

Privacy Policy

Who are we?

The AAC Group comprises companies that operate in the textile sector, particularly in the areas of development, production and provision of services associated with clothing.

This Privacy Policy applies to the AAC Group, composed of AAC Têxteis, S.A. and ATELIER R&D, LDA. / CAAP Studio, both headquartered at Rua de Roederstein, lote 4, Vilarinho das Cambas, 4760-774 Vila Nova de Famalicão, Portugal.

AAC Têxteis, S.A.: legal entity no. 501837264,

ATELIER R&D, LDA. / CAAP Studio: legal entity no. 514429070,

Throughout this policy, when we refer to the **“covered companies”**, we mean these two companies.

When we refer to the **“applicable company”**, we mean the specific AAC Group company that, in each situation, processes your personal data or to which the relationship relates.

Why do we have this Privacy Policy?

At the AAC Group, we value the privacy and protection of the personal data of the people with whom we interact.

This policy explains, in simple terms, what personal data we may collect, for what purposes we use it, with whom we may share it, how long we retain it, what measures we use to protect it, and how you can exercise your rights.

This policy takes into account the General Data Protection Regulation (RGPD) and Law no. 58/2019, which ensures the implementation of the RGPD in Portugal.

Who is responsible for processing your data?

The company responsible for processing your personal data will, in each case, be the AAC Group company that determines the purpose and means of the processing.

Accordingly, the controller may be:

- AAC Têxteis;
- CAAP Studio;
- or, in certain situations, both AAC Group companies, where the purposes or means of processing are determined jointly.

Within the AAC Group, matters relating to privacy and personal data protection are managed centrally by the shared Privacy, Human Resources and Social Responsibility services, in coordination with Management.

These shared services support both AAC Group companies and may process personal data whenever necessary for the purposes described in this Policy. The existence of these shared services does not, in itself, change the responsibility of the applicable company for the processing of the personal data concerning it.

The company responsible for processing will be determined according to the specific situation. For example:

- in the case of employees, it will generally be the employing company;
- in recruitment processes, it will be the company promoting the process or for which the vacancy is intended;
- in the case of clients, suppliers or service providers, it will be the company with which there is a contractual, commercial or operational relationship.

Access to personal data is limited to people who need that information to perform their duties. People with access to personal data are subject to confidentiality duties and must comply with internal data protection and information security rules.

How can you contact us about data protection?

For any matter related to the processing of personal data or to exercise your rights, you may contact us through the following means:

Data protection email:

candidaturas@aactexteis.pt

Address:

Rua de Roederstein, lote 4
Vilarinho das Cambas
4760-774 Vila Nova de Famalicão
Portugal

Telephone:

+351 252 800 200

Whenever possible, please indicate the company to which your request relates, for example AAC Têxteis, S.A. or ATELIER R&D, LDA. / CAAP Studio, so that we can respond more quickly and appropriately.

Whose personal data may we process?

We may process personal data of different people with whom we interact, namely:

- job applicants;
- employees and former employees;
- clients and potential clients;
- suppliers, service providers and partners;
- representatives, employees or professional contacts of clients, suppliers and partners;
- visitors to the premises;
- users of websites, digital platforms and contact channels;
- regulatory, certification, audit or other interested entities.

How do we collect your data?

We may collect your personal data directly from you, for example when you contact us, fill in forms, submit an application, visit our premises, enter into a contract with us or establish a professional, commercial or institutional relationship with one of the covered companies.

We may also collect personal data in the context of the employment relationship, recruitment processes, contracts with clients, suppliers or service providers, communications by email, telephone or *website*, audits, certifications, legal obligations or internal procedures.

In some situations, data may be provided by third parties, such as clients, suppliers, service providers, public entities, certification bodies, insurers, occupational health entities, occupational safety and health entities or other partners, whenever there is a legitimate basis for such processing.

What personal data may we process?

The personal data processed depends on your relationship with us and on the purpose in question.

We may process, for example:

- identification data, such as name, civil or tax identification number, date of birth and signature;
- contact details, such as address, email and telephone;
- professional data, such as role, employer, department, position and professional contacts;
- application data, such as curriculum vitae, professional experience, education, skills, interviews and assessments;
- employment, administrative and contractual data;
- attendance, training, remuneration, tax, social security and insurance data;
- data necessary to comply with occupational safety and health obligations;
- fitness-for-work data and applicable functional recommendations, within the legally admissible terms;
- financial, accounting and billing data;
- premises access data, visit records or contact records;
- technical data related to the use of websites, cookies, devices, IP address or digital interactions, where applicable.

