

Aliaxis Employee Privacy Notice

New Zealand

| | |
|--------------|--------------|
| Doc # | PO 28 – PR 1 |
| Issue # | 01 |
| Issue Date: | 01.04.2023 |
| Review Date: | 01.04.2025 |

This notice (hereafter the “Notice”) applies worldwide to all businesses in which the Group has a majority interest. Aliaxis HQ and/or any Aliaxis legal entity/affiliates are individually referred to as a “Company” or “we” or “us” in this document. All Companies are collectively referred to as the “Group”.

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

Contents

| | |
|--|---|
| 1. Purpose of this Notice | 1 |
| 2. Definitions | 1 |
| 3. Processing of Employees’ Personal Data | 2 |
| 3.1 General information. | 2 |
| 3.2 Types of Personal Data that we may collect | 2 |
| 3.3 Sensitive Personal Data | 2 |
| 3.4. Lawfulness of the Processing. | 3 |
| 3.5 Purposes of the Processing | 3 |
| 3.6. Disclosures of Personal Data | 3 |
| 3.7. International transfers of Personal Data | 4 |
| 3.8. Protection of the Personal Data | 4 |
| 3.9 Retention and Deletion of Personal Data | 4 |
| 4. Employees’ Data privacy rights | 5 |
| 5. Inquiries or concerns. | 5 |
| 6. Updates to this notice | 5 |

1. Purpose of this Notice

This Notice is valid as of 1st April 2023.

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

We respect the privacy rights of our Employees and are committed to handling Personal Data responsibly and in accordance with applicable laws. This Notice sets out the Personal Data that we collect and Process about you, the purposes of the Processing and the rights that you have in connection with it.

If you are in doubt regarding the applicable standards, or have any comments or complaints about this Notice, please contact us as explained under section 5 below.

2. Definitions

“**Personal Data**” means any information about an identified or identifiable natural person (i.e., an Employee). 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 natural person. For example, names, photos, email addresses, bank account details, medical information, IP addresses and other online identifiers constitute Personal Data.

"Processing" means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Sensitive Personal Data" means any information relating to an employee's race or ethnic origin, political or philosophical opinions, religious beliefs, physical or mental health or condition, sexual life, preference or orientation, trade union membership or affiliation, biometric data, genetic information, commission or alleged commission of a criminal offence and any related legal actions or past convictions.

"Employee" means current and past employees including those who work on a non-permanent basis, such as contingent workers, temporary and contract workers, independent contractors, consultants, professional advisors, secondees and interns.

3. Processing of Employees' Personal Data

3.1 General information

Companies process Personal Data related to Employees, including any information about dependents, beneficiaries and other individuals whose Personal Data has been provided to us.

For the purpose of this Notice, the Company that employs you or has entered into a contractual relationship with you will act as the data controller for your Personal data. Furthermore, Aliaxis HQ may also act as data controller for certain processing activities in relation to your Personal Data on a group-wide level.

3.2 Types of Personal Data that we may collect

The types of Personal Data we process about you include, but are not limited to: identification data and contact details (such as name, home address, telephone number, personal email address, date of birth), employment details (such as job title, position, office location, employment contract, etc.), national identifiers (such as ID/passport, immigration/visa status, social security numbers), Employee identification number, information about dependents and marital status, payroll data (such as salary, benefits, expenses, company allowances, stock and equity grants), financial information (such as bank account details or tax information), IT related information required to provide access to Company IT systems and networks (such as IP addresses, log files and login information), and any other information which may be voluntarily disclosed by an Employee.

Personal Data may be collected by different means, including:

- resumes and references;
- photographs;
- forms relating to an employee's health and welfare benefits;
- IT/security systems logs; and
- performance, potential and development assessments.

In most of the cases, Personal Data is collected directly from Employees but, in some cases, may be obtained indirectly from:

- other Company Employees (e.g., the Employee's manager, HR manager);
- other entities of the Group; and
- the Group's IT/security systems and applications used by Employees.

