PRIVACY POLICY REGARDING THE PROCESSING OF PERSONAL DATA OF NEW FASHION JSC

1. General provisions

1.1. This Privacy Policy regarding the processing of personal data (the "Policy") defines the general principles of and procedure for processing personal data (PD) and measures to ensure the security thereof at New Fashion Joint-Stock Company (OGRN (Primary State Registration Number) 1027700429690, INN (Taxpayer Identification Number) 7707099460) having its registered address at 10 Presnenskaya Embankment, 123112 Moscow (the "Company").

1.2. The objective of this Policy is to ensure the protection of the rights and freedoms of a person and a citizen in the course of processing his/her personal data, including protection of the rights to privacy and personal and family secrets, strict and unswerving compliance with the laws of the Russian Federation and international treaties of the Russian Federation in the field of personal data.

1.3. This Policy has been developed subject to the requirements of the Constitution of the Russian Federation, in accordance with Federal Law No. 152-FZ "On Personal Data" dated 27 July 2006 (Federal Law No. 152-FZ), Federal Law No. 149-FZ "On Information, Information Technologies and the Protection of Information" dated 27 July 2006, and other federal laws and regulations defining the cases and specifics of PD processing.

1.4. The following terms and definitions are used in this Policy:

- **automated PD** processing shall mean PD processing using computer hardware;
- **biometric PD** shall mean information describing the physiological and biological characteristics of a person, based on which his/her identity can be established and which are used by the processor to establish the identity of the PD subject;
- **PD blocking** shall mean temporary cessation of PD processing (except where processing is necessary to clarify PD);
- **data centre** shall mean a specialised organisation providing services for hosting server and network equipment, leasing out servers (including virtual ones), as well as Internet connection;
- **access to PD** shall mean familiarisation by certain persons (including employees) with PD of subjects, which are processed by the Company, subject to maintaining the confidentiality of this information;
- **PD information system** shall mean a set of PD contained in databases and information technologies and technical means that ensure the processing of the same;
- **counterparty** shall mean a party to an agreement with the Company that is not an employee of the Company;
- **PD confidentiality** shall mean the obligation of persons who have gained access to PD not to disclose the same to third parties and not to disseminate PD without the consent of the PD subject, unless otherwise provided for by law;
- **cloud computing infrastructure** shall mean a shared pool of configurable computing resources (data networks, servers, storage devices, applications and services, either individually or collectively) that are widely and conveniently accessible over a network on demand and can be made available quickly and with minimal operational costs or service provider interaction, and that have five key features: on-demand self-service; broad network access; resource pooling; rapid elasticity; measured services;
- **PD processing** shall mean any action (operation) or set of actions (operations) performed with PD, with or without the use of automation tools, including collection, recording, systematisation, accumulation, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, access to), blocking, deletion, destruction of PD;
- **processor** shall mean a government agency, a municipal authority, a legal entity or an individual that, independently or jointly with other persons, arranges and/or exercises PD processing, as well as determines the purposes of PD processing, the scope of PD subject to processing, and the actions (operations) performed with PD; in this Policy, processor shall mean the Company, unless specifically stated otherwise;
- **personal data (PD)** shall mean any information related to a directly or indirectly identified or identifiable individual (PD subject);
- **PD permitted for dissemination by the PD subject** shall mean PD, access to which by an unlimited range of persons is granted by the PD subject by way of giving consent to PD processing permitted by the PD subject for dissemination in the manner prescribed by Federal Law No. 152-FZ;
- **provision of PD** shall mean actions aimed at disclosing PD to a specific person or a specific group of persons;

- **dissemination of PD** shall mean actions aimed at disclosing PD an indefinite range of persons;
- **Roskomnadzor** shall mean the Federal Service for Supervision of Communications, Information Technology and Mass Media, which is an authorised federal executive body responsible for protecting the rights of PD subjects;
- **special categories of PD** shall mean information related to race, nationality, political views, religious or philosophical beliefs, health status;
- **PD subject** shall mean an individual to whom PD are attributable;
- **cross-border transfer of PD** shall mean transfer of PD to the territory of a foreign state to a foreign government agency, a foreign individual, or a foreign legal entity;
- **destruction of PD** shall mean actions, as a result of which it becomes impossible to restore the content of PD in the PD information system and/or as a result of which the tangible media containing PD are destroyed;
- **cookies** shall mean mainly small text files that are stored on a user's PC, tablet, mobile phone, or other device, which contain information about their previous actions on a website.

