STORE DNA

Data Processor Statement

Monolith Retail Solutions, Inc.

Article 1. Definitions

1.1. In this Processor’s Statement, capitalized words and expressions, whether in single or plural, have the meaning specified as set out below:

Annex: appendix to this Processor’s Statement which forms an integral part of it;
Statement: the Subscription & Services Statement,
Personal Data: all information relating to an identified or identifiable natural person as referred to in Section 4(1) GDPR;
Process: as well as conjugations of this verb: the processing of Personal Data as referred to in Section 4(2) GDPR;
Processor’s Statement: the present statement;
Sub Processor: the sub-contractor hired by Processor, that Processes Personal Data in the context of this Processor’s Statement on behalf of the Controller, as referred to in Section 28(4) GDPR.

1.2. The provisions of the Statement apply in full to this Processor’s Statement. In case provisions with regard to the Processing of Personal Data are included in the Statement, the provisions of this Processor’s Statement prevail.

Article 2. Purpose of the Personal Data Processing

2.1. The Controller and the Processor have concluded the present Processing Statement for the Processing of Data in the context of the Statement. An overview of the type of Personal Data, categories of data subjects and the purposes of Processing, is included in Annex 1.

2.2. The Controller is responsible and liable for the processing of Personal Data in relation to the Statement and guarantees that Processing is in compliance with all applicable legislation. Controller will indemnify and hold harmless Processor against any and all claims of third parties, those of the data protection authority in particular, resulting in any way from not complying with this guarantee.

2.3. The Processor undertakes to Process Personal Data only for the purpose of the activities referred to in this Processor’s Statement. The Processor guarantees that it will not use the Personal Data which it Processes in the context of this Processor's Statement for its own or third-party purposes without the Controller's express written consent, unless a legal provision requires the Processor to do so. In such case, the Processor shall immediately inform the Controller of that legal requirement before Processing, unless that law prohibits such information on import grounds of public interest.

Article 3. Technical and organizational provisions

3.1. The Processor will, taking into account the nature of the Processing and insofar as this is reasonable possible, assist the Controller in ensuring compliance with the obligations pursuant to the GDPR to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These measures will guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, in view of the risks entailed by Personal Data Processing and the nature of the data to be protected. The Processor will in any case take measures to protect Personal Data against accidental or unlawful destruction, accidental or deliberate loss, forgery, unauthorized distribution or access, or any other form of unlawful Processing.

3.2. Processor will provide a document which describes the appropriate technical and organizational measures to be taken by the Processor. This document will be attached to this Processor's Statement as Annex 2.

Article 4. Confidentiality

4.1. The Processor will require the employees that are involved in the execution of the Statement to sign a confidentiality statement – whether or not included in the employment statement with those employees – which in any case states that these employees must keep strict confidentiality regarding the Personal Data.

Article 5. Personal Data Processing outside Europe

5.1. The Processor will only be permitted to transfer Personal Data outside the European Economic Area if this is done in compliance with the applicable statutory obligations.

Article 6. Sub-processors

6.1. The Processor is entitled to outsource the implementation of the Processing on the Controller's instructions to Sub-processors, either wholly or in part, which parties are described in Annex 3. In case the Processor wishes to enable Sub-processors, the Processor will inform Controller of any intended changes concerning the addition or replacement of other processors. The Controller will to object to such changes within 10 (ten) working days. The Processor will respond to the objection within 10 (ten) working days.

6.2. Processor obligates each Sub-processors to contractually comply with the confidentiality obligations, notification obligations and security measures relating to the Processing of Personal Data, which obligations and measures must at least comply with the provisions of this Processor's Statement.

Article 7. Liability

7.1. With regard to the liability and indemnification obligations of Processor under this Processor's Statement the stipulation in the Statement regarding the limitation of liability applies.

7.2. Without prejudice to article 9.1 of this Processor's Statement, Processor is solely liable for damages suffered by Controller and/or third party claims as a result of any Processing, in the event the specific obligations of Processor under the GDPR are not complied with or in case the Processor acted in violence of the legitimate instructions of the Controller.

Article 8. Personal Data Breach

8.1. In the event the Processor becomes aware of any incident that may have a (significant) impact on the protection of Personal Data, i) it will notify the Controller without undue delay and ii) will take all reasonable measures to prevent or limit (further) violation of the GDPR.

8.2. The Processor will, insofar as reasonable, provide all reasonable cooperation requested by the Controller in order for Controller to comply with its legal obligations relating to the identified incident.

8.3. The Processor will, insofar as reasonable, assist the Controller with the Controller's notification obligation relating to the Personal Data to the Data Protection Authority and/or the data subject, as meant in Section 33(3) and 34(1) GDPR. Processor is never held to report a personal data breach with the Data Protection Authority and/or the data subject.