3.3 Sensitive Personal Data

As a general rule, a Company will not collect or process any Sensitive Personal Data from its Employees. However, in some circumstances and where required under national law, a Company may need to collect, or request on a voluntary disclosure basis, some Sensitive Personal Data for legitimate employment-related purposes, for example, information about your racial/ethnic origin, gender, and disabilities for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations; or information about your physical or mental condition to provide work-related accommodations, health and insurance benefits to you and your dependents, or to manage absences from work. In some countries, a Company may also process information about an employee's trade union affiliation.

3.4. Lawfulness of the Processing

The legal basis on which a Company relies to collect and process Personal Data will vary depending on the Personal Data itself and the specific purpose for which such Personal Data is collected.

In general, Companies will process Employees' Personal Data on the following legal and legitimate grounds:

- compliance with legal obligations to which a Company is subject (employment laws, tax laws, social security laws...);
- necessity for the performance of the employment or working relationship with the Employee;
- where such Processing is in the Company's legitimate interest and is not overridden by the Employees' data protection interests or fundamental rights and freedoms (e.g., for the general conduct of the Company's business or to carry out statistical studies about its workforce).

Where the Processing of your Personal Data is necessary to perform our work contract with you (i.e., to administer an employment or work relationship with us) or to comply with applicable laws, the provision of your Personal data is a statutory or contractual requirement. Therefore, we will not be able to manage our work relationship with you, nor to comply with applicable laws if you do not provide us with such Personal data.

Where legally required, the Company will ask you to give your prior consent in order to process Personal Data (e.g., for the Processing of Sensitive Personal Data).

3.5 Purposes of the Processing

Personal Data is generally Processed by the Group for the purpose of managing our employment or working relationship with you. Companies may also Process your Personal Data for the following purposes:

- internal recruitment, career development, promotion, internal mobility and succession planning;
- administration of pay benefits and equipment;
- assessment of Employee's qualifications and performances;
- assessment of business performances;
- administration of IT and security systems;
- physical security of the Employees, facilities and access to physical premises;
- management of work accidents and health and safety at work;
- management of Employees' travel management activities;
- management of internal communications;
- administration of e-mail services, social media platforms, newsletters and brand Centre;
- accounting, forecasting, budgeting and financial planning;
- administration of management fees;
- gathering evidence in case of disciplinary action or termination of the employment contract;
- having a contact point in the event of emergency;
- training and development; and
- to comply with applicable laws and regulations, or to exercise or defend the legal rights of the Company.

If a Company intends to further process Personal Data for a purpose other than the ones described in this Notice, it shall inform Employees about those other purposes and provide any other relevant information prior to that further Processing.

3.6. Disclosures of Personal Data

Each Company takes care to allow access to Personal Data only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it. In case a Company discloses Personal Data to another entity of the Group or to a third party, it will take all necessary steps to ensure an adequate level of protection of such data.

Your Personal Data may be disclosed to the following categories of recipients:

- a. Other Group companies:** we may share your Personal Data with other entities within the Group in order to administer human resources, Employees' compensation and benefits at an international level, as well as for other legitimate business purposes such as training/development, IT services/security, tax and accounting, and general business management;

- b. Third party service providers:** we may also make certain Personal Data available to third parties who provide services to us in connection with the related purpose(s) we collected Personal Data, such as external payroll providers, health, insurance and benefit plans providers and travel management agencies. We may also disclose Personal Data to external consultants, lawyers and advisors on a need-to-know-basis.
- c. Public authorities:** we may also disclose Personal Data to public authorities, such as national healthcare, pension, immigration and tax authorities, in accordance with applicable laws.
- d. Other third parties:** we may also disclose Personal Data to other third parties on other lawful grounds, including:
- where the Company is legally compelled to do so (for instance, to comply with valid legal processes such as search warrants, subpoenas or court orders, etc.);
 - such disclosure is required for the purpose of providing services and/or information to the concerned Employee;
 - such disclosure is justified by the Company's legitimate interests as defined above;
 - such disclosure is related to the Company's regular reporting activities to other Group Companies;
 - in connection with the sale, assignment or other transfer of all or part of our business; or
 - with your prior consent.

3.7. International transfers of Personal Data

Our Group operates at a global level and, as a result, a Company may need to transfer Personal Data to group affiliates or third-party service providers located in countries other than the ones in which your Personal Data was originally collected.