1.5. The PD subject shall have the right to:

1.5.1. Receive information regarding the processing of his/her PD.

1.5.2. Demand that the Company stop processing his/her PD, clarify, block, or destroy the same, if PD are incomplete, outdated, inaccurate, unreliable, illegally obtained, or are not required for the stated purpose of processing, as well as may take measures provided for by law to protect his/her rights.

1.5.3. Revoke his/her consent to the processing of PD by the Company at any time.

1.6. The Company's obligations:

1.6.1. The Company is required to provide the PD subject or his/her representative with the information stipulated by the applicable law.

1.6.2. In the event that unlawful PD processing is detected upon application by a PD subject or his/her representative or at the request of a PD subject or his/her representative or Roskomnadzor, the Company is required to block the unlawfully processed PD attributable to that PD subject or ensure that the same are blocked (if the PD are being processed by another person acting on behalf of the processor) immediately after such application or request for the verification period.

1.6.3. In the event that inaccurate PD are discovered upon application by a PD subject or his/her representative or at their request or at the request of Roskomnadzor, the processor is required to block the PD attributable to that PD subject or ensure that the same are blocked (if the PD are being processed by another person acting on behalf of the processor) immediately after such application or request for the verification period, unless blocking the PD is in violation of the rights and legitimate interests of the PD subject or third parties.

1.6.4. In the event that the fact of PD inaccuracy is confirmed, the processor, based on information provided by the PD subject or his/her representative or Roskomnadzor, or other necessary documents, is required to clarify the PD or ensure that the same are clarified (if the PD are being processed by another person acting on behalf of the processor) within seven (7) business days from the date of submission of such information and unblock the PD.

1.6.5. In the event that unlawful PD processing by the processor or a person acting on behalf of the processor is detected, the processor is required, no later than three (3) business days from the date of such detection, to terminate the unlawful PD processing or ensure that the unlawful PD processing is terminated by the person acting on behalf of the processor. In the event that lawful PD processing cannot be ensured, the processor is required, no later than ten (10) business days from the date of detection of the unlawful PD processing, to destroy such PD or ensure that the same are destroyed. The processor is required to notify the PD subject or his/her representative of the rectification of the violations committed or of the PD destruction, and in the event that the application of the PD subject or his/her representative or the request of Roskomnadzor has been sent by Roskomnadzor, the specified authority as well.

1.6.6. The Company shall assess and document, in accordance with the requirements established by Roskomnadzor, the damage that may be caused to PD subjects in the event of a violation of Federal Law No. 152-FZ in order to correlate the said damage and the measures taken by the Company aimed at ensuring the fulfilment of the obligations stipulated by Federal Law No. 152-FZ.

2. PD Processing Principles

2.1. The Company shall process PD in accordance with the following principles:

2.1.1. Lawful and fair basis for PD processing. The Company shall take all necessary measures to comply with the requirements of law, shall not process PD where this is not permitted by law and is not required to achieve the purposes set by the Company, and shall not use PD to the detriment of PD subjects.

