

# DATA PROCESSING AGREEMENT

Welcome to Nu Skin's Volumes & Genealogies System and/or Nu Skin Stela. To comply with international data protection laws and provide access to your downline information, you must carefully review and accept the terms and conditions of this Data Processing Agreement. By agreeing to the terms of your Brand Affiliate or Direct Seller Agreement, as applicable, you are agreeing to the terms of this Data Processing Agreement.

This Data Processing Agreement is between you as a Nu Skin brand affiliate or direct seller ("**You**" or the "**Processor**" or "**Data Fiduciary**") and

- Nu Skin International Inc., 75 W. Center Street, Provo, UT 84601, USA, ("**NSI**"); and

*On the one hand, if, and to the extent You process Personal Data of Data Subjects located in the European Economic Area ("**EEA**"), except in Romania; and*

- NSE Products Europe BV, Da Vincilaan 9, 1930 Zaventem, Belgium, company number 0642 635 688 ("**NSEPE**"); and

*On the other hand, if and to the extent You process Personal Data of Romanian Data Subjects.*

- Nu Skin Enterprises SRL, Str. Grigore Cobalcescu 46, mansard, Camera 13, Bucharest, Romania, company number 03007509 ("**NSRO**")

Hereinafter the "Joint Controllers" or "Data Principals", as applicable;

You and the Joint Controllers may be referred to each as a "Party" or together the "Parties".

**\*\*Please review this Data Processing Agreement in its entirety, and if you agree to its terms, enter your Name, Brand Affiliate or Direct Seller ID#, as applicable and click "I accept." Please download and retain a copy of this Data Processing Agreement for your records.\*\***

## A. Definitions

**Agreement:** means the International Sponsor and Brand Affiliate or Direct Seller Agreement, as applicable;

**Data Processing Agreement or DPA:** means this agreement, including (any) enclosures and modifications;

**Data Subject(s):** means the identifiable or identified natural person(s) whose Personal Data is or are processed;

**Data Protection Authority:** Any representative or agent of the government who has the authority to enforce local data privacy and security laws.

**Data Protection Laws** means all applicable worldwide legislation that concern Personal Data (including the collection and use thereof), advertising, marketing, privacy, data security, artificial intelligence, data protection or data transfer, including all privacy and security breach disclosure laws, in each case as the same has been interpreted to apply to privacy, data protection, breach disclosure or data transfer issues.

**"GDPR"** means, as appropriate and as amended from time to time: (i) the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of the UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**").

**Personal Data** means any information, that either individually or when combined with other information, could be used to distinguish or trace an individual's identity, such as their name, address, telephone number, national ID number, account information, and/or biometric records, including all information given protected status under any Data Protection Law.

**Personal Data Breach:** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

**Subprocessor:** means any entity which processes Information on behalf of Processor.

## **B. Processing**

1. The Parties will, each in their respective capacity, process the Personal Data in accordance with this Data Protection Agreement and all Data Protection Laws to which the Joint Controllers and/or Processor are subject.
2. All processing activities shall always be done in compliance with Annex 1 to this Data Processing Agreement.
3. Processor has no control on the purpose of the processing of Personal Data, nor may it independently take decisions concerning the use, storage or disclosure of the Personal Data, unless and to the extent it has been expressly agreed upon in this Data Processing Agreement.
4. Processor undertakes to implement and comply with the appropriate technical and organisational security measures necessary to protect the Personal Data in case of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or non-authorised access to Personal Data. When determining the appropriate technical and organisational security measures, Processor shall take into account: (i) the state of the art, (ii) the implementation costs related to these measures, (iii) the nature, scope, context and purposes of processing, (iv) the risks involved for the Data Subjects' rights and freedoms, in particular in case of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or non-authorised access to Personal Data transmitted, stored or otherwise processed, and (v) the probability that the processing shall have an impact on the rights and freedoms of the Data Subjects.
5. Processor will, when requested by one or more of the Joint Controllers, communicate to the requesting Joint Controllers all the information required concerning the processing of Personal Data and shall transfer to the requesting Joint Controllers any Data Subject's request or question in connection with the (processing of) Personal data.
6. Processor can grant its employees access to the Personal Data to the extent the employees need such access to the Personal Data to allow a proper performance of Processor's obligations under the Agreement and under the Data Processing Agreement. Processor will inform the concerned employees in writing about the Personal Data's confidential character along with the legal and contractual framework of the protection of Personal Data and shall impose a contractual confidentiality obligation upon the concerned employees.
7. Processor shall not transfer Personal Data to any third party, including Subprocessors, without the relevant Joint Controllers' explicit prior written consent.

