NLdigital

Version: 2026

Data Processing Agreement. Any2info B.V.

Part 1. Data Pro Statement

Part 2. Standard clauses for data processing

Part 1: Data Pro Statement

1. This Data Pro Statement has been prepared by the following data processor:

   • Any2info B.V., Westhoven 7, 6042 NV Roermond, the Netherlands.

   For questions regarding this Data Pro Statement or data protection, please contact: E-mail: support@any2info.com. Tel. no.: ++31 6 27 23 16 00.

2. This Data Pro Statement has been effective since April 2019.

   We regularly update the security measures described in this Data Pro Statement to ensure that we remain prepared and up to date regarding data protection. We will inform you of new versions through our regular communication channels.

3. This Data Pro Statement applies to the following products and services provided by the data processor:

   Application(s):

   A specific version of the data processor's online software that is accessible via one or more designated servers, a website or another designated IP address pursuant to the data processor's Software & Services Agreement Terms and Conditions.

   Services:

   Activities performed by employees of the data processor in the areas of software development, installation, consultancy and support pursuant to the data processor's Software & Services Agreement Terms and Conditions.

4. Description of the product/service

   App Studio Application:

   A web application for designing and building functional mobile applications (Apps) that can be accessed on a mobile device and/or desktop computer. Its main functions are entering, processing and displaying data for use by the Customer's data subject(s).

   Data Studio Application:

   An application for accessing one or more of the Customer's databases and configuring data into standardised messages through which data selected and released by the Customer is exchanged with the Platform Application at a specified time and/or subject to specified conditions.

AI Studio Application:

An application for designing, configuring and deploying AI Agents that use external Large Language Models (LLMs). These AI Agents can be integrated as functional components within App Studio or Data Studio, or as standalone chat functionality. Based on predefined rules, prompts or interactions, the AI Agents automatically process data, including analysing, interpreting or generating information using data provided by or on behalf of the Customer. Processing takes place exclusively on the basis of predefined access rights and configurations established by the Customer.

5. Intended use

The aforementioned products have been designed and configured to support business processes and business information through the entry, processing and display of data on mobile devices and/or desktop computers.

The nature, content and layout of the application(s), as well as the method and frequency of data exchanges with the Customer's databases, are determined by the Customer.

The applications are managed by one or more administrators appointed by the Customer. Users of the application(s) receive personal access rights following nomination and approval by the Customer.

The Personal Data recorded by the data processor in its applications consists of data received from the Customer for the creation of personal access rights for the designated data subject(s).

The products are not designed to process special categories of Personal Data or data relating to criminal convictions and offences.

The data processor's applications are installed under the Customer's responsibility on infrastructure and at locations made available by the Customer and/or a third party appointed by the Customer. The Customer and/or a third party appointed by the Customer is responsible for implementing and maintaining appropriate technical and organisational security measures for this infrastructure and these locations.

Insofar as the Customer uses AI Agents that independently interpret data or generate decisions, the Customer is responsible for implementing appropriate safeguards in accordance with the AI Act, including oversight by a human user (through a human-in-the-loop, human-on-the-loop or human-in-command approach).

6. The data processor has applied privacy by design when designing the product/service in the following ways:

- The products can be used to configure customised mobile applications that support business processes and business information.
- The applications include data minimisation, encryption and safeguards against external breaches and/or unauthorised access. Privacy-friendly user settings are also implemented by default.

- The applications contain only the fields required for their functional operation. All fields are optional and are added at the Customer's request.
- Customers determine the nature and content of the Personal Data, including any attachments selected by them, that is exchanged with the data processor's applications. Customers can modify and delete this data and these documents.
- The data processor does not verify the data and will access it only at the Customer's request, for example when this is necessary to respond to a helpdesk enquiry.
- AI Studio has been developed in accordance with the principles of data minimisation, explainability and zero data retention. Data provided by the Customer is processed only temporarily for the purpose of functional AI interaction and is not used to train models. Unless otherwise agreed, this data is neither stored nor reused.

7. The data processor uses the Standard Data Processing Clauses, which can be found in Appendix 2 to the Agreement.

8. The data processor processes its Customers' Personal Data within the EU/EEA. The countries in the European Economic Area (EEA) also include Norway, Liechtenstein and Iceland.

9. If Personal Data made available by the Customer in the applications is processed outside the EU/EEA by or on behalf of the Customer, the Customer will ensure that an appropriate level of protection applies.

10. The data processor may use third-party sub-processors to process Personal Data within its applications. If this is necessary, the Customer will be informed and will be asked to provide its consent. Insofar as AI Agents use external AI models or services through API integrations, these parties, such as LLM providers, are regarded as sub-processors. The current list of AI sub-processors will be provided to the Customer upon request. If the Customer supplies its own API key, responsibility for the relevant processor rests with the Customer.

11. If Personal Data originating from the Customer's sub-processors is exchanged through the data processor's applications, the Customer is responsible for implementing measures and/or entering into agreements with these sub-processors to ensure an appropriate level of protection. The Customer is also responsible for providing information to the data subject(s).

12. The data processor's applications support the option for the Customer and/or its data subject(s) to submit a request to modify and/or delete Personal Data.

