Privacy

ALIAXIS GROUP POLICY n° 28

Aliaxis

Prepared by
Group Legal Department / Global Security and Information Department

Reviewed by
Group CLO / Group CIO

Approved by
Group CEO

Revision n°
1

Date
May 2018

RESPONSIBILITY FOR REVIEW

Group CLO / Group CIO

RESPONSIBILITY FOR APPROVAL

Group CEO

APPLICATION

This Policy applies worldwide to all businesses in which the Aliaxis Group has an interest of more than 50 %. In this document, Aliaxis HQ and/or any Aliaxis legal entity/affiliates are individually referred to as a "Company". All Companies are collectively referred to as the "Group".

Each Company is responsible for the implementation of this Policy in compliance with applicable local laws and within the framework of its corporate legal independence.

Contents

1
General Principles

Privacy is the right of individuals to determine if, when, how and to what extent data about themselves may be collected, stored, transmitted, used and shared with others. By protecting personal data from its customers, suppliers and employees, the Group demonstrates its commitment to respect their privacy.

Privacy and data protection laws have been and are being enacted to protect personal data of individuals.

"**Personal Data**" means any information about an identified or identifiable individual (e.g.: an employee or a customer). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. For example, names, photos, email addresses, bank account details, medical information, IP addresses and other online identifiers constitute Personal Data.

Privacy and data protection laws cover any type of Personal Data processing activities (consultation, use, transfer, storage, destruction, etc.). As a company, we are processing Personal Data on a daily basis, notably the Personal Data of our employees and of our customers and suppliers.

The present Policy is based on the new European regulation related to the processing of Personal Data[1], referred to as the General Data Protection Regulation ("GDPR"), as this is currently one of the strictest legislation on Personal Data and aims to comply with its requirements.

The Group has decided to implement this Policy throughout the Group to ensure an adequate level of protection for all Personal Data. Nevertheless, as privacy requirements and sanctions may vary from country to country, Companies should also comply with local privacy and data protection laws which are not addressed in this Policy.

1. Regulation (EU) 2016/679 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.

2
Purpose of this Policy

The purpose of this Policy is to lay down the principles that each Company will adopt regarding the use and protection of Personal Data.

Overall, the approach to privacy is the following:

- coordination at Group Level,
- management and responsibility at Company level.

Compliance with this policy is the responsibility of each Company. One person (a “Data Protection Coordinator”) shall be appointed within each Company to be in charge of privacy issues and of the implementation of privacy policies.

3
Privacy Requirements

a. Minimization & Accuracy

Companies can only collect and process Personal Data which are adequate, relevant and necessary for their activities.

Besides, Personal Data should be accurate and kept up to date where necessary.

b. Transparency

Each Company shall ensure that Personal Data are processed in a transparent manner in relation to the individuals concerned (the “Data Subjects”). This means that each Company should provide accurate details in privacy notices about:

- the Personal Data that is being collected and processed;
- the purposes and legal basis for the processing of Personal Data; and
- to whom the Personal Data might be disclosed or transferred.

These privacy notices shall be provided either before or at the time of collection of Personal Data where practical.

c. Protection

Each Company is committed to ensuring the protection of the Personal Data in its possession.

In order to prevent unauthorized access or disclosure or any other unlawful form of processing of Personal Data, each Company has set up appropriate physical, technical and procedural measures to protect Personal Data, in accordance with Aliaxis Group Policy n° 11 – Information & Communication Technology and Aliaxis’ Standard Operating Procedure n° PO11-PR24.

Access to Personal Data is restricted to authorized employees only in order to fulfil their job responsibilities. Furthermore, each Company has implemented appropriate technical measures including but not limited to access authorizations, authentication, firewalls, anti-virus measures, back-up, and disaster recovery plan, which are designed to provide a level of security appropriate to the risk of processing Personal Data.

3

Privacy Requirements (2)

d. Data retention

Each Company shall retain Personal Data in accordance with applicable laws and only as long as it is necessary to fulfil the purposes for which such data are collected. The specific retention periods shall be defined locally based on the national regulations and the specific and reasonable needs of each Company.

