ZYNCEO

DATA PROCESSING AGREEMENT

Version 2.0

Last updated: 10 July 2026

Legal entity	Zyncport B.V.
Trading name	Zynceo
Registered office	Spoorstraat 35b, 8271 RG IJsselmuiden, The Netherlands
Chamber of Commerce	42002045
VAT number	NL869230888B01
Legal and security	team@zynceo.com
Website	www.zynceo.com

GDPR data processing terms for the Zynceo SaaS platform and Shopify app.

Contents

Article 1. Parties
Article 2. Definitions
Article 3. Applicability and order of precedence
Article 4. Roles of the Parties
Article 5. Instructions of the Controller
Article 6. Subject matter, nature and purpose of the Processing
Article 7. Categories of Personal Data
Article 8. Special categories of Personal Data
Article 9. Categories of Data Subjects
Article 10. Obligations of the Controller
Article 11. Obligations of the Processor
Article 12. Confidentiality
Article 13. Technical and organisational measures
Article 14. Rights of Data Subjects
Article 15. Personal Data Breaches
Article 16. Subprocessors
Article 17. International transfers
Article 18. AI providers and AI Processing
Article 19. Autopilot and publication to Shopify
Article 20. Duration, return and deletion
Article 21. Removal of the Shopify app and privacy requests
Article 22. Audits and inspections
Article 23. Assistance with GDPR obligations
Article 24. Requests from public authorities and supervisory authorities
Article 25. Liability
Article 26. Term and termination
Article 27. Amendments
Article 28. Governing law and disputes
ANNEX 1. DETAILS OF THE PROCESSING
ANNEX 2. TECHNICAL AND ORGANISATIONAL MEASURES
ANNEX 3. SUBPROCESSORS
ANNEX 4. CONTACT POINTS

This Data Processing Agreement forms part of the agreement between Zyncport B.V. and the Controller and supplements the General Terms and Conditions and Privacy Policy of Zynceo.

Article 1. Parties

1.1 This Data Processing Agreement is entered into between:

Zyncport B.V.
Trading under the name Zynceo
Spoorstraat 35b
8271 RG IJsselmuiden
The Netherlands
Dutch Chamber of Commerce number: 42002045
VAT identification number: NL869230888B01
Privacy, security and legal enquiries: team@zynceo.com
Support: support@zynceo.com

Website: www.zynceo.com
Hereinafter referred to as the Processor.
And:
The customer, user, organisation or business that creates an Account, enters into a Subscription, connects a Shopify Store or otherwise uses Zynceo.

Hereinafter referred to as the Controller.

1.2 The Processor and the Controller are jointly referred to as the Parties.

1.3 This Data Processing Agreement applies to any Processing in which the Processor processes Personal Data on behalf of the Controller.

1.4 This Data Processing Agreement automatically takes effect as soon as the Processor processes Personal Data on behalf of the Controller.

1.5 The person accepting this Data Processing Agreement on behalf of the Controller declares that they are authorised to represent the Controller.

Article 2. Definitions

2.1 Account

Access to Zynceo linked to a user, organisation, email address, Shopify Store and Subscription.

2.2 Subscription

The free or paid plan under which the Controller uses the Service.

2.3 GDPR

Regulation EU 2016/679, the General Data Protection Regulation.

2.4 Autopilot

The functionality through which Zynceo may automatically generate, assess, schedule, store or publish Content.

2.5 Data Subject

The natural person to whom Personal Data relates.

2.6 Content

All texts, images, prompts, instructions, metadata, drafts, translations, analyses and other information processed through the Service.

2.7 Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data.

2.8 Service

The Zynceo SaaS platform for AI-powered SEO content creation, blog automation, content optimisation, internal linking, translations, image generation and Shopify integrations.

2.9 Personal Data

Any information relating to an identified or identifiable natural person.

2.10 In Writing

Communication by letter, email, support ticket, dashboard notification, Account setting or other electronic communication that can be stored and consulted at a later time.

2.11 Shopify Store

The Shopify environment of the Controller connected to Zynceo.

2.12 Subprocessor

An external party engaged by the Processor to process Personal Data on behalf of the Controller.

2.13 Processing

Any operation performed on Personal Data, including collection, receipt, recording, storage, consultation, analysis, organisation, modification, transmission, publication, restriction, anonymisation, deletion and destruction.

2.14 Processor

Zyncport B.V., to the extent that it processes Personal Data on behalf of the Controller.