We only process personal data that is necessary, appropriate and relevant for each purpose.

What do we use your personal data for?

When you contact us to request information, clarify doubts, request support, submit requests or obtain a response about our products, services or activities, we may process your contact details and the content of the communication in order to respond to your request and follow up on the matter.

This processing may be necessary for pre-contractual steps, the performance of a contract, compliance with legal obligations or the pursuit of legitimate interests of the covered companies, depending on the context of the contact.

We may use your personal data for different purposes, depending on the relationship with the applicable company.

Category of data subject	Purpose	Legal basis	Responsible company
Job applicants	Management of recruitment and selection processes, application review, contact and interviews	Pre-contractual steps, legitimate interest and/or consent where applicable	Company promoting the recruitment process
Employees or former employees	Management of the employment relationship, payroll processing, training, attendance, tax obligations, social security, insurance and occupational safety and health	Performance of the employment contract, compliance with legal obligations and legitimate interest	Employing company
Clients, potential clients, suppliers and service providers	Commercial, contractual, administrative, financial and logistics management, audits and access control	Performance of a contract, pre-contractual steps, legal compliance and legitimate interest	Contracting or commercially responsible company
Visitors	Access management, premises security, contact with visited persons, protection of people, property and information	Legitimate interest and compliance with internal procedures or legal obligations	Visited company
Users of websites or digital channels	Website operation, response to requests, statistical analysis, cookie management and digital communications	Legitimate interest, consent or legal compliance, as applicable	Company responsible for the website

Consent will only be requested when it is the appropriate legal basis for the purpose in question, for example to retain applications for future opportunities, send marketing communications when required, use non-essential cookies or use image, video, voice or testimonials for public disclosure purposes.

Where processing is necessary to perform a contract, comply with legal obligations, respond to requests, manage employment relationships, ensure occupational safety and health, comply with tax, accounting or legal requirements, or pursue the legitimate interests of the applicable company, processing will not, as a rule, depend on consent.

How long do we keep your data?

We keep your personal data only for the period necessary to fulfil the purpose for which it was collected.

In some cases, we may have to keep the data for longer, for example to comply with legal, tax, employment, accounting or contractual obligations, audits, certifications or for the establishment, exercise or defence of legal claims.

Where processing is based on consent, we keep the data while that consent remains valid or until it is withdrawn, unless another legal basis justifies retention.

Whenever there is no valid reason to keep the data, it will be deleted, anonymised or securely archived, as applicable.

What if you submit an application?

If you submit a spontaneous application or respond to a vacancy, we will process the personal data you provide to us, such as name, contact details, curriculum vitae, professional experience, education, skills and other information relevant to the recruitment process.

This data will be used to analyse the application, contact the candidate, conduct interviews, assess suitability for the intended profile and, where applicable, prepare the conclusion of an employment contract.

The processing of application data may be based on pre-contractual steps, the company's legitimate interest in managing recruitment and selection processes, or the candidate's consent where the retention of the application for future opportunities is concerned.

Data collected in the recruitment process will not be subject to exclusively automated decisions. Where applicable, analysis criteria or selection support tools may be used to assess the suitability of the application for the intended profile. However, the final decision will always be made with human involvement.

The company adopts appropriate technical and organisational measures to protect personal data against loss, destruction, alteration, unauthorised access, improper disclosure or any other unlawful processing.

Persons authorised to access personal data may only do so within the scope of their duties and are bound by a duty of confidentiality.

Candidates may exercise their rights under the terms indicated in this policy, including the right to withdraw consent where processing is based on that ground.

Who may we share your data with?

We may share personal data with third parties where this is necessary for the purposes described in this policy or to comply with legal obligations.

This may include, for example:

- payroll processing entities;
- accounting entities;
- training entities;
- insurers;
- occupational health entities;
- occupational safety and health entities;
- consultants, auditors and certification bodies;
- logistics providers;
- banking entities;
- information technology service providers;
- hosting, maintenance or system support providers;
- judicial, tax, regulatory or administrative authorities.

Where these entities process personal data on behalf of the applicable company, appropriate contracts or instruments must be in place defining the rules for processing, security, confidentiality and use of the data. The GDPR provides for specific obligations applicable to processors and to processing carried out on behalf of the controller.

