DATA PROCESSING AGREEMENT

This Data Processing Agreement forms part of and is subject to the Agreement (as defined below).The Parties enter into this Data Processing Agreement in order to govern the sharing of personal data under the Agreement.

1. Definitions

1.1 In this Data Processing Agreement, any reference to a paragraph shall be to a paragraph of this Data Processing Agreement and the following terms shall have the meanings set out below unless the context requires otherwise:

Agreement	the agreement concluded between the Company and the Client in accordance with the terms of service of Scraping Fish service, available at https://scrapingfish.com;
Applicable Data Laws	as applicable and binding on the Client, the Company and/or the Service, including, if and to the extent applicable: (a) in member states of the European Union (EU) and/or European Economic Area (EEA): the GDPR and all relevant EU and EEA member state laws or regulations giving effect to or corresponding with any of the GDPR; (b) in the United Kingdom (UK): (i) the Data Protection Act 2018; and (ii) the UK GDPR, and/or any corresponding or equivalent national laws or regulations; and (c) in the United States of America (USA): the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. and implementing regulations (CCPA); and (d) any Applicable Laws replacing, amending, extending, re-enacting or consolidating the above Applicable Data Laws from time to time;
Applicable Law	as applicable and binding on the Client, Company and/or the Service, including (if and to the extent applicable) applicable laws of the EU, the EEA or any of the EU or EEA's member states or the USA from time to time together with applicable laws in the UK from time to time;

Appropriate Safeguards	such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Applicable Data Laws from time to time;
CCPA	the California Consumer Privacy Act of 2018 (Cal. Civ. Code §1798.100 et seq.), as amended by the California Privacy Rights Act of 2020 (CPRA), together with any implementing regulations, and any subsequent amendments, collectively governing the processing of Personal Information of California resident;
Company	Narf sp. z o.o. with its registered office in Warsaw at Aleja Jana Pawła II 27, 00-867 Warsaw, Poland, entered in the Commercial Register of the Polish Court Register (rejestr przedsiębiorców KRS) kept by the District Court for Capital City of Warsaw in Warsaw, XIII Commercial Department, under KRS number 0001004209, with its share capital of PLN 6.000,00, holding taxpayer identification number NIP 5273029809 and statistical number REGON 523747406, represented by Paweł Kobojek, the President of the Management Board.
Client	shall mean an entity using the functionalities of the Service, who has full legal capacity.
Data Protection Losses	means all liabilities, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and (b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and (iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

Data Subject Request	a request made by a Data Subject or a Consumer to exercise any rights of Data Subjects or Consumers under Applicable Data Laws;
GDPR	the General Data Protection Regulation, Regulation (EU) 2016/679 as amended from time to time;
Personal Data	any information relating to an identified or identifiable natural person processed by the Client through the use of the Service from websites or online sources targeted by the Client;
Service	the service provided by the Company under the Agreement;
Sub-Processor	another Processor (or, if and to the extent the CCPA may apply, sub-contractor) engaged by the Company for carrying out processing activities in respect of the Personal Data on behalf of the Client or an Authorised Affiliate (as updated by the Company from time to time), which as at the date of our Agreement are as set out in Annex A to this Data Protection Agreement;
Supervisory Authority	any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Applicable Data Laws;
UK GDPR	the UK General Data Protection Regulation, which became effective on the 1st January 2021 as amended from time to time.

1.2 Business, Consumer, Controller, Data Subject, Personal Data, Personal Data Breach, Personal Information, processing, Processor, Service Provider have the meanings given to those terms and equivalent terms in Applicable Data Laws.

1.3 Capitalised terms that are not separately defined shall have the same meaning given to those terms elsewhere in the Agreement.

2. Processor and Controller or Service Provider

2.1 The parties agree that, for the Personal Data, the Client shall be the Controller and the Company shall be the Processor. If and to the extent the CCPA may apply, the parties agree that the Company shall act as a Service Provider and shall process and transfer Personal Information solely for the purpose of performing its obligations under the

Agreement for or on behalf of the Client or its affiliate and for no commercial purpose other than the performance of such obligations.