2.15 Controller

The party that determines the purposes and means of the Processing.

Article 3. Applicability and order of precedence

3.1 This Data Processing Agreement applies exclusively to Processing activities in which Zyncport B.V. acts as Processor.

3.2 Zyncport B.V. acts as an independent controller for Personal Data it processes for its own purposes.

3.3 This includes Processing for:

a. Account management;
b. contract management;
c. Shopify Billing;
d. administration;
e. fraud prevention;
f. security of its own systems;
g. business communication;
h. support management;
i. compliance with legal obligations.

3.4 The Zynceo Privacy Policy applies to the Processing activities referred to in Article 3.3.

3.5 In the event of a conflict, the following order of precedence applies:

a. mandatory data protection law;
b. this Data Processing Agreement;
c. a separate signed privacy or security agreement;
d. the Zynceo General Terms and Conditions;
e. the Zynceo Privacy Policy;
f. other Zynceo documentation.

3.6 This Data Processing Agreement does not limit any obligation arising directly from the GDPR or other applicable data protection law.

Article 4. Roles of the Parties

4.1 The Controller determines the purposes and means of the Processing within its own business, Shopify Store, website, customer relationships and marketing activities.

4.2 The Controller determines which functionalities are used, which Shopify permissions are granted and which Personal Data is made available through the Service.

4.3 The Processor processes Personal Data solely on behalf of and in accordance with the Controller's Instructions In Writing.

4.4 The Processor does not independently determine the purpose of the Processing covered by this Data Processing Agreement.

4.5 The Processor may make technical and organisational decisions required to carry out the Controller's instructions securely and efficiently.

4.6 Such technical and organisational decisions may not independently change the purpose of the Processing.

Article 5. Instructions of the Controller

5.1 The Processor processes Personal Data solely on the basis of documented instructions from the Controller.

5.2 Documented instructions include:

a. this Data Processing Agreement;
b. the General Terms and Conditions;
c. Account settings;
d. granted Shopify permissions;
e. activated functionalities;
f. selected publication settings;
g. prompts and Content instructions;
h. support requests submitted In Writing;
i. additional agreements made In Writing between the Parties.

5.3 The Controller is responsible for the accuracy, completeness and lawfulness of its instructions.

5.4 The Processor may refuse, suspend or restrict an instruction where it:

a. breaches the GDPR or other law;
b. infringes the rights of Data Subjects;
c. breaches Shopify rules;
d. breaches the terms of an AI provider;
e. creates a security risk;
f. is not reasonably technically feasible;
g. may cause damage to the Service, other users or Third Parties.

5.5 Where the Processor believes that an instruction breaches data protection law, the Processor will inform the Controller without undue delay.

5.6 The Processor may suspend the relevant instruction until the Parties have amended the instruction or established its lawfulness.

5.7 The Processor is not required to inform the Controller where prohibited by law or a binding order.

Article 6. Subject matter, nature and purpose of the Processing

6.1 The subject matter of the Processing is the processing of Personal Data for the provision, security and support of Zynceo.

6.2 The Processing may include:

a. connecting a Shopify Store;
b. synchronising store content;
c. receiving and storing Content;
d. analysing products, collections, blogs and pages;
e. generating and rewriting Content;
f. creating translations;
g. generating or processing images;
h. generating metadata;
i. performing SEO analyses;
j. creating internal link suggestions;
k. scheduling and publishing Content;
l. operating Autopilot;

m. processing API requests and webhooks;
n. providing technical support;
o. investigating errors and incidents;
p. securing and monitoring the Service;
q. creating and managing backups;
r. deleting, anonymising or exporting data.

6.3 The Processor processes Personal Data solely for:

a. providing the Service;
b. operating selected functionalities;
c. carrying out instructions from the Controller;
d. providing support;
e. securing the Processing;
f. preventing misuse and fraud;
g. resolving technical errors;
h. complying with legal obligations applicable to the Processor.

6.4 The Processor does not use Personal Data covered by this Data Processing Agreement for its own direct marketing purposes.

6.5 The Processor does not sell or rent Personal Data.

Article 7. Categories of Personal Data

7.1 Depending on the selected functionalities, the Processor may process the following categories of Personal Data:

a. names and business contact details of users;
b. business email addresses;
c. company names and job titles;
d. user roles and Account permissions;
e. IP addresses;
f. browser and device information;
g. language, country and time zone;
h. technical identification numbers;
i. Shopify Store ID and Shopify domain;
j. API tokens and webhook information;
k. technical logs and error messages;
l. support messages and attachments;
m. prompts and Content instructions;
n. Content in which the Controller has included Personal Data;
o. Generated Content that may contain Personal Data;
p. product reviews or customer feedback provided by the Controller;
q. other Personal Data entered by the Controller through the Service.

