This Data Processing Addendum (**"DPA")** applies to all customers using Nosto's Service and / or any Additional Services ("**Customer**", "**you**") as defined in Nosto's Terms of Use. This DPA should be read carefully in order to understand your rights and responsibilities, as well as ours.

By accessing or using the Service you acknowledge and agree that you have read, understood, and agree to be bound by this DPA. We may update this DPA from time to time; by continuing to use the Service after Nosto publishes notice of a modification on www.nosto.com you thereby accept the modification.

This DPA includes Schedules 1, 2 and 3 and shall be considered an integral part of Nosto's Terms of Use (available at www.nosto.com/terms/, as updated from time to time) between the Customer and Nosto, or any other agreement between the Customer and Nosto governing Customer's use of the Service provided by Nosto, such as an Order Form (the "**Agreement**").

1. **Effectiveness.**

   a. For the avoidance of doubt, this DPA applies only to Nosto Service purchased from Nosto and does not apply to a service the Customer purchases from any seller of record other than Nosto.

   b. The Customer represents and warrants to Nosto that he or she has the legal authority to bind and lawfully enter the Customer into the Order Form.

   c. This DPA will terminate automatically upon termination of the Order Form or Terms of Use (as the case may be), or as earlier terminated pursuant to the terms of this DPA.

SCHEDULE 1

Data Processing Terms

1. DEFINITIONS

Unless otherwise defined in the Order Form, all capitalized terms used in this DPA will have the meanings outlined below:

a. **"Customer Data"** is defined as the "personal data" (as defined in GDPR) that is processed within Nosto Infrastructure under the Customer's accounts.

b. **"CCPA"** is defined as United States SB-1121 California Consumer Privacy Act of 2018.

c. **"EEA"** is defined as the European Economic Area.

d. **"GDPR"** is defined as Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

e. **"Nosto Infrastructure"** is defined as Nosto and its service providers and / or subcontractor's data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within Nosto's control and are used to provide the Services.

f. **"Nosto Security Standards"** is defined as the security standards attached to this DPA as Schedule 2.

g. **"Processing"** has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

h. **"Regulation"** is defined as all legislation that applies to the protection of natural persons with regard to the processing of personal data and the free movement of such data including but not limited to the CCPA and GDPR.

i. **"Standard Contractual Clauses"** is defined as agreement pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the GDPR forming part of this DPA.

2. DATA PROCESSING

2.1 Scope and Roles. This DPA applies when Customer Data is processed by Nosto and its subcontractors. In this context, Customer shall act as "controller", Nosto shall act as "processor" and Nosto's subcontractor(s) shall act as "Sub-processor" with respect to Customer Data (as each term is defined in the GDPR). Notwithstanding the foregoing, Nosto shall act as the data controller with respect of the personal data we may have collected from you during registration or provision of support services, if any.

2.2 Details of the Data Processing. The details of the data processing such as subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects are specified in the Schedule 3 "Data Processing Details".

2.3 Compliance with Applicable Laws. Each party will comply with laws, rules and regulations applicable to it and binding on it in the performance of this DPA, especially including Regulation. As controller, the Customer shall ensure that it has the necessary rights and that it has obtained the necessary consents from the data subjects for Nosto's (and its Sub-processors') processing of personal data. The Customer shall ensure that they have the relevant privacy statement and cookie policy in place or that they otherwise inform the data subjects of the processing of personal data in accordance with the Regulation. By using the Service, you represent and warrant that you have informed and obtained necessary consents from the end user of your Online Store needed for the processing of their personal data and, to the extent applicable, your employees.

2.4 Special Categories of Personal Data. Customer hereby acknowledges and agrees that sending or storing any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation "Special

Categories of Personal Data" in the Service is strictly forbidden. By using the Service, you represent and warrant that you will not send or store any Special Categories of Personal Data in the Service.

2.5 Instructions for Data Processing. Nosto (and its subcontractors) will process Customer Data only in accordance with Customer's documented instructions, including with regard to transfers of personal data to a third country, unless required to do so by mandatory law to which the processor is subject, in which case Nosto shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The parties agree that this DPA is Customer's complete and final instructions to Nosto in relation to the processing of Customer Data. Processing outside the scope of this DPA (if any) will require a prior written agreement between Nosto and Customer regarding additional instructions for such processing, including an agreement on any additional fees the Customer will pay to Nosto for carrying out such instructions.