## **C. Transfer of Personal Data from the EEA**

To the extent Processor is located outside the EEA in a country which is not covered by an adequacy decision pursuant to Article 45 of GDPR, the Parties hereby enter into the Standard Contractual Clauses in Annex 2 in respect of any transfer of Personal Data from one or more Joint Controllers to Processor.

## **D. Obligation to assist**

1. Processor commits to assist the Joint Controllers in ensuring compliance with their legal obligations under all applicable privacy laws concerning security of the processing, the notification of a Personal Data Breach to the supervisory authority and the Data Subject, the drafting of a data protection impact assessment (if applicable), and prior consultation.

2. The Joint Controllers have a right to audit to verify the compliance of Processor with its obligations under the Data Processing Agreement. The Joint Controllers can conduct such audit once a year. The audit can be performed by the Joint Controllers or another auditor mandated by the Joint Controllers. The Joint Controllers will inform Processor at least 15 working days in advance about the working day during which the audit will occur.

If Processor, in its opinion, would receive during the audit an instruction, from the Joint Controllers or from another auditor mandated by the Joint Controllers, that infringes any Data Protection Laws, Processor shall immediately inform the Joint Controllers hereof.

3. Processor shall Immediately notify one of the Joint Controllers, in writing, of the following:

- i. A Data Subject's request to access, rectify, erase, transport, object to, or restrict Personal Data processed pursuant to this Data Protection Agreement;
- ii. Any request or complaint received from Joint Controllers' customers or employees;
- iii. Any question, complaint, investigation, or other inquiry from a Data Protection Authority; and
- iv. Any request for disclosure of Information from a public entity related in any way to Data Processor's Processing of Information under this Attachment.

#### **E. Duration and termination**

1. The Data Processing Agreement shall enter into force on the date You accept it. If Processor has already processed Personal data in the framework of the Agreement prior to the signing of the Data Processing Agreement, the Data Processing Agreement shall apply retroactively from the start of the processing of Personal Data by Processor in the name and on behalf of the Joint Controllers.
2. The Data Processing Agreement shall remain in force for the duration of the Agreement. If the Agreement terminates, the Data Processing Agreement shall terminate automatically.
3. Upon termination of the Data Processing Agreement, or upon the Joint Controllers' request to delete or return Personal Data, Processor will delete or return existing copies of Personal Data unless local law requires storage of the Information. In instances where local law requires Processor to store Personal Data, Processor will protect the confidentiality, integrity, and accessibility of the Personal Data; will not actively Process the Personal Data anymore; and will continue to comply with this Data Protection Agreement.

#### **F. Miscellaneous**

1. The Data Processing Agreement is severable. If one or more provisions that do not affect the essence of the Data Processing Agreement are declared fully or partially invalid, void or unenforceable, this shall not affect the validity and enforceability of the remaining provisions. The Data Processing Agreement will remain in force between the Parties, as if the invalid, void or unenforceable provision never existed.
2. In the aforementioned case, the Parties undertake to renegotiate in good faith the Data Processing Agreement to modify or replace the (fully or partially) void, invalid or unenforceable provision by a provision that most closely matches the purpose of the invalid, void or unenforceable provision.
3. Compliance by each Party with its obligations under the Data Processing Agreement is free of charge and cannot depend on the payment of a fee, unless expressly agreed otherwise.
4. This Data Processing Agreement constitutes the entire agreement between the Parties relating to its subject-matter and supersedes all prior arrangements (both oral and written) between the Parties with regard to the processing of Personal Data.

#### **G. Indemnity**

Processor will indemnify and hold the Joint Controllers and their affiliated companies, and each and any of the Joint Controllers’ or their affiliated companies’ shareholders, officers, directors and employees harmless from and against any claim, demand, liability, loss, action, causes of action, costs, or expenses, including, but not limited to, reasonable attorney’s fees, resulting or arising from, directly or indirectly, any acts or omissions by You in conducting Your independent business, including without limitation, breach of representations and warranties, material breach of the Data Processing Agreement and other agreements between the Parties, or any other claims or causes of action.