2.2 To the extent the Client is not sole Controller of any Personal Data it warrants that it has full authority and authorisation of all relevant Controllers to instruct the Company to process the Personal Data in accordance with the Agreement. If and to the extent the CCPA may apply, the Client warrants that it has full authority and authorisation to instruct the Company to process Personal Information as a Service Provider in accordance with the Agreement.

2.3 The Company shall process Personal Data in compliance with the obligations of the Processors (or, if and to the extent the CCPA may apply, Service Providers) under Applicable Data Laws and the terms of the Agreement.

3. Instructions and details of processing

3.1 The Client's documented instructions for the processing of Personal Data are provided in the Agreement ("**Instructions**"). The Company shall process Personal Data solely on the basis of such Instructions and only to the extent necessary to provide the Service. The Company shall not be responsible for determining the legality of the Client's scraping targets or Instructions. However, if the Company considers that the Instructions are not compliant with the Applicable Data Laws, the Company shall inform the Client accordingly.

3.2 The processing of the Personal Data by the Company under the Agreement shall be for the subject-matter, duration, nature and purposes, the types of Personal Data and categories of Data Subjects are set out in Annex A to this Data Processing Agreement.

4. Technical and organisational measures

4.1 Taking into account the nature of the processing, the Company shall implement and maintain, at its cost and expense, technical and organisational measures:

4.1.1 in relation to the processing of Personal Data by the Company, as set out in the Annex B to this Data Processing Agreement; and

4.1.2 to assist the Client insofar as is possible in the fulfilment of the Client's obligations to respond to Data Subject Requests relating to Personal Data.

5. Using staff and other processors

5.1 Subject to paragraph 5.2 and 5.3 below, the Company shall not engage any Sub-Processor for carrying out any processing activities in respect of the Personal Data in accordance with the Agreement without the Client's written authorisation of that Sub-Processor (such authorisation not to be unreasonably withheld, conditioned or delayed).

5.2 The Client authorises the appointment of each of the Sub-Processors listed in Annex A to this Data Protection Agreement.

5.3 The Company shall:

5.3.1 prior to any Sub-Processor carrying out any processing activities in respect of the Personal Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under this Data Protection Agreement (as relevant to the specific processing services being performed) that is enforceable by the Company;

5.3.2 ensure each such Sub-Processor complies with all such obligations; and

5.3.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

5.4 The Company shall notify the Client of any intended changes concerning the addition or replacement of Sub-Processors at least 7 days in advance, thereby giving the Client the opportunity to object to such changes. If the Client objects to the new Sub-Processor on reasonable grounds relating to data protection, the Company shall use reasonable efforts to make available to the Client a change in the Services or recommend a commercially reasonable change to the Client's use of the Services to avoid processing of Personal Data by the objected-to new Sub-Processor. If no alternative is reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within 14 days after the Company's receipt of the objection, the Client may terminate the Agreement with respect to those Services which cannot be provided without the use of the objected-to new Sub-Processor.

5.5 The Company shall ensure that all persons authorised by it (or by any Sub-Processor) to process the Personal Data are subject to a binding written contractual obligation to keep the Personal Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Company shall, where practicable and not prohibited by Applicable Law, notify the Client of any such requirement before such disclosure).

6. Assistance with compliance and Data Subject Requests

6.1 The Company shall:

6.1.1 refer all Data Subject Requests it receives to the Client without undue delays;

6.1.2 provide such reasonable assistance as the Client reasonably requires in responding to Data Subject Requests.

6.2 The Company shall not respond to any request received directly from a Data Subject relating to the exercise of rights under Applicable Data Laws unless the Company has received documented instructions to do so from the Client or such response is required by Applicable Law.

6.3 If the Company receives any request, complaint, inquiry, or other communication from a Data Subject in relation to Personal Data processed on behalf of the Client, the Company shall forward such request to the Client without undue delay and shall not take further action unless instructed by the Company.