2.1.2. Limiting PD processing to achieving specific, predetermined, and legitimate purposes.
2.1.3. Processing only those PD that meet the previously stated purposes of processing the same; correspondence of the content and scope of PD being processed to the stated purposes of processing; prevention of PD processing that is incompatible with the purposes of collecting PD, as well as excessive PD in relation to the stated purposes. The Company shall not collect or process PD that are not required to achieve the purposes specified in this Policy and shall not use PD of subjects for any purposes other than those specified.
2.1.4. Preventing the merging of databases containing PD processed for purposes that are incompatible with each other.
2.1.5. Ensuring the accuracy, sufficiency, and relevance of PD in relation to the purposes of PD processing. The Company shall take all reasonable measures to maintain the relevance of PD being processed, including, but not limited to, the exercise of the right of each subject to receive their PD for review and to demand that the Company clarify, block, or destroy the same if the PD are incomplete, outdated, inaccurate, illegally obtained, or are not required for the processing purposes stated above without explaining the reasons for such a requirement.
2.1.6. Storing PD in a form that allows identifying the PD subject for no longer than required by the PD processing purposes, unless the PD storage period is established by federal law, an agreement, to which the PD subject is a party, a beneficiary, or a guarantor.
2.1.7. Destroying PD upon achieving the stated purposes of the processing thereof or in the event of loss of the need to achieve these purposes, if the Company is unable to rectify the violations of the PD processing procedure established by law, the PD subject withdraws the consent to processing, the PD processing period established by the consent to PD processing expires, unless otherwise provided by law.

3. PD Processing Purposes

3.1. The purposes of PD processing, the categories and list of PD being processed, the categories of subjects whose PD are being processed, the methods and terms of their processing and storage, the procedure for destroying PD upon achieving the purposes of processing the same or upon occurrence of other legal grounds are defined in **Appendix 1** to this Policy.

4. PD Processing Procedure and Terms

4.1 The Company shall carry out:
- non-automated PD processing;
- automated PD processing with or without the transfer of the received information via information and telecommunications networks;
- mixed PD processing.

4.2 PD processing may include, among other things, collection, recording, systematisation, accumulation, storage, clarification (updating, modification), extraction, use, transfer (provision, access, distribution), blocking, deletion, destruction.
4.3 The Company may process PD in the following cases:
4.3.1 With the consent of the PD subject to the processing of his/her PD.
4.3.2 PD processing is necessary to achieve the objectives stipulated by an international treaty of the Russian Federation or by law, to implement and perform the functions, powers, and duties imposed on the processor by the laws of the Russian Federation.
4.3.3 PD processing is necessary to perform an agreement, to which the PD subject is a party, a beneficiary, or a guarantor, as well as to enter into an agreement at the initiative of the PD subject or an agreement whereunder the PD subject will be a beneficiary or a guarantor.
4.3.4 PD processing is necessary to exercise the rights and legitimate interests of the processor or third parties, or to achieve socially significant goals, provided that the rights and freedoms of the PD subject are not violated.
4.3.5 PD are processed that are subject to publication or mandatory disclosure in accordance with federal law.
4.4 The Company shall not disclose PD to third parties without the consent of the PD subject, unless otherwise provided by law.
4.5 The Company shall disseminate PD based on a separate consent to PD processing. Consent to the processing of PD permitted for dissemination by the PD subject shall be drawn up separately from other consents of the PD subject to the processing of his/her PD.

4.6 PD shall be provided (transferred) to governmental authorities, including inquiry and investigation agencies, the Federal Tax Service, the Pension Fund of the Russian Federation, the Social Insurance Fund, and other authorised executive authorities in accordance with the legal requirements of the Russian Federation.
4.7 The Company shall not process biometric PD.
4.8 When collecting PD, among other things, via the Internet, the Company shall ensure the recording, systematisation, accumulation, storage, clarification (updating, modification), and extraction of PD using databases located on the Company's premises (in the Russian Federation) and in data centres on the territory of the Russian Federation.
4.9 The Company may carry out cross-border transfer of PD in accordance with the procedure established by the applicable law, subject to compliance with the requirements of Article 12 of Federal Law No. 152-FZ.
4.10 The processor shall process information about the user of the processor's websites (obtained using cookies and technical data collection services) for the purposes specified in Appendix 1 to this Policy.
4.11 The processor shall not compare and/or combine (link) the technical information of the website user with PD and/or other information at the processor's disposal.
4.12 Destruction of PD must exclude the possibility of restoration of the same using software or physical methods.
4.13 The PD destruction procedure is defined in Appendix 1 to this Policy. The fact of PD destruction shall be confirmed in accordance with the requirements established by Roskomnadzor.