7.2 The standard functionality of Zynceo is not designed to process protected Shopify customer data.

7.3 For its standard functionality, the Processor does not require access to:

a. names of store customers;
b. residential or shipping addresses of store customers;
c. telephone numbers of store customers;
d. payment card information;
e. bank details;
f. checkout information;
g. order history;
h. payment information of store customers.

7.4 Where a future optional functionality requires access to protected Shopify customer data:

a. access will be limited to the minimum data required;
b. the Controller must expressly activate the functionality;

c. Shopify must permit the required access;
d. the Controller will be informed in advance;
e. Annex 1 will be amended where required;
f. the Controller must have a valid legal basis.

7.5 The Processor does not process full payment card information or bank details of the Controller.

7.6 Payments for the public Shopify app are processed through Shopify Billing.

Article 8. Special categories of Personal Data

8.1 The Service is not intended for the Processing of special categories of Personal Data.

8.2 These categories include data concerning:

a. health;
b. racial or ethnic origin;
c. religious or philosophical beliefs;
d. political opinions;
e. trade union membership;
f. genetic data;
g. biometric identification;
h. sexual behaviour or sexual orientation.

8.3 The Service is also not intended for criminal offence data or data relating to children.

8.4 The Controller may not process such data through the Service unless:

a. the Processing is strictly necessary;
b. a valid legal basis and applicable exception exist;
c. appropriate additional security measures have been implemented;
d. the Processor has agreed to the Processing In Writing in advance.

8.5 If the Controller enters such data without prior approval, the Processor may block the Processing or delete the data.

Article 9. Categories of Data Subjects

9.1 The Processing may relate to:

a. users of the Zynceo Account;
b. employees of the Controller;
c. directors of the Controller;
d. freelancers and contractors;
e. business contacts;
f. customers and visitors of the Shopify Store, to the extent their data is included in Content by the Controller;
g. persons included in prompts, Content, reviews, images or support messages.

9.2 The Controller must limit the categories of Data Subjects to those required for the selected functionalities.

Article 10. Obligations of the Controller

10.1 The Controller guarantees that it is authorised to have the Personal Data processed by the Processor.

10.2 The Controller is responsible for:

a. having a valid legal basis for Processing;
b. informing Data Subjects;
c. maintaining an accurate privacy notice;
d. obtaining consent where required;
e. complying with retention periods;
f. handling data protection requests;

g. correctly configuring the Shopify Store;
h. granting appropriate Shopify permissions;
i. securing its own systems and Accounts;
j. removing access for former employees;
k. reviewing prompts and Content;
l. preventing unnecessary Personal Data from being included in AI prompts;
m. reviewing AI output before publication;
n. assessing and reporting Personal Data Breaches to supervisory authorities and Data Subjects;
o. complying with Shopify rules and applicable law.

10.3 The Controller only provides Personal Data that is required for the Service.

10.4 The Controller ensures that its instructions do not infringe the rights of Data Subjects or Third Parties.

10.5 The Controller informs the Processor where the Processing creates special risks.

10.6 The Controller remains responsible for the accuracy and lawfulness of all Content and data made available to the Processor.

Article 11. Obligations of the Processor

11.1 The Processor processes Personal Data only to the extent required to provide the Service and carry out the Controller's instructions.

11.2 The Processor ensures that persons with access to Personal Data:

a. only receive access where required;
b. receive appropriate instructions;
c. are bound by confidentiality;
d. follow appropriate security requirements.

11.3 The Processor implements appropriate technical and organisational measures as described in Annex 2.

11.4 Taking into account the nature of the Processing and the information available, the Processor assists the Controller with:

a. Personal Data security;
b. data protection requests;
c. Personal Data Breaches;
d. data protection impact assessments;
e. prior consultation with supervisory authorities;
f. deletion and export of data.

11.5 The Processor makes available information reasonably required to demonstrate compliance with this Data Processing Agreement.

11.6 Where legally required, the Processor maintains a record of Processing activities carried out on behalf of controllers.