2.6 Access or Use. Nosto will not access or use Customer Data, except as necessary to provide the Service as defined in Order Form. Nosto may also use statistical, aggregated or otherwise anonymized data collected by the Service, provided that such data will not be directly or indirectly identifiable to the Customer or its customers.

2.7 Disclosure. Nosto will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Nosto a demand for Customer Data, Nosto will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Nosto may provide the Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Nosto will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy unless Nosto is legally prohibited from doing so.

2.8 Nosto Personnel. Nosto restricts its personnel from processing Customer Data without authorization as described in the Schedule 2 "Nosto Security Standards". Nosto will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

2.9 Customer Controls. The Service provides the Customer with controls to enable the Customer to delete or block Customer Data as described within the Service. Nosto makes available a number of features and functionalities that the Customer may elect to use. The Customer is responsible for properly (a) configuring and using the Service, (b) using the controls available in connection with the Service, and (c) taking such steps as the Customer considers adequate to maintain appropriate security, protection, deletion and backup of Customer Data. The Customer may use these controls as Nosto's assistance by appropriate technical and organizational measures (as stated in the GDPR) for the fulfilment of the Customer's obligation as controller under the Regulation to respond to requests for exercising the data subject's rights.

2.10 Assistance with Prior Consultation and Security of Processing. The information made available by Nosto under Schedule 2 "Nosto Security Standards" is intended to assist the Customer in complying with the Customer's obligations under the GDPR articles 32 to 36, taking however into account the nature of processing and the information available to Nosto.

2.11 Customer Indemnification. You agree to indemnify and hold Nosto (and our subsidiaries, officers, directors, employees) harmless from any claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your breach of the above sub-section 2.4 (Special Categories of Personal Data) and 2.5 (Instructions for Data Processing) of the Section 1 "Data Processing Terms".

3. TRANSFERS OF PERSONAL DATA

3.1 Regions. While providing the Service to the Customer, Nosto uses third party service providers and subcontractors ("Sub-processors") located in USA. Therefore, it is necessary for Nosto to transfer Customer Data to Sub-processors based on either the Data Processing Agreements which incorporate the Standard Contractual Clauses or by abiding to the EU-USA Privacy Shield. By accepting the Terms of Use and / or the Order Form, the Customer authorizes Nosto to enter into the required Data Processing Agreement(s), including where applicable the Standard Contractual Clauses, with Sub-processors on behalf of the Customer. Nosto has implemented technical and organizational precautions defined in this DPA to protect the security and integrity of Customer Data processed by Nosto Infrastructure.

3.2 Application of Standard Contractual Clauses. The Standard Contractual Clauses will apply to Customer Data that is transferred, either directly or via onward transfer, to Sub-processor located in USA. The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply: if Sub-processor in question has adopted an alternative recognized compliance standard for the lawful transfer of personal data (such as Privacy Shield) outside the EEA.

4. SECURITY RESPONSIBILITIES OF NOSTO

4.1 Nosto is responsible for implementing and maintaining the technical and organizational measures for the Facilities as described in Schedule 2 (Nosto Security Standards) and Section 3.2 of Schedule 1 (Data Processing Terms) designed to help the Customer secure Customer Data against unauthorized processing and accidental or unlawful loss, access or disclosure.

4.2 The technical and organizational measures include the following:

(i) Nosto has implemented and will maintain measures to ensure the physical security of the Facilities as set out in Section 1.2. of Schedule 2 (Nosto Security Standards);

(ii) Nosto has implemented and will maintain measures to ensure the security of the Nosto Infrastructure as set out in Section 1.1 of Schedule2 (Nosto Security Standards);

(iii) Nosto has implemented and will maintain measures to control access rights for Nosto employees and contractors in relation to the Nosto Infrastructure as set out in Section 1.1 of Schedule2 (Nosto Security Standards). The Customer has implemented and will maintain measures to control access rights to Customer Data;

(iv) and Nosto will process Customer Data in accordance with the Customer's instructions as described in Section 2.5 of Schedule 1 (Data Processing Terms).