5. PD Confidentiality

5.1. The Company's employees who have access to PD must ensure the confidentiality of such data.
5.2. The Company may, with the consent of the PD subject, assign PD processing to another person, unless otherwise provided by law, under an agreement to be entered into with this person, which provides for an obligation of the person processing PD on behalf of the Company to comply with the PD processing principles and rules and processing requirements prescribed by law as a material condition. The processor's assignment must be in compliance with all requirements stipulated by para. 3 of Article 6 of Federal Law No. 152-FZ.
5.3. The Company may host its PD information systems in a data centre (cloud computing infrastructure). In this case, the agreement with the data centre (cloud service provider) may include a requirement to prohibit access by data centre personnel to the Company's PD information systems hosted in the data centre (cloud computing infrastructure) as a material condition.

6. Consent of the PD Subject to the Processing of His/Her PD

6.1. The PD subject shall decide on whether to provide his/her PD to the Company and give consent to the processing of the same freely, of his/her own free will, and in his/her own interests. The consent to PD processing must be specific, objective, informed, conscious, and unambiguous and may be provided by the PD subject in any form that allows confirmation of the receipt thereof, unless otherwise established by law.
6.2. To the extent stipulated by federal law, PD processing shall only be effected with the written consent of the PD subject. Consent in the form of an electronic document signed with an electronic signature in accordance with the laws on electronic signature shall be equivalent to written consent on paper containing the handwritten signature of the PD subject.
6.3. The consent of PD subjects to the provision of their PD is not required when the Company receives, within the framework of its established powers, reasoned requests from prosecution authorities, law enforcement agencies, investigative and inquiry agencies, security agencies, public labour inspectors when they exercise public supervision and monitoring of compliance with labour laws, and other authorities having the powers to request information, as provided by law.

7. Information on Measures Taken to Protect PD

7.1. The security of PD being processed by the Company shall be ensured by adoption of legal, organisational, and technical measures necessary and sufficient to ensure compliance with the legal requirements for PD protection.
7.2. Legal measures to be taken by the Company include:
- developing the Company's in-house policies and procedures implementing legal requirements, including the Company's PD Processing and Security Policy and Regulations;
- The Company's employees who have access to PD must ensure the confidentiality of such data.

7.3. Organisational measures to be taken by the Company include:

- appointing a person responsible for arranging PD processing;
- appointing a person responsible for ensuring PD security in PD information systems;
- limiting the range of the Company's employees who have access to PD and organising a permit system for accessing the same;
- ensuring that the Company's employees directly involved in PD processing familiarise themselves with the rules of personal data laws, including the PD protection requirements, this Policy, and other in-house policies and procedures of the Company on PD processing;
- training all categories of the Company's employees directly involved in PD processing in the rules for handling PD and ensuring the security of PD being processed;
- defining the responsibilities for ensuring the PD processing security and the liability for violating the established procedure in the job descriptions of the Company's employees;
- regulating PD processing processes;
- keeping records of and storing tangible media containing PD, preventing theft, substitution, unauthorised copying, and destruction;
- identifying the type of threats to PD security that are relevant for PD information systems, taking into account the possible damage to PD subjects that may be inflicted if security requirements are breached, determining the PD protection level and requirements for PD protection during the processing thereof in information systems, which, if implemented, ensure the established PD protection levels;
- identifying threats to PD security when PD are being processed in information systems and generating a private model (models) of current threats based on the same;
- accommodating technical means for PD processing within a protected area;
- restricting access by unauthorised persons to the Company's premises, preventing them from being in premises where PD are being processed and technical means for PD processing are accommodated without supervision by the Company's employees.