8.4. Processor will not be responsible and/or liable for the (timely and correctly) notification obligation to the relevant supervisor and/or data subjects, as meant in Section 33 and 34 GDPR.

Article 9. Cooperation

9.1. The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to respond to requests for exercising rights of data subjects, in particular the right of access (Section 15 GDPR), rectification (Section 16 GDPR), erasure (Section 17 GDPR), restriction (Section 18 GDPR), data portability (Section 20 GDPR) and the right to object (Section 21 and 22 GDPR). The Processor will forward a complaint or request from a data subject with regard to the Processing of Personal Data to the Controller as soon as possible, as the Controller is responsible for handling the request.

9.2. The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to carry out a data protection impact assessment (Section 35 and 36 GDPR).

9.3. The Processor will provide the Controller with all the information reasonably necessary to demonstrate that the Processor fulfills its obligations under the GDPR. Furthermore, the Processor will – at the request of the Controller – enable and contribute to audits, including inspections by the Controller or an auditor that is authorized by the Controller. In case the Processor is of the opinion that an instruction relating to the provisions of this paragraph infringes the GDPR or other applicable data protection legislation, the Processor will inform the Controller immediately.

9.4. The Processor is entitled to charge any costs associated with Cooperation with the Controller.

Article 10. Termination and miscellaneous

10.1. With regard to the termination under this Processor’s Statement the specific provisions of the Statement apply. Without prejudice to the specific provisions of the Statement, the Processor will, at the first request of the Controller, delete or return all the Personal Data, and delete all existing copies, unless the Processor is legally required to store (part of) the Personal Data.

10.2. The Controller will adequately inform the Processor about the (statutory) retention periods that apply to the Processing of Personal Data by the Processor.

10.3. The obligations laid down in this Processor’s Statement which, by their nature, are designed to continue after termination will remain in force also after the termination of this Processor’s Statement.

10.4. The choice of law and competent court comply with the applicable provisions of the Statement.

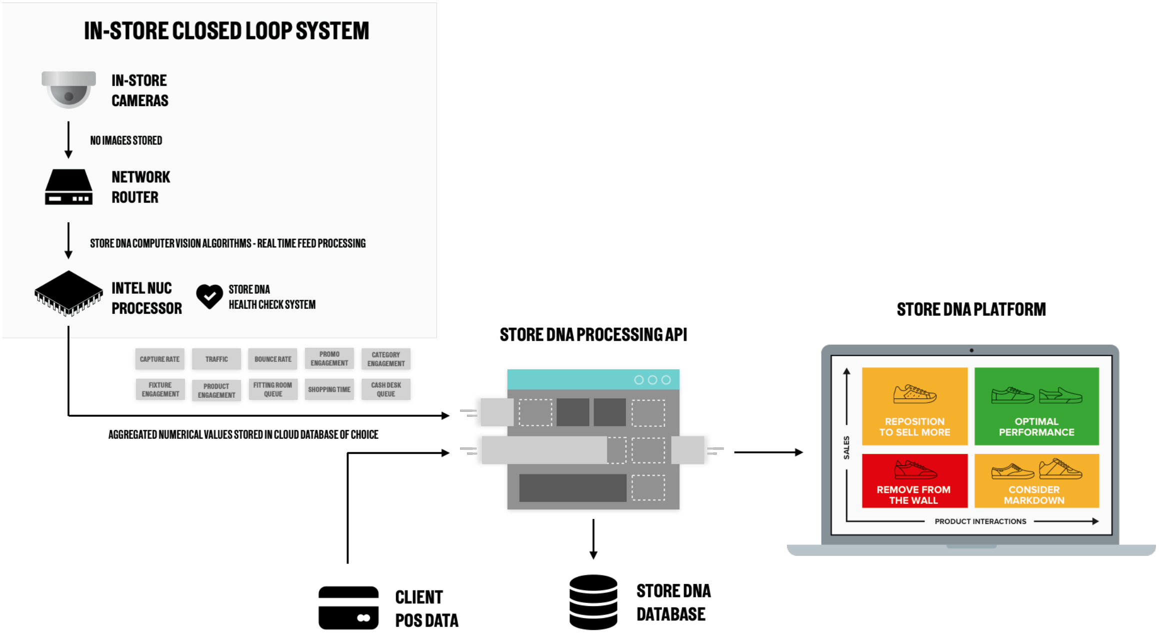
ANNEX 1 OVERVIEW PERSONAL DATA

The Processor under this Statement confirms that it does not store **ANY** personally identifyable data.