13. Following termination of the Agreement with a Customer, the data processor will, in principle, delete the Personal Data it processes for the Customer within three months, in such a manner that the data can no longer be used and is no longer accessible ("rendered inaccessible").

Security Policy

14. The data processor will implement appropriate technical and organisational measures to secure its product or service, safeguard the confidentiality, integrity and availability of Personal Data, and protect the rights of data subject(s). When implementing these measures, the data processor will take into account the state of the art, implementation costs, and the nature, scope, context and purposes of the processing. These measures include:

    - Appropriate access security provisions to ensure that Personal Data is accessible only to authorised users.
    - An appropriate and up-to-date mechanism for detecting and preventing malicious software, including but not limited to computer viruses.
    - The use of secure network connections.

    The Customer and/or a third party appointed by the Customer is responsible for implementing appropriate technical and organisational measures to secure all Personal Data made available by the Customer in the data processor's applications. These measures include:

    - The use of secure networks, equipment, devices and connections.
    - Appropriate access security provisions to ensure that Personal Data is accessible only to authorised users.
    - An appropriate and up-to-date mechanism for detecting and preventing malicious software, including but not limited to computer viruses.
    - Keeping operating systems and security software on networks, equipment and/or devices up to date.
    - Creating timely and frequent backups to prevent the loss of Personal Data.
    - Storing backups at a physically separate location that is protected against fire and other hazards.

Specific Use of AI Studio

15. The data processor makes AI Studio available as a technical tool that enables the Customer to deploy AI functionality in a controlled manner within the limits of the GDPR and the AI Act. The Customer is responsible for:

    - Classifying AI applications under the AI Act, including determining whether they qualify as high-risk AI systems.
    - Informing data subjects about the use of AI in accordance with applicable transparency obligations.
    - Correctly implementing human oversight mechanisms.
    - Preventing automated decision-making without a lawful basis as referred to in Article 22 of the GDPR.

The data processor provides support in the form of:

- Logging configurations and interactions with AI Agents.
- Technical documentation regarding the models used.
- Configurable options for explainability and the retention policy applicable to generated output.

Data Breach Protocol

16. In the event that an incident nevertheless occurs, the data processor applies the following data breach protocol to ensure that the Customer is informed:

    - If the data processor discovers a data breach within its organisation, it will inform the Customer as soon as possible.
    - The data processor provides monitoring tools for identifying potential security incidents.
    - The data processor will provide as much relevant information as possible, including a description of the incident, the nature of the breach, the nature of the Personal Data and/or the categories of affected data subjects, an estimate of the number of affected data subjects, the databases that may be affected and an indication of when the incident occurred.
    - The data processor will inform the Customer of the possible consequences.
    - The data processor will inform the Customer of the measures taken by the data processor.
    - The data processor will inform the Customer of the measures to be taken by the Customer.
    - The data processor will not independently notify the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) or the data subjects. The decision whether or not to submit a notification remains the Customer's responsibility.
    - At the Customer's request, the data processor will support the Customer during the notification process.
    - Questions can be submitted by the Customer to support@any2info.com.
    - The data processor will continue to keep the Customer informed of further developments.

Part 2: Standard Clauses for Data Processing

Version: March 2025

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in their capacity as an ICT supplier, processes Personal Data on behalf of their Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: statement issued by Data Processor in which they provide information such as the intended use of their products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor as required under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing their products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.

2.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of

significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating their reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written agreed upon instructions provided by Client by Data Processor.

2.4 Client or their customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.

2.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data, and shall not make any decisions on the use of the Personal Data and other such matters.

2.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 Client shall guarantee Data Processor that they act in accordance with the GDPR, that they provide a high level of protection for their systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1 Data Processor shall implement the technical and organisational security measures set out in their Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of their products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 Data Processor seeks to ensure that the security measures they shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.5 Data Processor shall be entitled to adjust the security measures they have implemented if to their discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments they chooses to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honour such requests to adjust their security measures. If Data Processor makes any adjustments to their security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing. .

Article 4. Data breaches

4.1 Data Processor does not guarantee that their security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, they shall notify Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.2 It is up to the Controller (the Client or their customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or their customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet their breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.4 If Data Processor incurs any reasonable costs in doing so, they are entitled invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are

confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that their employees comply with the requirements described in this article.

Article 6. Term and termination

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data they currently store and which they have obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, they shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of their statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

7.1 Where possible, Data Processor shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, they shall refer the Data Subject to Client where possible.

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.3 Data Processor will lend their cooperation to Client's requests for the deletion of personal data insofar as Client cannot carry this out themself.

7.4 Data Processor shall be able to demonstrate their compliance with their requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.5 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at their own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with their obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to their discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures they have implemented.

7.6 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to their discretion such are appropriate, taking into account the processing risks associated with their product or service, the state of the art, the costs of implementation, the market in which they operate, and the intended use of the product or service.

7.7 Data Processor shall be entitled to invoice Client for any costs they incur in implementing the measures referred to in this article.

Article 8. Sub-processors

8.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (sub-processors) to help them process the Personal Data, and if so, which third parties.

8.2 Client hereby authorises Data Processor to hire other sub-processors to meet their obligations under the Agreement.

8.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes . Data Processor shall ensure that any third parties they hire shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.