STILLFRONT
GROUP

Data Protection and Privacy Policy

Classification code: Internal

Version: 2.1

Valid from: 2020-09-02

Table of Contents

1. Introduction

Each individual is entitled to protection of its personal integrity, which includes a number of rights and freedoms determined in various legislations. The right to protect the integrity of personal data is generally referred to as the right to data privacy. Everyone's right to data privacy is secured through a rigorous legal framework of rules and principles applicable throughout the entire lifecycle of the personal data. Moreover, the legal framework protects and ensures certain rights granted to individuals to make sure the individual is in control of its personal data and that any measures taken with personal data is conducted in a transparent manner.

The purpose of this Data Protection and Privacy Policy (this "**Policy**") is to, on a high level, outline how Stillfront Group AB (publ) and its subsidiaries ("**Stillfront**", or the "**Group**") shall process Personal Data when conducting its business to comply with applicable data protection laws. Moreover, this Policy describes which core measures that shall be observed to protect and maintain the fundamental rights and freedoms pertaining to data privacy.

2. Definitions

Unless otherwise stated, the capitalized terms used in this Policy shall have the same meaning as set forth in the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**").

3. Scope of this Policy

This Policy applies for all processing activities of Personal Data carried out within the Stillfront Group, either when such processing activities is carried out by an entity as a Controller, Processor and/or Joint Controller. All processing activities carried out by the Stillfront Group shall comply with this Policy and applicable data protection laws. To the extent the same Personal Data is processed by more than one legal entity, such entities shall ensure that the roles and responsibilities under applicable data protection laws are identified and regulated as appropriate.

This Policy aims to set forth a supplementary framework to applicable data protection laws. Processing of Personal Data in accordance with this Policy does not, however, automatically imply that the processing of Personal Data complies with applicable data protection laws.

For the avoidance of doubt, this Policy sets forth a minimum level to be considered when processing Personal Data and shall apply to processing activities subject to the GDPR. If a Group company conducts business which falls outside the scope of the GDPR, any other applicable data protection laws must be complied with. Applicable data protection laws will take precedence if it conflicts with this Policy, or it has stricter requirements than this Policy.

4. Fundamental Principles for Processing of Personal Data

The GDPR states a number of fundamental principles that Stillfront always needs to comply with when processing Personal Data. These fundamental principles form the main core of the GDPR and apply for all processing activities carried out by the subsidiaries.

The fundamental principles include:

- lawfulness - Personal Data shall be processed in a lawful, fair and transparent manner in relation to the data subject;
- purpose limitation - Personal Data shall only be processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- data and storage minimization - Personal Data shall only be processed and stored if necessary to fulfil the purposes for which the Personal Data was collected;
- accuracy - Personal Data shall be accurate, complete and, where necessary, up to date);
- security - Personal Data shall be protected and processed in a secure way; and
- accountability - each Group company shall be able to demonstrate compliance with applicable regulations relating to processing of Personal Data when acting as a data controller.

5. Legal Grounds for Processing of Personal Data

When a Group company processes Personal Data as a data controller, that Group company must be able to state the legal basis that the processing of Personal Data relies on. Processing of Personal Data may not be carried out if a group company has no legal basis for the processing. Personal Data may only be processed where it meets one of the following lawful conditions:

- the data subject has given consent to the processing of his/her Personal Data for one or more specific purpose - in order to be valid, a consent shall be unambiguous and freely given by the data subject, on the basis of correct information to make sure that the data subject has been able to understand the extent of the consent;
- processing is necessary for performance or execution of a contract to which the data subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract - this legal ground only comprises contracts with the data subject and not the performance or execution of contracts in general;
- processing is necessary for compliance with a legal obligation to which the data controller is subject - such legal obligation must be established in applicable EU-member state law or in EU law to which the Controller is subject;
- processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data, in particular where the data subject is a child.

Moreover, a group company shall only process special categories of data (cf. article 9 of the GDPR) if the data subject has given its consent to the processing or otherwise if the processing is explicitly authorized under applicable data protection laws.

STILLFRONT GROUP

Criminal data (cf. article 10 of the GDPR) shall only be processed by a group company if explicitly authorized by applicable data protection laws.