Data handled by the Processor are as follows:

- Capture rate,
- Traffic,
- Shopping time,
- Bounce rate,
- Shopping paths,
- Window / Promo / Category / Fixture / Product engagement,
- Fitting room / Cash desk queue,
- Demographics (gender / age ratios),

are handled in the in-store closed loop systems according to below scheme, and are thus not related to personally indetifyable data.



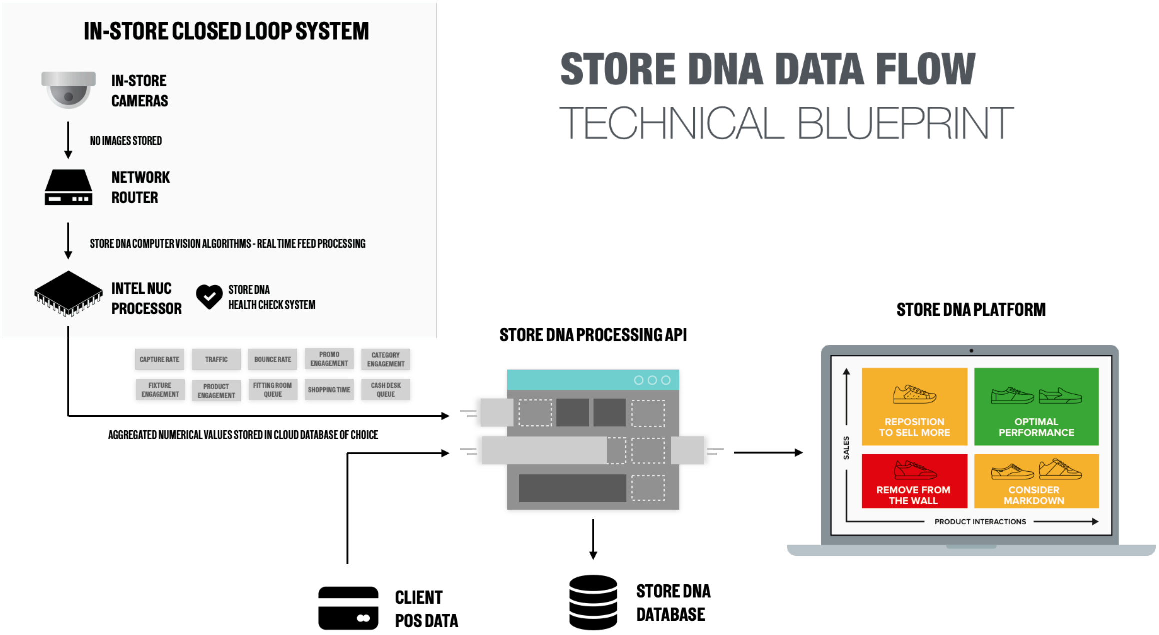
ANNEX 2 SPECIFICATION OF THE SECURITY MEASURES

All data handled by the Processor is stored and processed on-premise, within Client's network. Processor handles further the data using OpenVPN through specified whitelisted IP addresses. Point-to-point connections including camera streams, API calls and other requests use Transport Layer Security (HTTPS) secure protocol which ensures all data sent in the network is encrypted.

All hardware procured or approved by the Processor is running the latest firmware updates and enabled authentication to limit access only to the Processor. Cameras and other sensors mounted in the store are part of a closed loop system, including the which is located in (IT) room with physical security (locked door).

Processor’s in-store platform sends metadata about CPU/RAM usage and health checks to Processor’s health check system. This is done in order to provide high uptime and availability of the system. The in-store installation comes with equipped routers which can detect system/network issues and restart machines automatically (self-healing).

Schematic overview of the system composition and data flow for Processor’s system, followed by the Technology Requirements for the installation are as below.


STORE DNA DATA FLOW
TECHNICAL BLUEPRINT
IN-STORE CLOSED LOOP SYSTEM
IN-STORE CAMERAS
NO IMAGES STORED
NETWORK ROUTER
STORE DNA COMPUTER VISION ALGORITHMS - REAL TIME FEED PROCESSING
INTEL NUC PROCESSOR
STORE DNA HEALTH CHECK SYSTEM
CAPTURE RATE
TRAFFIC
BOUNCE RATE
PROMO ENGAGEMENT
CATEGORY ENGAGEMENT
FIXTURE ENGAGEMENT
PRODUCT ENGAGEMENT
FITTING ROOM QUEUE
SHOPPING TIME
CASH DESK QUEUE
AGGREGATED NUMERICAL VALUES STORED IN CLOUD DATABASE OF CHOICE
STORE DNA PROCESSING API
STORE DNA PLATFORM
SALES
REPOSITION TO SELL MORE
OPTIMAL PERFORMANCE
REMOVE FROM THE WALL
CONSIDER MARKDOWN
PRODUCT INTERACTIONS
CLIENT POS DATA
STORE DNA DATABASE