11.7 The Processor applies data protection by design and by default where appropriate.

11.8 The Processor does not collect or process more Personal Data than is reasonably required for the Service.

11.9 The Processor deletes or returns Personal Data following termination in accordance with Article 20.

Article 12. Confidentiality

12.1 The Processor treats Personal Data and confidential information of the Controller as confidential.

12.2 The Processor only grants access to employees, contractors and Subprocessors who require such access.

12.3 Persons with access are bound by contractual, statutory or professional confidentiality obligations.

12.4 Personal Data may be disclosed where required by law.

12.5 The Processor informs the Controller in advance of a mandatory disclosure, unless prohibited by law.

12.6 The confidentiality obligation continues after termination of this Data Processing Agreement.

Article 13. Technical and organisational measures

13.1 The Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks of the Processing.

13.2 When determining the measures, the Processor takes into account:

a. the state of the art;
b. implementation costs;
c. the nature and scope of the Processing;
d. the context and purposes;
e. the likelihood and severity of risks to Data Subjects.

13.3 The measures may include:

a. access management;
b. authentication;
c. encrypted connections;
d. secure storage of passwords and tokens;
e. logging and monitoring;
f. backups and recovery;
g. vulnerability and update management;
h. API and webhook security;
i. separation of duties and restricted administrative rights;
j. procedures for incidents and Personal Data Breaches;
k. supplier and Subprocessor management;
l. continuity and availability.

13.4 The current categories of security measures are described in Annex 2.

13.5 The Processor may change security measures where required due to technical developments, new risks or changes to the Service.

13.6 A change may not materially reduce the overall level of protection.

13.7 No technical or organisational measure can completely eliminate all security risks.

Article 14. Rights of Data Subjects

14.1 The Controller is responsible for handling requests from Data Subjects.

14.2 The Processor assists the Controller where reasonably and technically possible with requests concerning:

a. information;

b. access;
c. rectification;
d. deletion;
e. restriction;
f. data portability;
g. objection;
h. withdrawal of consent;
i. human review of automated decisions.

14.3 Where a Data Subject contacts the Processor directly regarding Processing covered by this Data Processing Agreement:

a. the Processor will not respond substantively without instructions from the Controller;
b. the Processor will refer the Data Subject to the Controller where possible;
c. the Processor will forward the request where reasonable and permitted.

14.4 The Processor may charge reasonable fees for assistance requiring substantial custom work, manual Processing or technical development.

14.5 Fees will not be charged where the assistance forms part of the normal Service or must legally be provided at the Processor's expense.

Article 15. Personal Data Breaches

15.1 The Processor informs the Controller without undue delay after becoming aware of a Personal Data Breach involving Personal Data processed on behalf of the Controller.

15.2 The Processor aims to provide an initial notification within 48 hours after confirming the Personal Data Breach.

15.3 The initial notification may be preliminary where not all information is available.

15.4 The Processor provides, to the extent known and applicable:

a. a description of the Personal Data Breach;
b. the suspected date and duration;
c. the categories of Personal Data;
d. the categories and estimated numbers of affected Data Subjects;
e. the suspected cause;
f. the likely consequences;
g. measures taken and proposed;
h. a contact point for further questions.

15.5 The Processor may provide information in phases where it is not immediately available in full.

15.6 The Processor takes reasonable measures to:

a. stop the Personal Data Breach;
b. limit its consequences;
c. prevent recurrence;
d. preserve relevant information securely.

15.7 The Controller remains responsible for notifications to the Dutch Data Protection Authority and Data Subjects.

15.8 The Processor will not submit a notification on behalf of the Controller unless:

a. the Parties agree this In Writing;
b. the Processor is legally required to do so.

15.9 The Processor maintains an internal record of relevant Personal Data Breaches and security incidents.

Article 16. Subprocessors

16.1 The Controller grants the Processor general authorisation In Writing to engage Subprocessors.

16.2 The Processor may use Subprocessors for:

a. hosting;

b. cloud infrastructure;
c. database management;
d. AI processing;
e. image generation;
f. email processing;
g. logging and monitoring;
h. analytics;
i. support;
j. security;
k. storage and backups;
l. Shopify integrations.

16.3 The Processor maintains an up-to-date list of active Subprocessors.

16.4 Where reasonably available, the list includes:

a. the name of the Subprocessor;
b. the purpose of the Processing;
c. the categories of Personal Data;
d. the Processing location;
e. the applicable transfer mechanism.

16.5 The current list is made available through the legal documentation on www.zynceo.com or on request through team@zynceo.com.