**H. Liability**

The Joint Controllers’ liability is restricted in conformity with the provisions of the International Sponsor and Brand Affiliate or Direct Seller Agreement, as applicable.

**I. Mandatory and binding arbitration**

- 1. THIS DATA PROCESSING AGREEMENT IS SUBJECT TO ARBITRATION. UTAH WILL BE THE EXCLUSIVE VENUE FOR ARBITRATION OR ANY OTHER RESOLUTION OF ANY DISPUTES ARISING UNDER OR RELATED TO THIS DATA PROCESSING AGREEMENT.** The place of origin of this Contract is the State of Utah, USA, and it will be governed by, construed in accordance with, and interpreted pursuant to the laws of Utah, without giving effect to its rules regarding choice of laws. The exclusive venue for any and all Disputes and jurisdiction will be in Salt Lake County, Utah, USA. Processor consents to the personal jurisdiction of any court within the State of Utah and waive any objection to improper venue.
2. Processor agrees that any Dispute will be resolved and settled in accordance with and pursuant to the terms and conditions of this Data Processing Agreement, and by the rules and procedures set forth in Chapter 7 (Arbitration) of the Policies and Procedures or may be viewed online in the Office section of a company web site. The arbitration proceedings will be conducted in Salt Lake City, Utah, USA. The arbitration will be conducted in the English language, but at the request and expense of a party, documents and testimony will be translated into another language. One arbitrator will be appointed to hear and decide disputes, which arbitrator will be selected by consent of all parties. The parties will each bear their own costs and expenses and an equal share of the (i) cost of the arbitrator and (ii) administrative fees of arbitration. Neither the parties nor the arbitrator may disclose the existence, content, or results of any arbitration without the prior written consent of both parties. Judgment on any award rendered by the arbitrator may be entered in any court having jurisdiction.
3. A “Dispute” is defined as any and all past, present or future claims, disputes, causes of action or complaints, whether based in contract, tort, statute, law, product liability, equity, or any other cause of action, (i) arising under or related to this Data Processing Agreement, (ii) between other Brand Affiliates and/or Direct Sellers and me arising out of or related to a Distributorship, or our business relationships as independent contractors of NSI, (iii) between NSI and me, (iv) related to NSI or its past or present affiliated entities, their owners, directors, officers, employees, investors, or vendors, (v) related to the Products, (vi) regarding NSI’s resolution of any other matter that impacts my Distributorship, or that arises out of or is related to NSI’s business, including my disagreement with NSI disciplinary actions or interpretation of the Agreement or the Data Processing Agreement.
4. PROCESSOR agreeS to accept and be bound by thIS Arbitration Agreement if Processor accesses any NU SKIN web site and uses the information therein.

**Annex 1: Overview of the Data Processing Agreement and the Processing Operations**

A. Subject matter of the Data Processing	<ul style="list-style-type: none"><li>Marketing of Joint Controllers’ products in Processor’s Resident Country (as defined in the Agreement) through person-to-person marketing</li></ul>
--	---

Agreement	<ul style="list-style-type: none"> <li>• Sponsoring of new Brand Affiliates or Direct Sellers, as applicable, in the countries where Joint Controllers is open for business</li> </ul>
B. Duration of the processing	<ul style="list-style-type: none"> <li>• Limited to the duration of the Data Processing Agreement</li> </ul>
C. Nature and purposes of the processing	<ul style="list-style-type: none"> <li>• Processor is authorized to access and consult Personal Data for the purpose of management of Customers, Brand Affiliates and Direct Sellers (including training and product support, administration of the distributorship organization)</li> </ul>
D. Type of Personal Data that are processed	<ul style="list-style-type: none"> <li>• The Personal Data processed concern the following categories: (i) account information such as name, photo, birthday, contact details (address, email, phone, social media handles/numbers); (ii) business information such as market of registration, purchase volumes, auto-ship contracts; and (iii) order information such as purchase details and auto-ship contract details.</li> </ul>
E. Categories of Data Subjects	<ul style="list-style-type: none"> <li>• The Personal Data processed concern the following categories of Data Subjects: Customers, Brand Affiliates and Direct Sellers</li> </ul>

**IMPORTANT NOTE:**

Non-English versions of this Annex 2, if any, are provided for convenience only. In case of discrepancy, the English version shall prevail.  
. This Annex applies to the extent that you process Personal Data of Data Subjects located in the European Economic Area.