7.4. Technical measures to be taken by the Company include:

- developing a PD protection system based on a model of current threats for the PD protection levels established by the Government of the Russian Federation when processing PD in information systems;
- using information security tools that have passed a compliance assessment procedure to neutralise current threats;
- evaluating the efficiency of measures taken to ensure PD security;
- implementing a permit system for employee access to PD in information systems and to hardware and software tools for information protection;
- keeping records of any actions involving PD by users of information systems where PD are being processed;
- restricting the software environment;
- detecting malicious software (using antivirus software) in the Company's information network nodes that provide for the appropriate technical capabilities;
- secure inter-network interaction (using firewalling);
- identifying and verifying the user's authenticity (authentication) when logging into the information system;
- monitoring software continuity, including software for information security tools;
- detecting intrusions into the Company's information system that violate or create preconditions for violation of established PD security requirements;
- protecting the virtualisation environment;
- taking measures to detect, prevent, and eliminate the consequences of computer attacks on PD information systems and to respond to computer incidents therein;
- protecting network devices and communication channels, through which PD are transferred;
- recovering PD modified or destroyed due to unauthorised access to the same (creating a PD backup and recovery system).

7.5. When hosting an information system in a data centre (cloud computing infrastructure), some of the security measures may be taken by the data centre (cloud service provider), which shall be reflected in the agreement between the Company and the data centre (cloud service provider).

8. Final Provisions

8.1. Other rights and obligations of the Company as a PD processor and a person that are processing PD on behalf of other processors are determined by the PD processing laws of the Russian Federation.

8.2. The Company's officers and employees guilty of violating the rules governing PD processing and protection shall bear financial, disciplinary, administrative, civil, and criminal liability in accordance with the laws of the Russian Federation.

8.3. This Policy shall be revised as necessary. This Policy must be revised in the event of significant changes in international or Russian laws on PD processing.

When making amendments to the Policy, the following shall be taken into account:

- changes in the information infrastructure and/or the information technologies used by the Company;
- the practice of PD processing law enforcement established in the Russian Federation;
- changes in the terms and features of PD processing in connection with the introduction of new information systems, processes, and technologies into its operations.

8.4. In compliance with the requirements of para. 2 of Article 18.1 of Federal Law No. 152-FZ, this Policy shall be posted freely available on all pages of the processor's websites (or websites used by the processor), which are used for collecting PD.

Appendix to the Privacy Policy

No.	Processing purpose	Categories and list of personal data to be processed	Categories of subjects	Legal basis	Processing method	Processing and storage period	Destruction procedure
1.	Researching own customer preferences to improve product and service quality	• Surname, name • City • Age • Shopping preferences • Contact phone number • Preferred communication method • Other details specified in the questionnaire	Customers and other persons who took part in the research	• Customers' consent to the processing of personal data for marketing communications	Automated	Throughout the validity of the consent to the processing of personal data for marketing communications	Removal from information systems
2.	Newsletter subscription	• Contact email address	Buyers and other persons who provided the consent to marketing communications	• Customers' consent to the processing of personal data for marketing communications	Automated	Throughout the validity of the consent to the processing of personal data for marketing communications	Removal from information systems
3.	Receiving and reviewing requests and claims, providing customer support	• Surname, name, patronymic • Contact email address and phone number • City • Delivery address • Call audio recording • Nicknames in social networks • Service rating Information • Other data specified in messages • Correspondence history	Consumers and other persons who contact the customer service	• Compliance with consumer protection laws • Ensuring the Company's rights and legitimate interests	Mixed	No more than 3.5 years since the date of appeal	Removal from information systems, destruction of tangible media (shredder and other methods)
3.1.	Submitting requests via the feedback form	• Name • Contact email address and phone number • City • Other data specified in request	Buyers and other persons who contact the customer service	• Compliance with consumer protection laws • Ensuring the Company's rights and legitimate interests	Automated	No more than 3.5 years since the date of appeal	Removal from information systems

