Aperam Corporate Policy

Personal Data Privacy Policy

Approved by Management Committee on 17 July 2014

Document Information

Short Description:

The aim of this Policy is to define Personal Data Privacy principles and standards that Aperam has committed to in order to ensure that Personal Data are treated in an appropriate manner and in compliance with enforced data regulations. Aperam recognizes that Personal Data must be treated with caution, including employees' or business partners' data. Aperam therefore has adopted practical and legal measures in order to protect Personal Data handled under its responsibility.

This policy has been adopted based on Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (European Directive 95/46/EC).

Scope:

This policy is relevant to all staff, including Management and Directors of Aperam and all of its subsidiaries. It is also relevant to any third party acting on behalf of or in the interest of Aperam and/or its subsidiaries, including in case of a joint venture with another company or organization.

1. Introduction: General Principles

Aperam is committed to protect the personal data and privacy of any form by adopting following guiding principles for 'Personal data':

1. They shall be processed fairly and lawfully.
2. They shall be collected only for one or more specified and legitimate purposes, and shall not be further processed for any other purposes.
3. They shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. They shall be accurate and, where necessary, kept up to date.
5. If processed for any purpose or purposes, they shall not be kept for longer than is necessary for that purpose or those purposes. They shall be deleted as soon as they are no longer needed for the purposes for which they were collected.
6. They shall be processed in accordance with the rights of data subjects.
7. They shall be processed fairly and transparently. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. They shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. Definitions & General Commitments

2.1 Definitions

For the better understanding of the present statements, one should consider the following definitions:

Personal Data means data which relates to a natural person (i. e. a living individual who can be identified from those data, or from any other information which is, or is likely to be, in possession of the data controller)

Data Subject means any natural person, i. e. a living individual whose personal data are processed in the context of a process falling in the scope of this Policy.

Processing of Personal Data means obtaining, recording or retaining Personal Data, or any other operation on such data such as organization, adaptation or alteration, retrieval, consultation, use, disclosure, alignment or combination, blocking, erasure or destruction.

Sensitive Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning physical or mental health or sexual life.

Data Controller means a natural or legal person which collect for Aperam or Aperam subsidiaries Personal Data.

Data Protection Officer is a natural person, i.e. an individual who has been appointed by the Aperam Compliance Management Committee as a responsible person for the Personal Data Processing.

Compliance Management Committee is an executive group of 6 Aperam employees overseeing the implementation and regulation of Personal Data Privacy Policy. (see section 3 hereafter)

Personal Data Processor means a natural person or a legal entity which processes Personal Data on behalf of the Data Controller.

2.2 Aperam's commitments

- The Aperam Group Management Committee has overall responsibility for the implementation of this Policy.
- All directors, officers and employees of Aperam and its Subsidiaries worldwide that capture and process Personal Data must comply with this Policy.
- In all cases where the evidence is sufficient to warrant disciplinary action in case of failure to comply with the statements of the present Policy, such action will be taken in compliance with all applicable laws.
- Questions about compliance with this Procedure and/or with specific privacy policies may be addressed to the Compliance Management Committee through Compliance officer.

2.3 Data Subjects rights

Data Subjects shall be informed about the following:

- The data being processed or transferred.
- The identity of the Data controller(s) and of its representative if any, and any potential Data Protection Processor.
- The purposes of the processing for which the data are intended.
- His/her rights such as:
  - the recipients or categories of recipients of the data;
  - the right to access or rectify or block the data concerning him/her.

Every Data Subject has the right to obtain without constraint, at reasonable intervals and without excessive delay or expense, a copy of all data relating to him/her. Data Subject has no right to have access to any Personal Data not relating to him/her. Every Data Subject has the right to obtain the rectification, erasure or blocking of data in particular if the data are incomplete or inaccurate.