## EU/UK GDPR Annex

### Controller to Processor

This EU/UK GDPR Annex shall apply to the extent there are any Restricted Transfers (as defined below):

In this Annex, the following terms shall have the meanings set forth in this Section 1, unless expressly stated otherwise:

- a. "Europe" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.
- b. "European Data Protection Laws" means data protection laws applicable in Europe, including the EU GDPR, the UK GDPR and the FADP, in each case as may be amended, superseded or replaced.
- c. "FADP" means the Swiss Federal Act on Data Protection.

d. "Relevant Body":

(i) in the context of the EU GDPR, means the European Commission; and/or

(ii) in the context of the UK GDPR, means the UK Government (Secretary of State); and/or

(iii) in the context of the Swiss FADP, the Federal Data Protection and Information Commissioner ("FDPIC").

e. "Restricted Country":

(i) in the context of the EEA, means a country or territory outside the EEA; and/or

(ii) in the context of the UK, means a country or territory outside the UK; and/or

(iii) in the context of Switzerland, means a country or territory outside of Switzerland, that the Relevant Body has not deemed to provide an "adequate" level of protection for Personal Data pursuant to a decision made in accordance with applicable European Data Protection Laws.

f. "Restricted Transfer" means the disclosure, grant of access or other transfer of Personal Data to any person located in:

(i) in the context of the EEA, a Restricted Country outside the EEA (an "EEA Restricted Transfer");

(ii) in the context of the UK, a Restricted Country outside the UK (a "UK Restricted Transfer"); and/or

(iii) in the context of Switzerland, a Restricted country outside Switzerland (a "Swiss Restricted Transfer").

g. "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of Personal Data to third countries.

h. "Supervisory Authority" means: (i) in the context of the EU GDPR, the Belgium Data Protection Authority; (ii) in the context of the UK GDPR, the UK Information Commissioner's Office (ICO); and (iii) in the context of the FADP, the FDPIC.

(i) "UK" means the United Kingdom.

(j) "UK Transfer Addendum" means the template Addendum B.1.0 issued by the UK Information Commissioners Office (ICO) and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof (the "Mandatory Clauses").

For purposes of this Annex, the terms "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing/Process/Processed" and "Processor" shall have the meaning ascribed to the corresponding terms in the GDPR.

#### **A. SIGNATURE OF THE SCCs**

Where the SCCs apply in accordance with the DPA, each of the parties is hereby deemed to have signed the SCCs by signing the applicable Brand Affiliate or Direct Seller Agreement.

#### **B. MODULE**

Module Two (Controller to Processor) of the SCCs shall apply to any Restricted Transfer under this DPA.

#### **C. POPULATION OF EU AND SWISS SCCs**

The SCCs shall be populated as follows:

1. The optional "Docking Clause" in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

2. The Parties agree that the certification of deletion of Personal Data that is describe in Clause 8.5 of the SCCs shall be provided by the data importer to the data exporter only upon data exporter's written request.

3. Parties agree that audits described in Clause 8.9 of the SCCs shall be carried out in accordance with Section 10 of the DPA.
4. In Clause 9, OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the additional or replacement of Subprocessors shall be the advance notice period set out in Section 11 of the DPA.
5. In Clause 11, the optional language is not used and is deleted.
6. In Clause 13, all square brackets are removed and all text therein is retained.
7. In Clause 17, OPTION 1 applies, and the parties agree that the SCCs shall be governed by the law of Belgium in relating to any EEA and Swiss Restricted Transfer.
8. For the purposes of Clause 18, the parties agree that any dispute arising from the SCCs in relation to any EEA and Swiss Restricted Transfer shall be resolved by the courts of Belgium and Clause 18(b) is populated accordingly.

#### **D. POPULATION OF THE ANNEXES TO THE SCCs**

Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Annex 1 (**TERMS OF PROCESSING**) to this DPA, with Nu Skin being “data exporter” and Processor being “data importer”.

Part C of Annex I to the Appendix to the SCCs is populated as follows: The competent supervisory authority shall be the Supervisory Authority set forth in Section 1 of this Annex.