16.6 The Processor informs the Controller at least 14 days in advance of a material addition or replacement of a Subprocessor.

16.7 Notification may take place through:

a. email;
b. dashboard notification;
c. the Subprocessor list;
d. a change log in the Service.

16.8 The Controller may submit a reasoned objection within 14 days where a new Subprocessor creates a demonstrable privacy or security risk.

16.9 The Parties will attempt to find a reasonable solution to a valid objection.

16.10 Where no reasonable solution is available, the Processor may:

a. not provide the relevant functionality;
b. offer an alternative Subprocessor;
c. terminate the affected part of the Service.

16.11 The Controller may terminate the affected part of the Service in that situation.

16.12 Where an urgent change is required due to security, availability, service failure or law, the Processor may immediately replace a Subprocessor and inform the Controller afterwards.

16.13 The Processor imposes obligations on Subprocessors that provide at least an equivalent level of protection for the relevant Processing.

16.14 The Processor remains responsible for the performance of obligations by Subprocessors to the extent required by the GDPR.

Article 17. International transfers

17.1 The Processor processes Personal Data within the European Economic Area where practically feasible.

17.2 Personal Data may be processed outside the European Economic Area where a Subprocessor or technical infrastructure is located outside the European Economic Area.

17.3 For transfers to a country outside the European Economic Area, the Processor uses, where required:

a. an adequacy decision of the European Commission;
b. applicable Standard Contractual Clauses;
c. Binding Corporate Rules;

d. supplementary technical and organisational measures;
e. another legally permitted transfer basis.

17.4 Where Standard Contractual Clauses are used for a transfer from the Processor to a Subprocessor, the processor-to-processor module will be used where applicable.

17.5 Where required, the Processor assesses the risks of the transfer and the laws of the receiving country.

17.6 Where necessary, the Processor implements supplementary measures such as:

a. encryption;
b. pseudonymisation;
c. access restrictions;
d. data minimisation;
e. contractual safeguards.

17.7 Information about international transfers is included in the Subprocessor list or provided on reasonable request.

Article 18. AI providers and AI Processing

18.1 The Processor may engage AI providers for:

a. generating texts;
b. rewriting Content;
c. translations;
d. image generation;
e. SEO analysis;
f. classification;
g. quality control;
h. summaries;
i. internal link suggestions;
j. content planning.

18.2 Prompts, instructions and relevant store content may be transmitted to an AI provider where required for a selected functionality.

18.3 The Processor limits the Personal Data transmitted to what is reasonably necessary.

18.4 The Processor does not authorise AI providers to use identifiable Personal Data or User Content for general model training unless:

a. the Controller has provided separate and explicit consent;
b. this has been clearly communicated in advance;
c. a valid legal basis exists.

18.5 The Processor does not use identifiable Personal Data covered by this Data Processing Agreement for the general training of its own generative AI Models.

18.6 The Processor may use anonymised and aggregated data for statistics, quality measurement, product improvement and capacity planning.

18.7 The Processor may change an AI provider due to:

a. quality;
b. availability;
c. security;
d. cost control;
e. law;
f. technical operation.

18.8 An AI provider processing Personal Data on behalf of the Controller will be treated as a Subprocessor.

18.9 The Controller may not include unnecessary Personal Data, special categories of Personal Data or confidential customer data in prompts.

Article 19. Autopilot and publication to Shopify

19.1 Where the Controller enables Autopilot, the Processor may process data to automatically generate, assess, schedule, store and publish Content.

19.2 The Controller determines:

a. whether Autopilot is enabled;
b. which store is used;
c. which Content is generated;
d. publication frequency;
e. language;
f. target blog;
g. publication status;
h. quality score;
i. Content rules.

19.3 Autopilot only processes data required for the selected settings.

19.4 The Controller remains responsible for:

a. the lawfulness of the settings;
b. reviewing Generated Content;
c. publication of Content;
d. amendment and removal of Content;
e. informing Data Subjects where required.

19.5 Content already published remains in Shopify until the Controller removes or changes it.

Article 20. Duration, return and deletion

20.1 The Processing continues for as long as:

a. the Account remains active;
b. the Shopify Store remains connected;
c. the Processor processes Personal Data on behalf of the Controller;
d. retention is required to complete outstanding instructions.

20.2 Following termination, the Controller may choose:

a. return of available Personal Data;
b. deletion of Personal Data.

20.3 The Controller must submit a request for return within 30 days following termination.

20.4 Where the Controller does not provide a choice, the Processor deletes or anonymises the relevant data no later than 30 days following termination.