6.4 Taking into account the nature of the Processing and the technical capabilities of the Service, the Company shall provide reasonable assistance to the Client in fulfilling the Client’s obligation to respond to Data Subject requests under Applicable Data Protection Laws. Such assistance may include:

a) deletion of data stored within the Service, where technically possible;

b) providing information on whether the Company holds Personal Data linked to the request, subject to Section 6.5.

6.5 The Client acknowledges that, due to the nature of web scraping and the architecture of the Service, the Company may not be able to:

a) identify Personal Data relating to a specific Data Subject;

b) locate or extract specific records without information reasonably necessary to identify the relevant data; or

c) assist with requests where the Company cannot technically determine whether the data relates to the Data Subject.

In such cases, the Company’s assistance shall be limited to the technical measures reasonably available to it.

6.6 Any assistance provided by the Company under this section may be subject to reasonable fees if such assistance goes beyond what is necessary to comply with the Company's obligations under Applicable Data Laws.

7. No International data transfers

7.1 Unless the Client provides prior written consent, the Processor shall ensure that all Personal Data processed in connection with the Service is processed within the European Union.

8. Information and audit

8.1 The Company shall maintain, in accordance with Applicable Data Laws binding on the Company, written records of all categories of processing activities carried out on behalf of the Client.

8.2 The Client may by written notice to the Company request information regarding the Company's compliance with the obligations placed on it under this Data Processing Agreement. On receipt of such request the Company shall provide the Client (or auditors mandated by the Client) with a copy of the latest third party certifications and audits to the extent made generally available to its Clients. Such copies are confidential to the Company.

8.3 The Client may, at a time to be agreed between the parties, conduct an audit or inspection as reasonably necessary to verify the Company's (or any Sub-Processor's) compliance with the obligations under this Data Processing Agreement provided:

8.3.1 the security and confidentiality of other Clients shall be protected and the Company, or any Sub-Processor, is not placed in breach of any other arrangement with any other Client;

8.3.2 the Client's rights under this paragraph 9.3 may only be exercised once in any consecutive 12 month period, unless otherwise required by a Supervisory Authority or if the Client (acting reasonably) believes the Company is in breach of this Data Protection Agreement; and

8.3.3 the Client shall ensure that all information obtained or generated by the Client or its auditor(s) in connection with such inspections and audits is kept strictly confidential (save for disclosure required by Applicable Law).

9. Breach notification

9.1 The Company shall notify the Client of any Personal Data Breach involving Processed Data that is likely to result in a risk to the rights and freedoms of individuals within 24 hours of becoming aware and provide the Client with details of the Personal Data Breach.

9.2 The Client shall implement and maintain appropriate technical and organisational measures to protect Personal Data from personal data breaches (the „**Security Incidents**"), in accordance with standards set out in Annex B to this Data Processing Agreement.

10. Deletion of Personal Data and copies

10.1 The Company does not store the Personal Data. However, if, by any chance, the Company will be in possession of the Personal Data, following the end of the provision of the Service, the Company shall, at the Client's choice, either delete or return to the Client all Personal Data. The Company shall have no liability for any deletion or destruction of any such Personal Data undertaken in accordance with the Agreement.

11. Client obligations

11.1 The Client shall:

11.1.1 establish and maintain the procedure for the exercise of the rights of the Data Subjects whose Service Data are processed on behalf of the Client;

11.2.2 ensure compliance with the Applicable Data Laws, the provisions of this Data Processing Agreement by its personnel or by any third party accessing or using Personal Data on the Client's behalf, including maintaining all relevant regulatory registrations and notifications as required under Applicable Data Laws;

11.2.3 duly inform the Data Subjects about the processing of their Personal Data and the characteristics of the processing of this Personal Data;

11.2.4 ensure the existence of the legal basis for the processing, in particular by seeking the prior consent of the Data Subjects when this is required by the Applicable Data Laws, the practice of the Supervisory Authorities, or customary practice;

11.2.5 indemnify and hold the Company harmless against any Data Protection Losses arising from or relating to (i) the Client's Instructions, (ii) the Client's use of the Service in violation of Applicable Regulations, or (iii) any Personal Data processed by the Company on behalf of the Client.