Annex II to the Appendix to the SCCs is populated by reference to Annex II to this DPA (**MINIMAL ORGANISATIONAL AND TECHNICAL SECURITY MEASURES**).

#### **E. UK RESTRICTED TRANSFERS**

1. Part 1 of the UK Transfer Addendum. As permitted by Section 17 of the UK Transfer Addendum, the parties agree that:
  - i. Tables 1, 2 and 3 of Part 1 of the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (Personal Data Attachment) to this DPA and the foregoing provisions of Part 1 of Annex 2 (subject to the variations effected by the Mandatory Clauses described in (b) below): and
  - ii. Table 4 of Part 1 of the UK Transfer Addendum is completed by the box labelled “Data Importer” being deemed to have been ticked.
2. Part 2 of the UK Transfer Addendum. The parties agree to be bound by the Mandatory Clauses of the UK Transfer Addendum.
3. In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs shall be read as a reference to those SCCs as varied in the manner set out in this Part 2.

# **APPENDIX**

## **ANNEX I**

#### **A. LIST OF PARTIES**

**Data exporter(s):** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

**1. Name:** NSE Products Europe BVBA, in its own name and own behalf, as well as in the name and on behalf of the other Joint Controllers

Address: Da Vincilaan 9, The Corporate Village, Building Elsinore, 1930 Zaventem, Belgium

Contact person's name, position and contact details: Mikael Linder, President EMEA - +32 2 722 70 00, [privacy@nuskin.com](mailto:privacy@nuskin.com)

Activities relevant to the data transferred under these Clauses: the data exporter is responsible, among others, for the distribution of Nu Skin products in the European countries where Nu Skin is open for business.

**2. Name:** Nu Skin Enterprises SRL

Address: Str. Grigore Cobalcescu 46, mansard, Camera 13, Bucharest, Romania

Contact person's name, position and contact details: Lukas Rieder, VP Sales, [privacy@nuskin.com](mailto:privacy@nuskin.com)

Activities relevant to the data transferred under these Clauses: the data importer is an independent Nu Skin distributor marketing and selling Nu Skin products. As such, the data importer may be processing data of

Data Subject located in the European Economic Area.

\*\*\*\*\*

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

**The Brand Affiliate or Direct Seller executing the Brand Affiliate or Direct Seller Agreement, as applicable is the Data Importer under this DPA.**

Activities relevant to the data transferred under these Clauses: the data importer is an independent Nu Skin distributor marketing and selling Nu Skin products. As such, the data importer may be processing data of Data Subject located in the European Economic Area.

- Role (controller/processor): Processor
- Subprocessors: There are no subprocessors authorized under this DPA.

## **B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

- Customers and distributors

*Categories of personal data transferred*

- account information such as name, photo, birthday, contact details (address, email, phone, social media handles/numbers);
- business information such as market of registration, purchase volumes, auto-ship contracts; and
- order information such as purchase details and auto-ship contract details

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous basis



#### Nature of the processing

- Management of Customers, Brand Affiliates and Direct Sellers (including training and product support, administration of the distributorship and upline/downline organization)

#### Purpose(s) of the data transfer and further processing

- Processor/data importer is located outside of the EEA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- Up to the end of the Data Processing Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- n/a

### C. COMPETENT SUPERVISORY AUTHORITY

#### 1. Name: NSE Products Europe BV

Data exporter is established in an EEA country.

The competent supervisory authority is Belgian Data Protection Authority, Belgium.

#### 2. Name: Nu Skin Enterprises SRL

Data exporter is established in an EEA country.

The competent supervisory authority is The National Supervisory Authority for Personal Data Processing, Romania.

## **ANNEX II**

### **A. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

#### **a. Organizational measures**

- Data Security policy
- Notification procedure in case of physical/technical security incidents
- Information classification policy
- Plan to regularly assess organizational/technical measures' effectiveness

#### **b. Technical measures**

- Measures in case of fire-, burglary-, or water damage, or physical/technical incidents
- Control of access (physically and logical)
- User-ID and Password policy
- Processes to identify and apply security patches
- Anti-virus installed on all systems
- Firewall(s) implemented to protect information systems

- Encryption of sensitive personal data
- Back-up system

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

- n/a