6. Security and Incident Management

Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Each group company must ensure sufficient security of processing Personal Data by implementing technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate are as follows:

- the pseudonymisation and/or encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

All personnel have an obligation to report data protection breaches to the DPO and the General Counsel by writing on following email: dpo@stillfront.com. This will allow the DPO/legal team to investigate further and take the appropriate steps to attend the issue in a timely manner. Please see the Data Breach Procedure for further information.

7. Rights of the Data Subjects

As an important step in Stillfront's ambition to process Personal Data with a high standard of protection and in compliance with applicable legislation, each Group company shall at all times observe the various rights that are afforded to the data subjects under applicable data protection laws. Thus, each Group company shall take both technical and organizational measures in order to ensure that there are routines in place to manage requests from data subjects, in relation to the exercise of the following rights:

- right to receive information - each Group company shall take appropriate measures to provide information to the data subjects about the processing of the data subjects' Personal Data;
- right to access - the data subjects are entitled to information and access to the Personal Data that a Group company processes about them;
- right to rectification - the data subjects shall be able to request rectification of any inaccurate or incomplete Personal Data that a Group company processes about them;

- right to erasure - the data subjects are, under certain circumstances, entitled to request erasure of their Personal Data;
- right to restriction - the data subjects shall under certain circumstances have the right to request restriction of the processing of their Personal Data, i.e. each Group company shall have technical measures in place to mark or flag Personal Data as restricted in order to ensure that the Personal Data is not processed further;
- right to data portability - in some cases, the data subjects are entitled to receive their Personal Data in a structured, commonly used machine-readable format and to request the relevant Group company (if technically feasible) to transmit their Personal Data to another data controller; and
- right to object - the data subjects shall have the right to object to the processing of their Personal Data if the processing is based on a balance of interests or if the Personal Data is processed for direct marketing purposes.

Requests for access to Personal Data should be made in writing via email to the relevant Group company or to dpo@stillfront.com. Guidance on how such requests are to be handled is set out in the Data Subject Access Request Procedure and Data Subject Access Request Guidance.

8. Data transfers

If a Group company transfers Personal Data to another data controller, that Group company shall take care to conclude data protection agreements if required under GDPR and comply with other requirements under applicable data protection laws for such transfer.

A Group company shall only engage data processors (i.e. third parties that process Personal Data on behalf of that Group company) that provide the Stillfront Group company with sufficient guarantees that the data processor will comply with applicable data protection laws. To ensure compliance with applicable data protection laws, a data processing agreement must be concluded with the relevant data processor.

When a Group company transfers Personal Data from the EU/EEA to a country outside the EU/EEA, that Group company shall ensure that the requirements set out in applicable data protection laws are observed so that the transfer is lawful. This includes, inter alia, ensuring an adequate level of protection in accordance with article 46 of the GDPR.

9. Division of Responsibilities

Responsibilities of all personnel of the Stillfront Group

Personnel that are required to process Personal Data on behalf of Stillfront shall:

- Act only on instructions from the Controller.
- Comply with applicable data protection laws, this Policy and associated policies, procedures and guidelines in place. We take such compliance very seriously as any breach of applicable data protection laws puts Stillfront at risk and may result in a substantial fine or actions imposed upon Stillfront by relevant supervising authority(ies). Any breach of this Policy by any personnel may lead to disciplinary action under our procedures which may result in dismissal, in civil lawsuit or in criminal prosecution.

- Complete relevant training and awareness activities provided by Stillfront to support compliance.
- Take all those security measures available to Stillfront to protect the Personal Data against accidental, destruction or loss or unlawful forms or processing.
- Take all necessary steps to ensure that no breaches of information security result from their actions.
- Report all suspected information security breaches or incidents promptly to the Data Protection Officer at dpo@stillfront.com, so that appropriate action can be taken to minimise harm.