2.4 Data Transfers

Data Transfers to an External Processor

Personal Data can be processed by information systems owned and controlled by an external Processor in the EU or in the countries outside the EU. Before transmitting Personal Data to any such provider, the Data Protection Controller concerned must choose a provider providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with the following measures:

Golden Rule #1:

No Aperam Personal Data will be communicated/made available to an external Processor without having a written contract signed between the Aperam Subsidiary concerned and such external Personal Data Processor. Such contract shall include the standard contractual clause and the required data retention period.

Golden Rule #2:

No Aperam Personal Data will be communicated/made available to an external Personal Data Processor, unless such external Personal Data Processor provides an adequate level of protection.

Golden Rule #3:

In case of cross-border transfer from Europe to any country outside of Europe, the latest standard contractual clauses imposed by the European legislation (set of standard contractual clauses for the cross-border transfer of Personal Data From Controller to Processor) or by any national law shall also be included in the Agreement signed between the Aperam Subsidiary concerned and the Personal Data Processor, when applicable.

Data Transfers to an External Personal Data Controller

All transfers of Personal Data From Europe to External Data Controllers located out of the EU must respect the European rules on trans-border data flows (Articles 25-26 of Directive 95/46/EC: for instance making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC or by other adequate contractual means according to Articles 25 and 26 of the EU Directive).

2.5 Security breaches

Any suspected or actual security breach or similar incident that has, or might have, compromised the privacy or security of any Personal Data shall be immediately notified to the Compliance Management Committee.

The concerned Aperam Subsidiary(s) shall take all actions to address any such known security breach or attempted breach, in accordance with Compliance Management Committee's direction.

The security breach shall then be documented by the Compliance Management Committee in order to share the lesson learned.

3. Aperam Compliance Management Committee (roles and responsibilities)

The Compliance Management Committee consists of six (6) members:

- The Aperam Chief Financial Officer;
- The Aperam Head of Compliance;
- The Aperam Head of Combined Assurance;
- The Aperam Group General Counsel;
- The Aperam Head of Sustainability, HR & Corporate Communications;
- The Aperam Chief Information Officer;

The Compliance Management Committee shall remain in effect for the duration of this Policy.

The Compliance Management Committee shall undertake the following responsibilities:

- oversee the implementation of this Policy;
- investigate and resolve any major issues / problems related to Personal Data Privacy that may arise or may be reported to the Committee;
- take necessary measures to continuously improve Data Privacy framework;
- maintain and update the list of Aperam Subsidiaries bound by this Policy;
- initiate, validate and update specific policies for Global Tools related to Personal Data Privacy;
- update this Policy so as to ensure compliance with changes in laws, regulations, Aperam practices and procedures, Aperam corporate structure, or requirements imposed by data protection authorities. Changes of this core document shall be notified to the Aperam Subsidiaries;
- ensure that changes of this core document and changes to the list of Aperam Subsidiaries bound by this Policy are notified to the Data Protection Authorities granting the authorizations with a brief explanation of the reasons justifying the changes.

- communicate and share any information or issues that subsidiaries shall cooperate and assist each other to handle and support an investigation or inquiry by Data Protection Authorities.

The Compliance Management Committee Meetings are held on a periodic basis or upon request if needed.

Each member may, at his/her discretion, propose to the Compliance Officer to invite other members or consultants to attend meetings of the Compliance Management Committee. For sake of clarity, any consultant so invited will not take part in any decision and will not be deemed to be a member of the Aperam Compliance Management Committee.

4. Liability

Any Data Subject can enforce his / her rights based on this policy and in accordance to the local applicable law. These rights do not extend to those elements of this Policy pertaining to internal mechanisms implemented within Subsidiaries such as detail of training, audit program, compliance network, and mechanism for updating the rules.

5. Update of this policy

The Legal Department is responsible to update this Policy based on regulatory changes or other legal or organizational developments.

This policy is worded in English. Translations are made available in Dutch, French and Portuguese. In case of divergences between the English version and the Dutch, French or Portuguese versions, the English version will prevail.