AllesOnline

Version: 1.0

Data Processing Agreement

Alles Online B.V.

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard Clauses for Data Processing

NLdigital version March 2025

This document is an English translation, provided for convenience only, of the Dutch document 'Verwerkersovereenkomst Alles Online B.V.' (version 1.0, July 2026). In the event of any conflict or difference in interpretation between the Dutch version and this English translation, the Dutch version prevails.

Part 1: Data Pro Statement

This Data Pro Statement, together with the Standard Clauses for Data Processing, constitutes the data processing agreement for the product or service of the company that has drawn up this Data Pro Statement.

General information

1. **This Data Pro Statement has been drawn up by the following data processor:**
   Alles Online B.V., Jan van der Heydenstraat 18, 2665 JA Bleiswijk, the Netherlands. Chamber of Commerce (KvK) 55765939, VAT NL851852105B01. For questions about this Data Pro Statement or about data protection, the contact person for privacy & security is: Stefan Grevelink, stefan@allesonline.nl, phone +31 (0)85 003 0302.

2. This Data Pro Statement applies from 8 June 2026 (version 1.0).
   We regularly update this Data Pro Statement and the security measures described in it in order to remain prepared and up to date with regard to data protection at all times. We will keep you informed of new versions through our normal channels.

3. This Data Pro Statement applies to the following products and services of the data processor:
   Cluster 1: custom web application and software development and application management (CMS websites, web applications, portals and web shops, including maintenance, consultancy and support); and Cluster 2: managed web application hosting and infrastructure management. The Agreement between the Data Processor and the client specifies which products/services have been purchased.

4. Description of product(s)/service(s): AllesOnline develops and manages custom-built websites and web applications, largely based on its own content management system (Cluster 1: software development, maintenance, application management and support), and hosts and manages these web applications on a managed Kubernetes environment, including storage, databases, e-mail handling and back-ups (Cluster 2).

5. Only in specific custom applications has account been taken of the processing of special categories of personal data (Article 9 GDPR), data relating to criminal convictions and offences (Article 10 GDPR) or government-issued personal identification numbers. Where a client processes such data in such a custom application, AllesOnline configures that application accordingly with appropriate additional security measures, separate arrangements are made in that respect, and the client is supported in any DPIA.

6. **Privacy by design/privacy by default**
   AllesOnline facilitates privacy by design/by default through, among other things, data minimisation (forms contain only the necessary fields), encrypted storage of passwords, the option of two-factor authentication, an authorisation model with roles and permissions (default 'no access'), deletion functions and configurable retention periods, and separate development, acceptance and production environments. Final responsibility for privacy by design/by default lies with the client; AllesOnline provides advice in this respect.

7. The Data Processor uses the Standard Clauses for Data Processing, which can be found as an annex to the Agreement.

8. The Data Processor in principle processes the personal data of its clients within the EU/EEA. For a limited number of supporting services, such as error monitoring and bot/spam protection, data is transferred to the United States; the Data Processor has safeguarded an adequate level of protection in the following way: the Data Processor has concluded Standard Contractual Clauses (SCCs) with the relevant sub-processors in the United States and/or these sub-processors are certified under the EU-US Data Privacy Framework, combined with data minimisation. This concerns: Sentry (error monitoring; used by default) and the Google services reCAPTCHA (bot protection for forms) and Maps (map display), which are used depending on the assignment via a key held by the Data Processor. In addition, a few transactional e-mail domains (Mailgun) are still hosted in the US region and are being migrated to the EU region; in the meantime, the same safeguards (SCCs/DPF) apply to this transfer.

9. **The Data Processor uses the following sub-processors:**
   DigitalOcean (hosting, storage, databases; Amsterdam region, EU); Mach3Builders BV (SaaS CMS and hosting for client websites; Netherlands, EU); TransIP (domain registration/DNS and web hosting; NL, EU); Mailgun (transactional e-mail; primarily EU region, a few remaining domains still in the US region, being migrated to the EU); SimpleBackups/SimpleStorage (database back-ups; EU, Stockholm, Sweden); Microsoft 365 (Exchange/Teams; supporting e-mail and support communication in which personal data of data subjects may incidentally be processed; EU Data Boundary); Sentry (error monitoring; US, DPF/SCCs; used by default); Google reCAPTCHA and Google Maps (bot protection and map display respectively; US, DPF/SCCs; depending on the assignment, via a key held by the Data Processor). Services chosen or supplied by the client itself (such as a payment provider or the client's own OpenAI key) are direct processors of the client.

