Privacy Policy

Direction Générale France - 2020

ayming

Protecting the security and confidentiality of your personal data and that of your employees is a strategic issue for the Ayming Group. For this reason, we have put in place this Personal Data Protection Policy to guarantee the security of the information you provide to us. We hope it will help you understand what data the Ayming Group may collect, the scope of the data processed, and how the Ayming Group uses and protects it.

Scope

The Personal Data Protection Policy applied by the Ayming Group protects the information that you entrust to us within the framework of our missions, our commercial/contractual exchanges or via our website (registration / download / contact form).

Fair collection of relevant and strictly necessary data

Only the data necessary for the exercise of our missions are collected, stored and updated. The storage of your personal data in our systems is primarily the result of a decision on your part to entrust this data to us; we do not capture this data without your knowledge and without informing you.

For the sake of transparency when collecting your data, we provide you with as much information as possible about the purpose of this collection and the nature of the rights you have.

Type of data processed

In the context of our commercial approaches, we collect various categories of personal data concerning your employees, whether you are a prospect, customer or supplier, such as identification data (surname, first name, title), professional contact details (addresses, telephone numbers, email, position) and a history of customer relations (appointments, satisfaction marks, complaints, responses to satisfaction surveys, etc.).

Your data is communicated to us when you contact us and in notably from the form available on our website, via partners or directly by you within the framework of our exchanges.

In addition, as a Client, within the framework of the realization of missions, you are led to communicate to us various categories of information necessary for the good realization of the mission. The contract binding us details the data, the purposes of processing, the operations carried out, the storage periods and the security measures implemented by us.

Use of your personal data

When you provide us with personal data, we use it, in accordance with your instructions or the agreed purposes, to process the assignments you have entrusted to us, to answer your questions, or to enable you to access specific information or offers.

Moreover, only in the context of our commercial relations:

- we may store and process your professional data (surname, first name, position, ...) and share it within the Ayming group in order to better understand your needs and how we can adapt our services;
- we (or a third party acting on our behalf) may use your personal data to contact you about an Ayming Group offer that may meet your needs, or to invite you to complete online surveys to assess your satisfaction and help us better understand your expectations.

If you do not wish your personal data to be used for direct marketing or market research, we will respect your choice. We do not sell your personal data to third parties.

Data retention period

Your data is not retained beyond what is necessary; retention periods vary according to the nature of the data, the purpose of the processing and legal or regulatory requirements.

The data collected from the forms on our websites are kept for a period of 3 years from the last exchange.

The retention period for data received within the framework of our contractual relationship is specified in the contract.

Reinforced safety features

The Ayming Group has a CISO (Chief Information Security Officer), who works on guaranteeing the security, availability and integrity of the information system and data.

It is our responsibility to ensure that your data is not inappropriately disclosed. Thus, access to personal data on all our systems is subject to strict conditions of implementation, including:

- the implementation of filtering and control systems on our networks (Firewall),
- centralized management of rights profiles. All access requests are managed via our ticketing tool integrating validation workflows,
- the detection of external and internal intrusions and the implementation of procedures of regularly tested alerts,
- proven backup and disaster recovery features that ensure data can be restored in the shortest possible time.

The servers, owned by the Group, are hosted in France by a renowned HDS approved hosting provider offering all the guarantees of optimal service quality with increased performance. Our servers are administered by our IT department in order to have perfect control over security. This organization is fully in line with the ISO 27001 certification process undertaken by Ayming.

Ayming France is certified ISO 27001:2013, since 2019 for its Acciline+ activities and all solutions resulting from the Acciline+ solution, as well as for its activities related to Financing and Innovation Management. All of our IT procedures have been brought into line with the requirements of the ISO 27001:2013 standard and the Management of Ayming France has confirmed its commitment to data protection by initiating steps to extend this scope to its other activities.

Ayming Spain is certified ISO 27001:2013 for its Innovation activities.

Transmission of your personal data to third parties

The transmission of data to third parties may be justified:

- When the circumstances of the mission require it: transfer to subcontractors who are themselves bound by contractual clauses guaranteeing the security and confidentiality of your data or to independent service providers who are themselves subject to ethical rules of conduct by their profession (lawyers and doctors involved in professional risk management missions). Such transmission is specified in the contract.

Communication to bodies governed by public or private law, where such communication is provided for by the Law. These transfers are carried out in accordance with the regulations in force. As Ayming is an international group, we may be led to transfer personal data outside the European Union, in particular to entities of its group, for the exclusive purpose of managing our activity. In this case, we undertake to put in place adequate protection mechanisms.

A demanding control of our subcontractors

The Ayming Group ensures that your data continues to benefit from an adequate level of protection in terms of security and confidentiality throughout its processing. We therefore pay particular attention to ensuring that our subcontractors are able to guarantee the security and confidentiality of the data we entrust to them.

Rights of access to your data

In accordance with the regulations in place,

- you benefit from a right of access, limitation, portability, deletion and correction of your personal data;
- you can also, for legitimate reasons, oppose the processing of your personal data;
- you can withdraw your consent to the processing of your data for the future. In this case, any processing carried out prior to the withdrawal will be deemed lawful.

These rights can be exercised by sending us a letter accompanied by a copy of an identity document to the following address:

Groupe AYMING – DPO (Data Protection Officer)
185 avenue des Grésillons
92622 Gennevilliers cedex
dpo@ayming.com

Compliance check:

In order to guarantee the correct application of our rules and the compliance of our practices over time, our DPO follows up with each Ayming Group data controller and audits are carried out by our team of internal quality auditors, trained in the specific rules of the GDPR.

A report on these actions is drawn up by the DPO, directly with the Ayming Group's General Management.

Document update:

This document is updated to take into account changes in the content of the services offered to you.

General Management France

Personal data protection policy

Version - September 2020