3.2.	Sending messages to the chatbot in Telegram and by email (call centrer)	• Name • Contact phone number • Other data specified in messages • Service rating Information • Correspondence history	Buyers and other persons who contact the customer service	• Compliance with consumer protection laws • Ensuring the Company's rights and legitimate interests • Answers to queries on product search, size, availability in stores and other characteristics	Automated	No more than 3.5 years since the date of appeal	Removal from information systems
4.	Behavior analytics to improve customer experience based on partner merchants' websites to improve service levels and optimise placement of digital advertising materials	• Surname, name, patronymic • Registration number • Contact email address and phone number • System IDs, including pixel and web analytics system IDs • Subscription information • Cookies • Nicknames in social networks	Website visitors and social media users	• Fulfilling an agreement	Automated	No more than 1 year since the date of the last website visit	Removal from information systems
5.	Publishing marketing materials aimed at promoting products and information about the Company's activities, ensuring public relations	• Surname, name, patronymic • Information about activities • City • Contact email address and phone number • Nicknames in social media • Photos and videos	Influencers	• Fulfilling an agreement with a counterparty • Consent to the processing of personal data	Automated	Throughout the validity of the consent the dissemination (conditions and prohibitions are not established by the subjects); for other processing, during the term of the agreement and 5 years upon fulfilment of obligations under the agreement	Removal from information systems
6.	Arranging filming, preparing and producing advertising materials, publishing materials offline and online	• Surname, name, patronymic • Photos and videos • Date of birth • ID document details	Representatives of the Company's counterparties (models)	• Consent to the use of image • Fulfilling an agreement with a counterparty • Consent to the processing of personal data	Mixed	throughout the validity of the consent of the use of image and the consent to the dissemination (conditions and prohibitions are not established by the subjects); for other	Removal from information systems, destruction of tangible media (shredder and other methods)

						processing, during the term of the agreement and 5 years upon fulfilment of obligations under the agreement	
7.	Recruiting and approving candidates for vacant positions, forming a candidate pool	• Surname, name, patronymic • Age • Nationality • Work experience details • Contact details • Employment preference information • Information from CV and otherwise additionally communicated to the Company For online application: • Surname, name, patronymic • Age • Contact details • Employment preference information • Other information that may be additionally communicated to the Company	Applicants	• Applicant's consent to the processing of personal data • Necessity of processing for recruitment purposes • Necessity of processing for entering into an employment contract • Fulfilling agreements with a counterparty (recruitment websites and career agencies), providing a legal basis for processing • Necessity of processing for forming a candidate pool	Mixed	For 3 years from the date of submission of the applicant's CV or application for a vacant position	Removal or depersonalisation from information systems, destruction of tangible media (shredder and other methods)
8.	Drafting and entering into an employment contract, a civil-law contract	• Surname, name, patronymic • Gender • Date and place of birth • Nationality • Residence address • Contact email addresses and phone number • Information from documents required for employment in accordance with Article 65 of the Labour Code of the Russian Federation • Photo	Applicants	• Necessity of processing for entering into a contract • Compliance with labour, accounting and tax accounting, and social insurance laws	Automated	For 1 year from the date of submission of the applicant's CV for a vacant position (unless a contract has been entered into)	Removal from information systems
9.	Conducting due diligence procedures in relation to potential counterparties of the Company	• Surname, name, patronymic • Information on positions held and participation in companies • ID document details (if applicable)	Representatives of counterparties, counterparties	• Compliance with the requirements of tax laws	Automated	During the term of the agreement and for 5 years from the date of completion	Removal from information systems

10.	Interaction with counterparties, inter alia, entering into, fulfilling, and terminating agreements, keeping records of engaged counterparties, settlements under agreements, ensuring communications on entering into, fulfilling, and terminating agreements, outsourcing functions	• Surname, name, patronymic • Position and business unit • Corporate email address and phone number • Description of services rendered	Counterparties, representatives and other employees of counterparties	• Fulfilling agreements with counterparties, providing a legal basis for personal data processing • Ensuring the Company's rights and legitimate interests	Mixed	During the term of the agreement and for 5 years upon fulfilment of obligations under the agreement	Removal from information systems, destruction of tangible media (shredder and other methods)
11	Placing an order	• Surname, name • Contact phone number • Contact email • address • Order details • Date of birth (optional) gender (optional) see purpose No. 3	Buyers	Entering into and fulfilling agreements	Automated	Throughout the term of using the website (mobile app), and no more than for 5 years from the date of the last sign-in	Removal from information systems

12	Accepting payments for orders, provision of additional services (order confirmation, tracking, personal account)	• Surname, name, patronymic • Contact phone number • Contact email address	Buyers	Fulfilling an agreement	Mixed	No more than 5 years since order completion date	Removal from information systems, destruction of tengible media (shredder and other methods)