20.5 The Processor is not required to delete data where retention is legally required.

20.6 Data that must legally be retained:

a. will be restricted;
b. will not be used for other purposes;
c. will be deleted when the retention obligation ends.

20.7 Backups may temporarily continue to contain deleted Personal Data.

20.8 Personal Data in backups will generally be overwritten or made inaccessible within 90 days.

20.9 The Processor is not required to remove Content already published in the Shopify Store.

20.10 The Controller manages published Content within Shopify.

20.11 Anonymised and aggregated data that can no longer be linked to a person may be retained following termination.

Article 21. Removal of the Shopify app and privacy requests

21.1 When the Shopify app is removed, the Processor's active access to the relevant Shopify Store ends.

21.2 The Processor supports the mandatory Shopify privacy requests:

a. customers/data_request;
b. customers/redact;
c. shop/redact.

21.3 The Processor verifies the authenticity of these requests in accordance with Shopify security requirements.

21.4 Following a valid privacy request, the Processor checks whether Personal Data relating to the relevant Data Subject or Shopify Store is processed.

21.5 The Processor provides, deletes or anonymises relevant data in accordance with the received request and the instructions of the Controller.

21.6 The Processor generally processes a valid Shopify privacy request within 30 days.

21.7 Where the Processor does not process protected customer data relating to the relevant Data Subject, the Processor may record and close the request accordingly.

21.8 Data that must legally be retained will not be deleted for as long as the retention obligation applies.

21.9 Content already published to Shopify remains in the Shopify Store and falls under the management of the Controller after the app is removed.

Article 22. Audits and inspections

22.1 The Processor makes available information reasonably required to demonstrate compliance with this Data Processing Agreement and Article 28 of the GDPR.

22.2 The Controller first uses available:

a. documentation;
b. security information;
c. questionnaires;
d. audit reports;
e. statements;
f. certifications.

22.3 The Controller may request one additional audit per calendar year.

22.4 The restriction in Article 22.3 does not apply in the event of:

a. a serious Personal Data Breach;
b. a specific suspicion of material non-compliance;
c. a binding request from a supervisory authority;
d. a legal obligation.

22.5 An audit must be announced In Writing at least 30 days in advance, unless a supervisory authority requires a shorter period.

22.6 An audit:

a. takes place during normal business hours;
b. may not unreasonably disrupt the Service;
c. must be limited to relevant Processing activities;
d. must take account of the security of other customers;
e. must protect confidential information.

22.7 A physical or technical audit must be carried out by an independent expert bound by confidentiality.

22.8 The Processor is not required to grant access to:

a. data of other customers;
b. source code;
c. trade secrets;
d. internal fraud detection systems;

e. information that may compromise the security of the Service.

22.9 Audit costs are borne by the Controller.

22.10 Where an audit shows that the Processor materially fails to meet its obligations, the Processor bears the reasonable costs of the required follow-up assessment.

22.11 The Parties agree in advance on the scope, schedule and costs of an audit.

Article 23. Assistance with GDPR obligations

23.1 The Processor assists the Controller where reasonably and technically possible with:

a. rights of Data Subjects;
b. security;
c. Personal Data Breaches;
d. data protection impact assessments;
e. prior consultation with supervisory authorities;
f. demonstrating compliance;
g. determining retention periods;
h. international transfers.

23.2 The Controller provides the information required by the Processor to provide assistance.

23.3 The Processor may charge reasonable fees for assistance that:

a. falls outside the standard functionality;
b. requires substantial manual work;
c. requires custom development;
d. results from inaccurate or incomplete instructions from the Controller.

23.4 The Processor informs the Controller of costs in advance where reasonably feasible.

Article 24. Requests from public authorities and supervisory authorities

24.1 The Processor only provides Personal Data to a public authority, supervisory authority or court where:

a. this is legally required;
b. a valid binding order has been received;
c. the Controller provides a valid instruction.

24.2 Where reasonable, the Processor verifies:

a. the authority of the requesting party;
b. the validity of the request;
c. the scope of the requested data.

24.3 The Processor informs the Controller in advance, unless prohibited by law.

24.4 The Processor limits disclosure to the data necessary under the request.

24.5 The Processor may challenge a manifestly unlawful, excessive or unauthorised request where reasonable and legally permitted.