For example, Companies may need to transfer Personal Data to other countries for internal recruitment, career planning and international mobility purposes. In such a case, the Company will implement appropriate safeguards to ensure that an adequate level of protection for any Personal Data transferred.

Where the transfer relates to Personal Data of European residents to countries outside the European Union (EU) and European Economic Area (EEA), the Company will take the required measures to provide an adequate level of data protection under EU law, such as entering into EU standard contractual clauses with the party who is receiving the data.

Where transferring Personal Data of New Zealand resident individuals to countries outside of New Zealand, we will ensure an adequate level of protection for any Personal Data transferred, whether by ensuring the recipient is required to protect that Personal Data under comparable laws or by entering into an appropriate contractual arrangement with any recipient that may process or use the data. If we are not able to ensure that a recipient is required to protect your Personal Data using comparable safeguards to those under New Zealand's privacy laws then we will only provide your personal information to those recipients if you have authorised us to do so.

3.8. Protection of the Personal Data

Each Company is committed to ensuring the protection of the Personal Data of its Employees. In order to prevent the loss, unauthorized access, use, modification 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 the Personal Data in its possession, in accordance with Aliaxis Group Procedure 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 plans, which are designed to provide a level of security appropriate to the risk of Processing your Personal Data.

3.9 Retention and Deletion of Personal Data

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 is collected. Generally, this means your Personal Data will be retained until the end of your employment or work relationship with us plus a reasonable period of time thereafter to respond to employment or work-related inquiries or to deal with any legal matters (e.g. judicial or disciplinary actions), to document the proper termination of your employment or work relationship (e.g. to tax authorities), or to provide you with ongoing pensions or other benefits. The specific retention periods shall be defined locally based on the national regulations and the specific needs of each Company. For more details about the retention of your Personal Data, please contact us as explained under section 5 below.

At the end of the retention period, the Company will 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 will securely store the Personal Data and isolate it from any further processing activity until deletion is possible.

4. Employees' Data privacy rights

Employees have the following rights under applicable laws:

- the right to obtain confirmation as to whether or not Personal Data concerning them are being processed and, where that is the case, the right to request access and/or to receive a copy of their Personal Data;
- the right to rectify or update any inaccurate or incomplete Personal Data;
- the right to restrict the Processing of their Personal Data on certain legal grounds;
- the right to reasonable assistance from us when making a request to access their Personal Data
- the right to lodge a complaint with a competent data protection authority.

Employees resident in the United Kingdom or European Union have additional rights under applicable laws including:

- the right to obtain the erasure of their Personal Data;
- the right to object to the Processing of their Personal Data on grounds relating to their situation, where such Processing is necessary for the purposes of a Company's legitimate interest;
- the right to receive their Personal Data in a structured, commonly used and machine-readable format and to have their Personal Data transmitted to another controller where the Processing is carried out by automated means and is based on the Employee's consent or on contractual terms with the Employee; and
- the right to withdraw their consent at any time if the Processing of Personal Data is based on their consent. Withdrawing consent will not affect the lawfulness of any Processing that is conducted prior to such withdrawal, nor will it affect the Processing of Personal Data conducted in reliance on lawful Processing grounds other than consent.

If you wish to exercise any of the rights above, please contact your local HR representative as explained in section 5 below. Evaluative information may be confidential to us. Where applicable, you may also personally rectify or update some of your Personal Data, depending on the tools and procedures set up by your Company (e.g., you can manage part of your profile on the intranet).

5. Inquiries or concerns

If you have any questions or concerns regarding the way we process Personal Data, or for any further information about this Notice, or if you wish to exercise your data privacy rights, please contact your local HR representative or your local Data Protection Coordinator. In New Zealand this is:

Data Protection Coordinator
privacy.nz@alixaxis.com

6. Updates to this notice

This Notice may be updated periodically to reflect any necessary changes in our privacy practices. In such cases, we will inform you on the intranet and indicate at the top of the Notice when it was most recently updated. We encourage you to check back on our Intranet periodically in order to be aware of the most recent version of this Notice.