Responsibilities of Data Protection Officer

The Data Protection Officer is responsible for the following tasks:

- Inform and advise Stillfront and the personnel who carry out processing of their obligations pursuant to applicable data protection laws and provisions.
- Monitor the Stillfront Group's compliance with applicable data protection laws and provisions and with this Policy and other policies, procedures and guidelines in relation to the protection of personal data in place for the Stillfront Group from time to time, including the assignment of responsibilities, awareness-raising and training of personnel involved in processing operations, and the related audits.
- Provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to article 35 of the GDPR.
- Cooperate with relevant supervisory authorities.
- Act as the contact point for the relevant supervisory authorities on issues relating to processing, including the prior consultation referred to in article 36 of the GDPR, and to consult, where appropriate, with regard to any other matter.
- Answer questions on data protection from data subjects, board members and other stakeholders.
- Make regular reports on data protection compliance and risks to the General Counsel.

Responsibilities of the Legal and Compliance Department

- Review and update this Policy and related privacy documents, templates and procedures on a regular basis.
- Make regular monitoring to ensure that privacy policies, procedures and guidance are being followed.
- Keep the Board of Directors and Data Protection Officer updated about privacy responsibilities, risks and issues.
- Ensure that data processing agreements are in place for third parties processing Personal Data on behalf of Stillfront and vice versa.

Responsibilities of the IT and Security Department

- Ensure all systems, services, software and equipment meet acceptable security standards and measures, including implementing required technical and organisational measures.
- Ensure operation of an active governance program to monitor, test and react to vulnerabilities of the systems and which has direct and indirect impact on the processing of Personal Data.
- Check, scan and test security hardware and software regularly to ensure it is functioning properly.
- Research and audit third-party services, such as cloud services Stillfront is using/considering using to store or process Personal Data.

Responsibilities of the employing department

- Ensure that all processing of personnel's' Personal Data is included in the record of processing activities of the relevant Group company.
- Inform the relevant personnel of their rights under this Policy and applicable data protection laws.
- Draft and update local related policies and procedures and ensure their compliance with relevant data protection laws and this Policy.
- Respond to personnel's requests regarding their Personal Data processed by the relevant Group company (including updating Personal Data when necessary).

Responsibilities of the IR/Marketing Departments:

- Ensure all marketing initiatives adhere to applicable data protection laws and this Policy.
- Ensure that all social media events, campaigns, means, advertisements and other ways of marketing, corresponds to applicable data protection laws and this Policy.

10. Training

Stillfront will provide the Studio Heads with regular training in this Policy and GDPR on a regular basis. Stillfront offers all subsidiary access to data privacy trainings through the OneTrust platform. Each Group company shall ensure that all its personnel which process Personal Data undergo regular training in this Policy and applicable data protection laws.

11. Compliance and Governance

Each Group company shall have internal procedures and documentation for being able to demonstrate its compliance with this Policy and applicable data protection laws.
Each Group company shall ensure that all relevant personnel of the Stillfront Group company are aware of the importance of protection of Personal Data and shall thus develop training and awareness programs, where the employees are informed and made aware in data privacy related matters.

Stillfront will monitor its compliance with this Policy on an ongoing basis. Stillfront will periodically verify that this Policy continues to conform to the applicable data protection laws and is being complied with.

Deviations or non-compliance with this Policy, including attempts to circumvent this Policy or applicable data protection laws may result in disciplinary actions, including termination, as allowed by applicable local laws. In some countries, violations of regulations designed to protect Personal Data may result in administrative sanctions, penalties, claims for compensation or injunctive relief, and/or other civil or criminal prosecution and remedies.

12. References to Associated Governing Documents

- IT Policy
- Data Breach Procedure
- Data Retention Procedure
- Data Subject Access Request Procedure

- Data Subject Access Request Guidance
- Guidance on Handling of Unstructured Personal Data

13. Document properties

Document title	Valid from
Processing of Personal Data Policy	27.08.2020

Document type	Department/Area
Policy	Corporate Governance

Version	Classification code	Approved by
2.1	Internal	The Board

Document owner
General Counsel

14. Revision history

Version	Valid from	Revision	Author
1.0	11.06.2019	Initial Version	CCO
2.0	27.08.2020	Annual Review	Johanna Bergsten, GC
2.1	2021-09-02	Annual Review	Johanna Lundberg, GC