Article 25. Liability

25.1 The liability of the Parties is governed by:

a. the GDPR;
b. other mandatory law;
c. this Data Processing Agreement;
d. the liability provisions in the Zynceo General Terms and Conditions.

25.2 The limitations of liability in the General Terms and Conditions apply to the extent they do not conflict with Article 82 of the GDPR or other mandatory law.

25.3 The Processor is not liable for damage resulting from:

a. unlawful instructions from the Controller;
b. the absence of a valid legal basis;
c. inaccurate or incomplete information;
d. unnecessary entry of Personal Data;
e. insufficient security by the Controller;
f. incorrect management of Shopify permissions;
g. publication or use of Content by the Controller;
h. acts or omissions of employees or Team Members of the Controller.

25.4 The Controller indemnifies the Processor against claims resulting from unlawful Processing for which the Controller is responsible.

25.5 An indemnity does not apply to the extent that damage was caused by a failure of the Processor.

Article 26. Term and termination

26.1 This Data Processing Agreement takes effect as soon as the Processor processes Personal Data on behalf of the Controller.

26.2 The Data Processing Agreement remains in force for as long as the Processor processes such Personal Data.

26.3 Termination of the Account, Subscription or Shopify connection terminates this Data Processing Agreement after:

a. outstanding instructions have been completed;
b. Personal Data has been returned or deleted;
c. mandatory retention periods have ended.

26.4 The following provisions continue after termination where required:

a. confidentiality;
b. deletion and return;
c. audits;
d. liability;
e. governing law;
f. obligations relating to retained data.

Article 27. Amendments

27.1 The Processor may amend this Data Processing Agreement where required due to changes in:

a. law;
b. supervisory authority guidance;
c. Shopify rules;
d. the Service;
e. Subprocessors;
f. security measures;
g. technical infrastructure.

27.2 Material amendments will be announced at least 30 days in advance.

27.3 Notification may take place through:

a. email;
b. dashboard notification;
c. the website;
d. a notification within the Service.

27.4 An amendment may not retroactively reduce the protection of Personal Data already processed.

27.5 Where the Controller does not accept a material amendment, the Controller may terminate the affected part of the Service before the effective date.

27.6 An amendment may take effect immediately where required due to:

a. mandatory law;
b. a serious security risk;
c. a binding order;
d. an urgent change involving a required Subprocessor.

27.7 The Processor informs the Controller in that situation as soon as reasonably possible.

Article 28. Governing law and disputes

28.1 This Data Processing Agreement is governed by Dutch law.

28.2 The Parties will first attempt to resolve a dispute through consultation.

28.3 Complaints and disputes may be sent to team@zynceo.com.

28.4 Disputes will otherwise be handled in accordance with the dispute provisions in the Zynceo General Terms and Conditions.

28.5 To the extent legally permitted, disputes will be submitted to the competent court of the District Court of Overijssel, Zwolle location.

ANNEX 1. DETAILS OF THE PROCESSING

1. Subject matter of the Processing

The Processing of Personal Data for the provision, security and support of Zynceo, a SaaS platform for AI-powered SEO content creation, blog automation, content optimisation, internal linking, translations, image generation and Shopify integrations.

2. Duration of the Processing

The Processing continues for as long as:

a. the Account or Subscription remains active;
b. the Shopify Store remains connected;
c. the Processor processes Personal Data on behalf of the Controller;
d. data is returned, deleted or lawfully retained in accordance with Article 20.

3. Nature of the Processing

The Processing may include:

a. collection;
b. receipt;
c. recording;
d. storage;
e. consultation;
f. analysis;
g. classification;
h. organisation;
i. synchronisation;
j. transmission;
k. generation;
l. rewriting;
m. translation;
n. modification;
o. publication;
p. logging;
q. security;
r. export;
s. anonymisation;
t. deletion;
u. destruction.

4. Purposes

a. providing the Service;
b. connecting Shopify Stores;
c. processing store content;
d. generating and optimising Content;
e. translating Content;
f. generating images;
g. performing SEO analyses;
h. operating internal linking;
i. operating Autopilot;
j. providing support;
k. securing the Service;
l. preventing fraud and misuse;
m. resolving technical errors;
n. carrying out instructions of the Controller.

5. Standard categories of Personal Data

a. names and business contact details of Zynceo users;

b. business email addresses;
c. company names and job titles;
d. Account roles and user permissions;
e. IP addresses;
f. browser and device information;
g. language, country and time zone;
h. Shopify domain and Store ID;
i. API tokens and webhook information;
j. technical logs and error messages;
k. support messages and attachments;
l. prompts and Content instructions;
m. Content that may contain Personal Data;
n. Generated Content that may contain Personal Data;
o. other data entered by the Controller.