At the end of the retention period, the Company shall ensure that Personal Data is deleted or anonymized, or if this is not possible (for example, because the Personal Data has been stored in backup archives), then the Company shall securely store the Personal Data and isolate it from any further processing activity until deletion is possible.

e. Data breaches

Each Company shall report and document Personal Data breaches in accordance with the attached related Procedure (Procedure 5: Data Breach).

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Personal Data breaches can include:

- access by an unauthorized third party;
- deliberate or accidental action (or inaction) by a Company or its sub-contractors;
- sending Personal Data to an incorrect recipient;
- computing devices containing Personal Data being lost or stolen;
- alteration of Personal Data without permission; and
- loss of availability of Personal Data.

f. Data Subjects' rights

Each Company shall implement adequate procedures to enable Data Subjects to exercise their rights in relation to their Personal Data (e.g.: the right to access / receive a copy of their Personal Data; the right to rectify / update their Personal Data; the right to opt-out of marketing communications; …).

4

Sanctions in case of infringements

If a Company is found to infringe privacy and data protection laws, such infringement may lead to fines, imprisonment sentences and/or civil suits from Data Subjects requesting damages.

Under the GDPR, Companies may face substantial fines up to 20 million euros or 4 % of the annual turnover of the Group, whichever is higher.

Furthermore, any data breaches or unlawful processing have a negative impact on the Company and the Group reputation and business (e.g.: public warnings by the Data Protection Authority or press/social media coverage).

Consequently, the Group requires the attention of all managers and employees involved in the processing of Personal Data about the risks and consequences resulting from privacy law infringements and insists on strict compliance with privacy and data protection laws.

5
Dawn raids

Data Protection Authorities may proceed with an unannounced visit/inspection at a Company's premises. Such inspections are generally referred to as "dawn raids".

In such case, employees shall follow the guidelines mentioned in Annex 1.

6
Implementation of this Policy

In the area of privacy, Companies should organize themselves to ensure that they comply with this Policy and applicable local laws. Local management is responsible for providing the necessary resources and means for the attainment of the objectives including, safeguards procedures, tools and appropriate trainings.

In order to comply with this Policy, each Company shall:

- appoint a Data Protection Coordinator;
- establish and maintain a record of its data processing activities (i.e. a Data Inventory);
- ensure compliance with this Policy and the following Procedures:
  - Procedure 1: Employee Privacy Notice
  - Procedure 2: Customer & Supplier Privacy Notice - Template
  - Procedure 3: Recruitment Notice - Template
  - Procedure 4: Website/Mobile app Notice - Template
  - Procedure 5: Data Breach
  - Procedure 6: Privacy & Confidentiality Charter
  - Procedure 7: Direct Marketing Strategy

Such Procedures may need to be amended to comply with local privacy and data protection laws. Each Company shall ensure that the privacy notices are easily accessible by their intended recipients.

This Policy shall be immediately applicable to European Companies and to Companies who are processing Personal Data of European residents. For other Companies, this Policy will become applicable based on the planning that will be defined by the GLT.

7
Updates

This Policy may be updated periodically to reflect any necessary changes in our privacy practices.

8
Inquiries or concerns

For any further information about this Policy or the processing of Personal Data, please contact the Group Legal Department or the Global Information Security Department:

Aliaxis Legal Department / Information Security Department
Avenue Arnaud Fraiteur 15-23
1050 Brussels – Belgium
T +32 2 775 50 50 | F +32 2 775 50 51
email: privacy@aliaxis.com

9
Annexes

- Annex 1: Dawn raid guidelines
- Annex 2: Procedures

Privacy in short

- New regulation entered into force in May 2018, regulating the collection and use of personal data
- Aliaxis has adopted certain requirements related to the collection, use, storage and protection of personal data throughout the Group
- Aliaxis Companies have to comply with this Privacy Policy as well as with any applicable local data protection laws
- Personal data breach must be immediately reported to your Data Protection Coordinator and the Aliaxis Privacy Team
- In case of question regarding privacy or the use of personal data, contact your Data Protection Coordinator or the Aliaxis Privacy Team: privacy@aliaxis.com

we make life flow

www.aliaxis.com

Aliaxis