11.2 The Client shall not:

11.2.1 process any sensitive personal data, special categories of Personal Data, Personal Data relating to criminal convictions and offences or any patient, medical or other protected health information regulated by the GDPR or similar national, federal or state laws, rules or regulations ("Sensitive Data), or use the Service in such a way as to generate Sensitive Data, without the Company's prior written consent; or

11.2.2 use the Service to obtain or transfer Personal Data from another party unless it has the agreement of such party and has put Appropriate Safeguards in place.

ANNEX A

DATA PROCESSING DETAILS

Subject-matter of processing:

Performance of our respective rights and obligations under the Agreement and delivery and receipt of the Services under the Agreement.

Duration of the processing:

Until the earlier of final termination or final expiry of the Agreement, except as otherwise expressly stated in the Agreement.

Nature and purpose of the processing:

The Company shall process Personal Data solely to the extent necessary to provide the Service to the Client. Such processing may include:

(a) retrieving data from online sources as instructed by the Client;

(b) transmitting such data through the Company's infrastructure; and

(c) returning the requested data to the Client in the form of an API response.

The Company does not store Personal Data and does not use Personal Data for its own purposes. The Company does not analyse, modify, enrich, index, profile or otherwise manipulate Personal Data.

Type of Personal Data:

The Company shall process only such Personal Data that the Client transmits through or retrieves by means of the Service, as well as any other Personal Data the Client provides in connection with the use of the Service, as further described in the Agreement. The Personal Data processed through the Service may include, where applicable, names, contact information (e.g., email, phone number), demographic information, marketing-related data, behavioural data, and any other Personal Data contained in the online resources targeted by the Client. Such Personal Data may arise incidentally from the Client's scraping activities and may include Personal Data contained in the online resources that the Client instructs the Service to access

Categories of Data Subjects:

The Company shall process Personal Data only to the extent submitted, transmitted, proxied, or retrieved by the Client through the use of the Service. The categories of Data Subjects (if any) are determined solely by the Client based on the targets and parameters defined by the Client. This may include, where applicable, individuals whose information is publicly available online, users of websites or online platforms targeted by the Client, customers or prospective customers of the Client, business contacts, employees or contractors of third-party entities, or any other individuals whose Personal Data appears in the online resources selected by the Client. The Company does not determine, select, or control the categories of Data Subjects and processes such data exclusively on behalf of the Client and in accordance with the Client's Instructions.

Lawful Basis for Processing

The Client's lawful basis for processing the Personal Data is either legitimate interest or consent.

Sub-Processors

Provider	**Service**	**Contact, incl. address and contact person (name, position, contact details)**
Hetzner Online GmbH	Servers / Hosting Services	Industriestr. 25 91710 Gunzenhausen, Germany +49 (0)9831 505-0 info@hetzner.com

ANNEX B
TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Company shall implement and maintain the following technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR:

1. **Access Control**

– Access to systems is restricted to authorised personnel on a need-to-know basis.

2. **Data Security**

– Encryption in transit (HTTPS/TLS) is used for all data transmitted through the Service.

3. **Infrastructure Security**

– The Service is hosted on secure data centers with industry-standard physical and network security controls.
– Firewalls and network isolation are implemented.

4. **Operational Security**

– Regular software updates, security patches and vulnerability assessments are performed.
– Anti-malware and intrusion detection systems are used.

5. **Organisational Measures**

– Employees or other persons acting under the authority of the Company with access to systems are bound by confidentiality obligations.
– Internal data protection policies and security practices are maintained.

6. **Data Retention and Deletion**

– Personal Data processed through the Service is not stored.

7. **Incident Management**

– The Company maintains procedures for detecting, reporting and responding to Personal Data breaches.