6. Excluded standard data

The standard functionality is not intended for:

a. complete customer profiles;
b. residential or shipping addresses;
c. order history;
d. checkout information;
e. payment card information;
f. bank details;
g. health data;
h. criminal offence data;
i. special categories of Personal Data;
j. data relating to children.

7. Categories of Data Subjects

a. users of the Zynceo Account;
b. employees and directors of the Controller;
c. freelancers and contractors;
d. business contacts;
e. persons included by the Controller in Content, prompts, images, reviews or support messages;
f. customers or visitors of the Shopify Store, to the extent their Personal Data is made available by the Controller.

ANNEX 2. TECHNICAL AND ORGANISATIONAL MEASURES

Depending on the relevant system, risks and state of the art, the Processor applies the following categories of measures.

1. Access management

a. role-based access and permissions;
b. restricted administrative rights;
c. access based on the need-to-know principle;
d. withdrawal of access when no longer required;
e. periodic review of relevant access rights.

2. Authentication

a. secure authentication methods;
b. secure storage of password hashes;
c. session management;
d. protection against unauthorised login attempts;
e. additional authentication for administrators where supported and appropriate.

3. Encryption and transport security

a. encrypted connections for data transmission;
b. secure communication with APIs;
c. secure storage of tokens and secrets;
d. encryption of stored data where appropriate and technically available.

4. Shopify and API security

a. limitation to required Shopify scopes;
b. verification of relevant webhooks;
c. secure processing of access tokens;
d. revocation or removal of connections following termination;
e. validation and restriction of API requests where appropriate.

5. Logging and monitoring

a. logging of relevant technical events;
b. monitoring of errors and availability;
c. detection of misuse and suspicious activity;
d. security logging;
e. restriction of access to logs.

6. Availability and recovery

a. backups where appropriate;
b. system monitoring;
c. recovery procedures;
d. maintenance and update processes;
e. measures supporting continuity of critical components.

7. Vulnerabilities and changes

a. periodic software updates;
b. management of technical dependencies;
c. assessment of critical vulnerabilities;
d. controlled changes to production environments;
e. restriction of unauthorised changes.

8. Organisational security

a. confidentiality obligations;
b. restricted access to Personal Data;
c. internal incident procedures;
d. arrangements with Subprocessors;

e. procedures for data protection requests;
f. procedures for deletion and export;
g. awareness among persons with access.

9. Data minimisation

a. processing only required data;
b. not requesting protected Shopify customer data by default;
c. limiting Personal Data included in prompts;
d. deleting or anonymising data when no longer required.

10. Incident management

a. procedures for detecting and assessing incidents;
b. containment and recovery;
c. internal recording;
d. communication with the Controller;
e. evaluation and measures to prevent recurrence.

ANNEX 3. SUBPROCESSORS

1. Current register

1.1 The Processor maintains a current register of Subprocessors that are actually used.

1.2 The register is made available through the legal documentation on www.zynceo.com or on request through team@zynceo.com.

1.3 Where reasonably available, the register includes for each Subprocessor:

a. name and country of establishment;
b. service provided;
c. purpose of the Processing;
d. categories of Personal Data;
e. Processing location;
f. applicable international transfer mechanism.

2. Possible categories of Subprocessors

The register may contain Subprocessors for:

a. Shopify platform and integrations;
b. hosting and cloud infrastructure;
c. database and storage;
d. AI text models;
e. AI image models;
f. email and system notifications;
g. logging and error tracking;
h. analytics;
i. support;
j. security;
k. backups and recovery.

3. Change procedure

3.1 The Processor informs the Controller of material changes in accordance with Article 16.

3.2 Only Subprocessors that actually process Personal Data on behalf of the Controller are included in the register.

3.3 Shopify Billing is not automatically considered a Subprocessor under this Data Processing Agreement where Shopify processes payment information for its own purposes and under its own responsibility.

ANNEX 4. CONTACT POINTS

Privacy enquiries and data protection requests
team@zynceo.com
Security notifications and Personal Data Breaches
team@zynceo.com
Support
support@zynceo.com
Legal enquiries
team@zynceo.com
Postal address
Zyncport B.V.
Trading under the name Zynceo
Spoorstraat 35b
8271 RG IJsselmuiden
The Netherlands