5. AUDIT RIGHTS

5.1 Nosto shall make available to the Customer all information necessary to demonstrate Nosto's compliance with its obligations set out in this DPA and in the Regulation.

5.2 Nosto will use its best endeavors to enter into contractual arrangements with Nosto's Sub-processors which entitle the Customer to contribute to audits, including inspections, with respect to Nosto Infrastructure. Notwithstanding the foregoing, the Customer acknowledges and agrees that Nosto cannot guarantee that the Customer will be entitled to audit Nosto's Sub-processors (or their Sub-processors) directly. Accordingly, upon the Customer's reasonable request (and at the Customer's sole cost) Nosto shall engage independent external auditors to audit that the processing of personal data within the Nosto Infrastructure complies with its data protection obligations. To prove compliance with its obligations, Nosto will provide the report to the Customer subject to a separate non-disclosure agreement. To the extent not covered by the independent audit reports, the Customer or the external auditor mandated by the Customer may audit Nosto's compliance with the data protection obligations under this DPA. For the sake of clarity, in no event shall Nosto's competitor be permitted to audit Nosto or the Nosto Infrastructure.

5.3 The Parties shall agree on the time and other details of the audit at least 30 business days in advance. The audit or inspection shall be conducted so that the time, work, costs and the inconvenience caused to Nosto's business is minimized (including but not limited to any inconvenience to Nosto's customers, partners, Sub-processors and vendors). Nosto's confidentiality obligations towards third parties shall be respected in the audit. The Customer's representatives and external auditors participating in the Audit shall sign separate confidentiality agreements.

5.4 Nosto shall correct any reported deficiencies without undue delay. Only if the audit reveals material deficiencies in Nosto's performance, Nosto shall bear its own costs for the audit.

6. SECURITY BREACH NOTIFICATION

6.1 If Nosto becomes aware of either (a) any unlawful access to any Customer Data stored on Nosto's equipment or in Nosto Infrastructure; or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Nosto will promptly: (a) notify the Customer of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

6.2 Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 6 (Security Breach Notification). An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of Nosto Infrastructure or Facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and

(ii) Nosto's obligation to report or respond to a Security Incident under this Section 6 (Security Breach Notification) is not and will not be construed as an acknowledgement by Nosto of any fault or liability of Nosto with respect to the Security Incident.

6.3 Notification(s) of Security Incidents, if any, will be delivered to one or more of the Customer's administrators by any means Nosto selects, including via email. It is the Customer's sole responsibility to ensure the Customer's administrators maintain accurate contact information on the Nosto management console at all times.

7. SUB-PROCESSING

7.1 Authorized Sub-processing. The Customer agrees that Nosto may use Sub-processors to fulfil its contractual obligations under this DPA and / or Order Form or to provide certain services on its behalf, such as support services. Schedule 3 (Data Processing Details) lists the Sub-processors that are currently authorized by Nosto to access Customer Data. Nosto will inform its Customers at least 14 days prior to authorizing or permitting any new Sub-processors to access Customer Data. The Customer hereby consents to Nosto's use of Sub-processors stated in Section 5 of Schedule1 (Data Processing Terms). Except as set forth in this DPA, or as the Customer may otherwise authorize, Nosto will not permit any Sub-processors to access Customer Data.

7.2 Sub-processors Obligations. When Nosto authorizes any Sub-processors as described in the above Section 5.1 of the Schedule 1 (Data Processing Terms):

7.2.1 Nosto will restrict the subcontractor's access to Customer Data only to what is necessary to maintain or to provide the Service to the Customer in accordance with the Order Form and Nosto will prohibit the Sub-processor from accessing Customer Data for any other purpose;

7.2.2 Nosto will impose appropriate contractual obligations in writing upon the subcontractor that are no less protective than this DPA, including relevant contractual obligations regarding confidentiality, data protection, data security and audit rights; and

7.2.3 Nosto will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processors that cause Nosto to breach any of Nosto's obligations under this DPA.

8. DUTY TO INFORM

Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Nosto, Nosto will inform the Customer without undue delay. Nosto will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is a) the Customer's property; b) the Customer’s responsibility; and c) that the Customer Data is at the Customer's sole disposition.