How do we protect your data?

We adopt appropriate technical and organisational measures to protect personal data against unauthorised access, loss, alteration, disclosure, destruction or unauthorised use. Persons authorised to access personal data may only do so within the scope of their duties and are subject to confidentiality obligations.

Among other measures, we may use:

- permanent access control;
- user profiles;
- passwords and authentication mechanisms;
- backups;
- *firewalls* and IT security measures;
- use of secure means of sharing information, including limited permissions, protected links and passwords, where applicable;
- confidentiality rules;
- access limited to those who need the data to perform their duties;
- assessment of suppliers with access to personal data;
- archiving and deletion procedures;
- internal awareness on data protection;
- security incident management.

What do we do in the event of a personal data incident?

If a situation occurs that may affect the security of personal data, such as loss, unauthorised access, unauthorised disclosure or accidental destruction, the covered companies follow internal procedures to analyse, contain and document the situation.

Where legally required, the personal data breach will be notified to the supervisory authority and/or to the affected data subjects. The GDPR provides specific rules on notification of personal data breaches.

All employees and service providers must report, as soon as possible, any suspected incident involving personal data.

What are your rights?

As a data subject, you may exercise the rights provided for in the applicable legislation, namely:

- **right of access to your data**, to know what data we process about you and obtain information about that processing.
- **right to rectification of data**, where it is incorrect, outdated or incomplete.
- **right to erasure of data**, where it is no longer necessary for the purpose for which it was collected, where you withdraw consent and there is no other legal basis for processing, or where another situation provided for by law applies. This right may not be fulfilled where retention of the data is necessary to comply with legal or contractual obligations or to defend rights.
- **right to restriction of processing**, for example where you contest the accuracy of the data, where the processing is under review or where the data is necessary for the establishment, exercise or defence of legal claims.
- **right to data portability**, where processing is based on consent or on a contract and is carried out by automated means. In these cases, you may receive the data you provided to us in a structured, commonly used and machine-readable format.

- **right to object to processing**, where processing is based on the legitimate interests of the applicable company or where direct marketing is concerned, under the terms provided by law.
- **right to withdraw consent**, whenever data processing is based on your consent. Withdrawal of consent does not affect the lawfulness of processing carried out before that withdrawal.
- **right not to be subject to exclusively automated decisions**, including profiling, where such decisions produce legal effects or significantly affect the data subject, except in the cases provided for by law.

To exercise your rights, you may contact us using the contact details indicated in this policy.

Requests relating to the exercise of data subject rights are received and followed up by the shared Privacy/Human Resources and Social Responsibility services of the AAC Group, in coordination with Management and with the applicable company.

We may request additional information to confirm your identity whenever this is necessary to protect your personal data.

As a rule, we will respond to your request within one month. This period may be extended in the cases provided for by law, for example where the request is complex or there are several requests.

The response to the data subject will be provided by the applicable company or on its behalf, depending on the specific situation and the nature of the request.

Can you lodge a complaint?

Yes. If you consider that the processing of your personal data violates the applicable legislation, you may lodge a complaint with the National Data Protection Commission (CNPD).

The CNPD is the national supervisory authority in Portugal for personal data protection.

CNPD contact details:

Av. D. Carlos I, 134 - 1st floor

1200-651 Lisbon

Website: www.cnpd.pt

Can data be transferred outside the European Union?

In some situations, we may use suppliers, systems or platforms that involve the transfer of personal data outside the European Economic Area.

Where this occurs, we will ensure that the transfer is carried out under the terms permitted by the applicable legislation, for example through an adequacy decision, standard contractual clauses or another legally provided mechanism.

Do we use cookies?

We may use cookies and similar technologies on the websites of the covered companies.

Some cookies are necessary for the operation of the website.

Where applicable, the user may accept, refuse or change their cookie preferences.

Can this policy be updated?

Yes. We may update this Privacy Policy whenever necessary, for example in the event of a change in the law, a change in the structure of the AAC Group, a change in the covered companies, new systems, new service providers, new data processing activities or a change in the available contact details.

The updated version will be made available through the appropriate channels.

We recommend that you consult this policy periodically to stay informed about how we process your personal data.

Final information

This Privacy Policy is intended to explain, simply and transparently, how the AAC Group processes personal data.

Where more specific information documents exist, for example for employees, applicants, cookies or certain internal processes, those documents complement this policy.