shall notify the Controller without undue delay and, in any event, within 48 hours after becoming aware of it, of any personal data breach affecting the personal data processed on its behalf. The notification shall include, to the extent available: (a) the nature of the breach, the categories and approximate number of data subjects and of records concerned; (b) a point of contact; (c) the likely consequences; and (d) the measures taken or proposed to address the breach and mitigate its effects. Where it is not possible to provide all the information at the same time, it shall be provided in phases and without further undue delay.

9.2. It is for the Controller to notify the breach to the supervisory authority and, where applicable, to communicate it to the data subjects. ARST Data shall not do so on its own initiative unless instructed by the Controller or required by law.

9.3. **Impact assessments and consultations.** ARST Data shall provide the Controller with the information reasonably necessary to carry out data protection impact assessments and, where applicable, prior consultations with the supervisory authority, taking into account the nature of the processing and the information available to it.

10. International transfers

10.1. ARST Data processes and stores the Controller's personal data in the European Union.

10.2. ARST Data shall not transfer those data to a third country or an international organisation, nor allow access to them from there, unless: (a) the relevant sub-processor is listed in Appendix 3 or is added in accordance with clause 7; and (b) the transfer is covered by a European Commission adequacy decision or by appropriate safeguards under Article 46 of the GDPR, such as the standard contractual clauses approved by Commission Implementing Decision (EU) 2021/914, together with any supplementary measures that may be appropriate.

11. Audit and information

11.1. ARST Data shall make available to the Controller all information necessary to demonstrate compliance with this Agreement, in particular the up-to-date description of the security measures, the list of sub-processors and, where they exist, third-party reports or certifications.

11.2. The Controller, directly or through an independent auditor bound by confidentiality who is not a competitor of ARST Data, may carry out audits and inspections of compliance with this Agreement, on 30 days' prior notice, at most once every twelve months unless there is a security breach or a request from a supervisory authority, during business hours, with a scope defined in writing and without access to the data of other customers or to the trade secrets of ARST Data. The audit shall preferably be carried out on a documentary basis and remotely.

11.3. Each Party shall bear its own costs. Time spent by ARST Data in excess of one Business Day per audit shall be invoiced at the day rate in the Service Order, unless the audit reveals a material breach by ARST Data.

11.4. The foregoing is without prejudice to the powers of the supervisory authorities and, where applicable, to those provided for in Schedule IV of the Master Agreement.

12. Duration and end of the processing

12.1. This Agreement shall remain in force for as long as ARST Data processes personal data on behalf of the Controller.

12.2. Upon termination of the provision of the Services, ARST Data shall, at the Controller's choice notified in writing, return the personal data or delete them, in accordance with the time limits in

clause 20 of the Master Agreement: download available for 30 days, deletion from the production systems within the following 30 days, and removal of the backup copies in their ordinary cycle, which does not exceed a further 30 days. If the Controller does not choose, ARST Data shall delete the data upon expiry of the download period. At the Controller's request, ARST Data shall certify the deletion in writing.

12.3. ARST Data may retain the data, duly blocked, only where Union or Member State law requires it to retain them, and for the period that law provides.

12.4. The Controller may also delete at any time, from the Platform, the portfolios it has uploaded. Their removal from the backup copies shall follow the ordinary cycle indicated above.

13. Liability

13.1. Each Party shall be liable for the damage it causes by breaching this Agreement or the GDPR in accordance with Article 82 of the GDPR.

13.2. As between the Parties, the limits in clause 17 of the Master Agreement shall apply, with the increased limit that it provides for this Agreement. Those limits do not affect the rights of data subjects against either of the Parties.

14. Governing law and jurisdiction

This Agreement is governed by Spanish law and by the GDPR. Disputes shall be resolved in accordance with clause 28 of the Master Agreement or, failing that, of the [General Terms of Use and Sale of arstdata.com](#).

Appendix 1. Description of the processing

Item	Description
Purpose	To estimate the current and future value of the vehicles in the Controller's portfolio, to calculate portfolio risk indicators (ratio of outstanding debt to value, shortfalls, alerts), to back-test the estimates against the Controller's sale prices and to deliver the Outputs to it.

Item	Description
Nature of the processing	Receipt, storage, consultation, calculation, retention, download and deletion, by automated processes and, occasionally, human intervention for support and quality control.
Categories of data subjects	Customers of the Controller who are natural persons, including sole traders, lessees or borrowers under the portfolio contracts.
Categories of personal data	Pseudonymised contract reference; country; make, model, trim, fuel, power, date of first registration and mileage of the vehicle; contract terms (start and end dates, contractual mileage, contractual residual value, outstanding debt); and, if the Controller provides them, sale prices and dates of vehicles already returned. Only if the Service Order authorises it: registration plate or VIN.
Special categories	None. The Controller shall not provide special categories of data or data relating to criminal convictions and offences.
Duration	That of the Service Order, plus the return and deletion periods in clause 12.
Frequency	Continuous while the Service is in force.

Appendix 2. Technical and organisational measures

Access control

Access to the Platform by means of personal credentials; passwords stored using a strong hashing function.

Individual API keys, revocable and associated with the Customer's account.

Administrative access to the servers restricted to authorised personnel, by means of cryptographic keys and a second authentication factor on the administration panels.

Logical separation of each customer's data; each user can access only the portfolios of their own account.

Confidentiality in transit and at rest

Communications encrypted by means of HTTPS with TLS 1.2 or higher.

Communication between servers over a private network.

Encrypted backup copies.

Integrity and availability

Daily and weekly backup copies, retained for 7 and 30 days respectively, stored outside the production server, within the European Union.

Automatic availability monitoring every five minutes from an independent server, with alerts.

Firewalls and public exposure limited to the necessary services; regular security updates.

Minimisation and pseudonymisation

Automatic rejection of files with columns identified as direct identifiers.

No use of the Controller's data for own purposes or to train other customers' models.

ARST Data does not use third-party artificial intelligence tools to process the personal data contained in the Controller's portfolios; maintenance tasks using such tools are carried out on test accounts only.

Logging and traceability

Logging of account security events (registrations, logins, failed logins, password changes).

Logging of the queries and of the consumption associated with each account.

Organisation

Duty of confidentiality of all persons with access.

Incident management and personal data breach notification procedure in accordance with clause 9.

Restoration test of the backup copies at least once a year.

Deletion at the end of the Service in accordance with clause 12.

Appendix 3. Authorised sub-processors

List of sub-processors: available to customers and prospective customers on request at info@arstdata.com. All sub-processors process the data within the European Economic Area and are bound by obligations equivalent to those of this agreement.