10. **The Data Processor supports the client with requests from data subjects in the following way:**
    The Data Processor does not take independent decisions on requests from data subjects, but supports the client in handling them. Depending on the application, the client can view, export, modify or delete data itself; in addition, a request for export, modification or deletion can be submitted via the helpdesk. Any additional costs will be communicated in advance, that is, before the work is carried out.,

11. **The Data Processor will cooperate with Data Protection Impact Assessments (DPIA) in the following way:**
    If the client is required to carry out a Data Protection Impact Assessment (DPIA), the Data Processor will cooperate following a reasonable request to that effect. Any additional costs will be communicated in advance, that is, before the work is carried out.

12. After termination of the Agreement with a client, the Data Processor will in principle delete the personal data it processes for the client within 3 months, in such a way that the data can no longer be used and is no longer accessible (rendered inaccessible). Deletion also includes the back-ups, in accordance with the regular back-up cycle.

13. Return of personal data after termination of the Agreement: at the client's request, the Data Processor will return the personal data before deletion, in a common, machine-readable format (for example a database export). Further arrangements will be made on this upon termination; any costs will be communicated in advance, before the work is carried out.

Security policy

14. **The Data Processor has taken the following security measures to protect its product or service.**
    The security measures taken are summarised below; the full details are laid down in AllesOnline's internal information security policy, which is available to the client on request:
    - Personal data is generally not pseudonymised.
    - Passwords are stored encrypted (hashed); data transmission is encrypted via TLS/SSL in accordance with the guidelines of the Dutch National Cyber Security Centre (NCSC).
    - Confidentiality, integrity, availability and resilience are safeguarded by access management with roles and permissions (least privilege) and two-factor authentication, strict separation of environments (development, testing, acceptance, production) and logical separation of client data, 24/7 logging and monitoring, protection against malware, patch and vulnerability management, including periodic vulnerability scans (Greenbone) and, for environments containing sensitive data, automated CVE scanning, secure development with version control and testing, and a duty of confidentiality for employees.
    - In the event of an incident, availability and access are restored in a timely manner through back-ups with restore capability and, where technically applicable, redundantly implemented infrastructure components, supported by 24/7 monitoring and an escalation procedure.
15. The Data Processor maintains an internal information security policy based on the principles of an Information Security Management System (ISMS), in accordance with the guidelines of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and the NCSC.

16. The Data Processor does not currently hold a formal privacy verification or security certification. AllesOnline has submitted an application for the Data Pro Verified mark (assessment and monitoring by SCOPE Europe). At the time of publication of this Data Pro Statement, the application was still being processed.

Data breach protocol

17. **In the event that something does go wrong, the Data Processor applies the following data breach protocol to ensure that the client is aware of incidents:**
    Potential security incidents are detected via 24/7 logging and monitoring and via reports to the helpdesk. Incidents are reported internally and recorded in the data breach register. If the Data Processor discovers a personal data breach, it will inform the client without undue delay via the known contact person, providing as much relevant information as possible: a description and the nature of the incident, the categories of personal data and of data subjects concerned, the estimated number of data subjects, the time of the incident, the possible consequences, and the measures taken and to be taken. The Data Processor does not itself notify the Dutch Data Protection Authority or the data subjects; that is the responsibility of the controller. The Data Processor will provide support in this respect if desired.

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 belonging to this Agreement, such as any applicable general terms and conditions.

Article 1. Definitions

The following terms have the following meanings in these Standard Clauses for Data Processing, in the Data Pro Statement and in the agreement:

1.1 **Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP):** the supervisory authority, as referred to in Article 4(21) of the GDPR.
1.2 **GDPR:** the General Data Protection Regulation.
1.3 **Data Processor:** the party which, in its capacity as an ICT supplier, processes Personal Data as a processor on behalf of its Client as part of the performance of the Agreement.
1.4 **Data Pro Statement:** a statement issued by the Data Processor in which it provides information on, among other things, the intended use of its product or service, the security measures implemented, sub-processors, data breaches, certifications and the handling of the rights of Data Subjects.
1.5 **Data Subject:** an identified or identifiable natural person.
1.6 **Client:** the party on whose behalf the Data Processor processes personal data. The Client may be either a controller or another processor.
1.7 **Agreement:** the agreement in force between the Client and the Data Processor, on the basis of which the ICT supplier provides services and/or products to the Client, of which the data processing agreement forms part.
1.8 **Personal Data:** any information relating to an identified or identifiable natural person, as referred to in Article 4(1) of the GDPR, which the Data Processor processes in the performance of its obligations under the Agreement.
1.9 **Data Processing Agreement:** these Standard Clauses for Data Processing, which, together with the Data Processor's Data Pro Statement (or similar information), constitute the data processing agreement within the meaning of Article 28(3) of the GDPR.