SCHEDULE 2

Nosto Security Standards

1. **Information Security Program.** Nosto will maintain an information security program in accordance with Article 32 of the GDPR (including the adoption and enforcement of internal policies and procedures) designed to (a) help the Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Nosto Infrastructure, and (c) minimize security risks, including through risk assessment and regular testing. Nosto will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   (a) the pseudonymization and encryption of personal data;

   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

1.1. **Security of Nosto Infrastructure**

1.1.1. **Data Centers**. All servers are hosted by Amazon Web Services ("AWS") which is among the biggest cloud computing providers and has a long track record running data centers reliably and securely. AWS manages data center infrastructure, physical security and continuity as a data center provider. For more details, please see the AWS security whitepaper. The Service is run in a virtual private cloud ("VPC") where access to each subsystem is limited with a firewall and accessing a subsystem requires a virtual private network ("VPN") connection with time-based one-time password ("TOTP") multi-factor authentication. Accessing the AWS resources via an API requires authentication to AWS Identity and Access Management ("IAM") with access key and secret access key. IAM authentication with a username and password requires TOTP multifactor authentication.

1.1.2. **Access to Nosto Infrastructure.** The Nosto Infrastructure Network will be accessible to Nosto Personnel, contractors and any other persons as necessary to provide the Services (such as Sub-processors). Nosto will maintain access controls as described above in Section 1.1.1. of this Schedule 2 (Nosto Security Standards) and policies to manage what access is granted to the Nosto Infrastructure from each network connection and for each user. Access permissions are granted only to those employees for whom access to the Nosto Infrastructure Network is necessary in order to perform their tasks.

1.1.3. **Auditing.** Audit logging of the Nosto Infrastructure is done on multiple levels, including activities performed by Nosto Personnel, Customers or system components. Attempts to modify audit configurations while the audit collection functions are active are logged. These logs are forwarded to a remote and centralized logging system where they can be monitored. Logs are saved in dedicated database cluster that is replicated for redundancy and availability. Configuration changes to AWS resources are tracked; these logs include detailed information about API calls to AWS resources.

1.2. **Physical Security**

1.2.1. **Physical Access Controls.** Access to Nosto facilities (the "**Facilities**") does not grant any access to the Nosto Infrastructure. Physical barrier controls are used to prevent unauthorized entrance to the Facilities. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Visitors at the Facilities are escorted by authorized employees or contractors.

1.2.2. **Unlimited Employee and Contractor Access.** Nosto provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to them, access privileges are promptly revoked, even if the employee or contractor continues to be an employee or contractor of Nosto or its affiliates.

1.2.3. **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Nosto also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including motion detection devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged.

2. Continued Evaluation. Nosto will conduct periodic reviews of the security of the Nosto Infrastructure and adequacy of its information security program as measured against industry security standards and its policies and procedures. Nosto will continually evaluate the security of its Nosto Infrastructure and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

SECTION 3

Data Processing Details

Subject matter of the processing	The subject matter of the data processing under this Addendum is the Customer Data.
Duration of the processing	As between Nosto and the Customer, the Customer (as controller) has the obligation to determine the duration of the data processing under this Addendum. After the end of the provision of the Services, the Customer shall either 1) delete the Customer Data using the controls available within the Service; 2) request for Nosto to delete the Customer Data; or 3) have the Customer Data returned by Nosto at the Customer's expense.
Nature of the processing	The Service analyzes the behavior of visitors in the Customer's Online Store in order to provide the visitors with meaningful purchase recommendations. Depending on the feature set used by the Customer, these recommendations may be displayed onsite or through emails or Facebook and Instagram.
Purpose of the processing	The purpose of the data processing under this Addendum is the provision of the Services initiated by the Customer.
Type of personal data	First name, last name, email address, user agent (browser), IP address, events, viewed products, order events, cart content, liked products, image files, disliked products, external campaign attributions, clicked recommendations, order information, phone number, zip code, country code and sent emails.
Categories of the data subjects	The data subjects are the Customer's customers.
Sub-processors	Amazon Web Services, Inc.