IMA GROUP
PRIVACY CHARTER

What is personal data?

Under the applicable regulations, **personal data means any information relating to a natural person who can be identified**, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the identity of the natural person.

Why do we collect personal data?

We collect information about you for the following purposes:

- to manage our contracts (pre-signing, signing, amendment, cancellation)
  Depending on the type of contract you have signed, we may collect, for example, your address, your bank details, your telephone number and your email address etc.

- to provide the services agreed in the contracts
  Depending on the type of contract you have signed, we may collect, for example, information about the reasons why you have purchased our services, your location and information about your health etc.

- to analyse data sets, mainly to help us improve our services.
  Our teams may collect, cross-reference and analyse data sets. The results of this analytical work help us, directly or indirectly, to provide better services.
  For example, we regularly conduct satisfaction surveys and collect information about any new needs expressed by the recipients of our services.

Our commitments

- Collection of strictly necessary data only
  We only collect your personal data for the purposes listed above. The information requested is therefore always needed for those purposes.

- Strict use of your data
  Your personal data is only used for the purposes listed above: to manage your contract, provide our services and conduct analytical work to improve our services.

Implementation of our commitments

Our personal data protection commitments are implemented through concrete measures concerning our employees, our tools and procedures, data security and our structure. The consistency of the measures is ensured through our Privacy Policy, recorded in a formal document that is regularly updated.

- Employee training and awareness-raising measures
  Our employees are very aware of the need to comply with our personal data processing commitments. We regularly conduct campaigns to improve their awareness and arrange mandatory training.

- Suitable collection tools and procedures
  Our information systems and procedures are designed to ensure a strict organisation of the collection of essential data, for the purposes listed above only.
  For example, we use required fields, drop-down menus etc.

- Data security
  The security of our information systems is governed by a specific policy, called the General Information Security Policy, which provides that the main aim of security systems is to protect information.
  The security principles are designed to address the identified security issues and are based on four main themes:

- Overseeing security and continuity;
- Ensuring the continuity of operations;
- Managing and protecting access to property and data;
- Protecting infrastructure.

- A suitable structure

- A system for identifying and managing risks
  A risk assessment is conducted for the protection of personal data, to enable an optimum management of the related risks.
  Risks are assessed according to the nature of the data and the purpose of each data processing operation.
  We pay special attention to the risks associated with the processing of health data.

- A Group Data Protection Officer
  The Data Protection Officer (DPO) is responsible for monitoring compliance with the provisions that apply to our data protection operations.
  The DPO is the point of contact for administrative and supervisory authorities, such as the French Data Protection Authority (CNIL), and the DPO undertakes to cooperate with those authorities.

- A Group Chief Information Security Officer
  The Chief Information Security Officer (CISO) ensures that our information systems security procedures are effective, including data protection mechanisms. The CISO updates all policies concerning information systems, including the general information security policy.

- An internal control and audit system
  The quality of the personal data protection system is ensured through a regular review, based on on-going controls and periodic controls.

Data subject rights

- Right of access
  You have the right to obtain information about the personal data we hold about you.

- Right to rectification
  You have the right to ask us to rectify your data if you consider it to be inaccurate or incomplete.

- Right to erasure (also known as the right to be forgotten)
  You may ask us to erase the personal data we hold about you. However, this right may not be exercised in some cases, if we are required or permitted to retain your data under the applicable regulations.

- Right to object
  You may object to our use of some of your personal data at any time. In particular, you may always object to our use of your personal data for marketing purposes. In all other cases, you will need to tell us the specific reasons why you object to the use of your personal data.

- Right to restrict processing
  You may ask us to suspend the use of your data until we have carried out the checks required to address a request exercising one of your other rights.

- Right to data portability
  You may recover the data provided through our digital platforms for your personal use or to pass it on to a third party of your choice.

Procedure for exercising your rights

You should submit a request to the Group Data Protection Officer at the following address: Direction des Affaires Juridiques - Avenue de Paris - 79000 Niort - France - dpo@ima.eu