Article 2. General provisions

2.1 These Standard Clauses for Data Processing apply to all processing of Personal Data carried out by the Data Processor in the context of providing its products and services, and to all Agreements and offers. The applicability of the Client's data processing agreements is expressly rejected.

2.2 The Data Pro Statement, and in particular the security measures included in it, may be adapted by the Data Processor from time to time to reflect changing circumstances. The Data Processor will notify the Client of significant changes. If the Client cannot reasonably agree to the changes, the Client is entitled to terminate the data processing agreement in writing, stating its reasons, within 30 days of being notified of the changes.

2.3 The Data Processor processes the Personal Data on behalf of and on the instructions of the Client, in accordance with the written instructions of the Client agreed with the Data Processor.

2.4 The Client, or its customer, is the controller within the meaning of the GDPR, has control over the processing of the Personal Data and has determined the purpose of and the means for the processing of the Personal Data.

2.5 The Data Processor is a processor within the meaning of the GDPR and therefore has no control over the purpose of and the means for the processing of the Personal Data, and consequently does not take decisions on, among other things, the use of the Personal Data.

2.6 The Data Processor gives effect to the GDPR as laid down in these Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to the Client to assess, on the basis of this information, whether the Data Processor provides sufficient guarantees with regard to the implementation of appropriate technical and organisational measures to ensure that the processing meets the requirements of the GDPR and that the protection of the rights of Data Subjects is sufficiently safeguarded.

2.7 The Client guarantees to the Data Processor that it acts in accordance with the GDPR, that it adequately secures its systems and infrastructure at all times, and that the content, use and/or processing of the Personal Data are not unlawful and do not infringe any rights of a third party.

2.8 An administrative fine imposed on the Client by the Dutch Data Protection Authority cannot be recovered from the Data Processor.

Article 3. Security

3.1 The Data Processor implements the technical and organisational security measures as described in its Data Pro Statement. In implementing the technical and organisational security measures, the Data Processor has taken into account the state of the art, the costs of implementing the security measures, the nature, scope and context of the processing operations, the purposes and intended use of its products and services, the processing risks and the risks, varying in likelihood and severity, to the rights and freedoms of Data Subjects that it could expect in view of the intended use of its products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the Data Processor's product or service is not set up for the processing of special categories of Personal Data, data relating to criminal convictions and offences, or government-issued personal identification numbers.

3.3 The Data Processor endeavours to ensure that the security measures it implements are appropriate for the use of the product or service as intended by the Data Processor.

3.4 In the Client's opinion, the security measures described provide a level of security that is appropriate to the risk involved in the processing of the Personal Data it uses or provides, taking into account the factors referred to in Article 3.1.

3.5 The Data Processor may make changes to the security measures implemented if, in its opinion, this is necessary in order to continue to provide an appropriate level of security. The Data Processor will record significant changes, for example in an amended Data Pro Statement, and will notify the Client of those changes where relevant.

3.6 The Client may request the Data Processor to implement further security measures. The Data Processor is not obliged to make changes to its security measures in response to such a request. The Data Processor may charge the Client for the costs associated with changes made at the Client's request. The Data Processor is not obliged to actually implement the changed security measures requested by the Client until the Parties have agreed those measures in writing and signed off on them.

Article 4. Personal data breaches

4.1 The Data Processor does not guarantee that the security measures will be effective under all circumstances. If the Data Processor discovers a personal data breach (as referred to in Article 4(12) of the GDPR), it will inform the Client without undue delay. The Data Pro Statement (under the data breach protocol) sets out the manner in which the Data Processor informs the Client about personal data breaches.

4.2 It is up to the controller (the Client, or its customer) to assess whether the personal data breach about which the Data Processor has provided information must be reported to the Dutch Data Protection Authority or the Data Subject. Reporting personal data breaches that must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR remains at all times the responsibility of the controller (the Client or its customer). The Data Processor is not obliged to report personal data breaches to the Dutch Data Protection Authority and/or the Data Subject.

4.3 The Data Processor will, where necessary, provide further information about the personal data breach and will cooperate in providing the Client with the information needed for a notification as referred to in Articles 33 and 34 of the GDPR.

4.4 The Data Processor may charge the Client for the reasonable costs it incurs in this context, at its rates applicable at that time.

Article 5. Confidentiality

5.1 The Data Processor ensures that the persons who process Personal Data under its responsibility are subject to a duty of confidentiality.

5.2 The Data Processor is entitled to provide the Personal Data to third parties if and insofar as such provision is necessary pursuant to a court decision, a statutory provision or a lawfully issued order from a government authority.

5.3 All access and/or identification codes, certificates and information regarding access and/or password policies provided by the Data Processor to the Client, and all information provided by the Data Processor to the Client that gives substance to the technical and organisational security measures included in the Data Pro Statement, are confidential and will be treated as such by the Client and will only be disclosed to authorised employees of the Client. The Client will ensure that its employees comply with the obligations set out in this article.

Article 6. Term and termination

6.1 This data processing agreement forms part of the Agreement and of any new or further agreement arising from it, enters into force at the moment the Agreement is concluded, and is concluded for an indefinite period.

6.2 This data processing agreement ends by operation of law upon termination of the Agreement or of any new or further agreement between the parties.

6.3 In the event of termination of the data processing agreement, the Data Processor will delete all Personal Data it holds that it has received from the Client, within the period laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and is no longer accessible (rendered inaccessible), or, if so agreed, will return the Personal Data to the Client in a machine-readable format.

6.4 The Data Processor may charge the Client for any costs it incurs in the context of Article 6.3. Further arrangements on this may be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if a statutory provision prevents the Data Processor from deleting or returning the Personal Data in whole or in part. In such a case, the Data Processor will only continue to process the Personal Data insofar as necessary under its statutory obligations. The provisions of Article 6.3 also do not apply if the Data Processor is a controller within the meaning of the GDPR with regard to the Personal Data.

Article 7. Rights of Data Subjects, Data Protection Impact Assessment (DPIA) and audit rights

7.1 The Data Processor will, where possible, cooperate with reasonable requests from the Client relating to rights of Data Subjects invoked by Data Subjects vis-a-vis the Client. If the Data Processor is approached directly by a Data Subject, it will, where possible, refer the Data Subject to the Client.

7.2 If the Client is required to do so, the Data Processor will, following a reasonable request to that effect, cooperate with a data protection impact assessment (DPIA) or a subsequent prior consultation as referred to in Articles 35 and 36 of the GDPR.

7.3 The Data Processor will cooperate with requests from the Client to delete personal data insofar as the Client cannot carry out such deletion itself.

7.4 The Data Processor may, if it so wishes, demonstrate compliance with its obligations under the data processing agreement by means of a valid Data Pro Certificate or an at least equivalent certificate or audit report (Third Party Memorandum) issued by an independent expert, if it has such a certificate or audit report at its disposal.

7.5 In addition, at the Client's request, the Data Processor will make available all further information reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If the Client nevertheless has grounds to believe that the processing of Personal Data is not taking place in accordance with the data processing agreement, the Client may, at its own expense and no more than once a year, have an audit carried out by an independent, certified, external expert who has demonstrable experience with the type of processing operations carried out under the Agreement. The audit will be limited to verifying compliance with the arrangements regarding the processing of the Personal Data as laid down in this Data Processing Agreement. The expert will be subject to a duty of confidentiality with regard to his or her findings and will only report to the Client those matters that constitute a failure

by the Data Processor to comply with its obligations under this data processing agreement. The expert will provide the Data Processor with a copy of his or her report. The Data Processor may refuse an audit or an instruction from the expert if, in its opinion, it is contrary to the GDPR or other legislation or constitutes an unacceptable breach of the security measures it has implemented.

7.6 The parties will consult on the findings of the report as soon as possible. The parties will implement the improvement measures proposed in the report insofar as this can reasonably be expected of them. The Data Processor will implement the proposed improvement measures insofar as it considers them appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.

7.7 The Data Processor is entitled to charge the Client for the costs it incurs in the context of this article.

Article 8. Sub-processors

8.1 The Data Processor has stated in the Data Pro Statement whether, and if so which, third parties (sub-processors) the Data Processor engages in the processing of the Personal Data.

8.2 The Client authorises the Data Processor to engage other sub-processors in the performance of its obligations under the Agreement.

8.3 The Data Processor will inform the Client of any change in the third parties engaged by the Data Processor, for example by means of an amended Data Pro Statement. The Client has the right to object to such a change by the Data Processor. The Data Processor will ensure that the third parties it engages commit to the same level of security with regard to the protection of the Personal Data as the level of security to which the Data Processor is bound vis-a-vis the Client under the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, together with the Data Pro Statement, form an integral part of the Agreement. All rights and obligations under the Agreement, including any applicable general terms and conditions and/or limitations of liability, therefore also apply to the data processing agreement.