

1. Introduction

Hightekers and its affiliated companies (hereinafter referred to as 'Hightekers', 'We', 'Our' or 'Us') are committed to protecting the privacy and security of your personal information. We are committed to protecting the privacy of our consultants, employees, clients and users of our services who communicate with us (online or offline), whether at a meeting or conference, at events, by telephone, via our mobile apps, our websites or our social media platforms.

We have therefore drawn up this privacy policy to inform you about the data we collect, what we do with your information and what we do to protect it, as well as the rights and choices you have regarding your personal information.

In this document, we refer to data protection legislation, namely EU Regulation 2016/679 of 27 April 2016, the General Data Protection Regulation (GDPR), which governs the processing of personal data within the European Union, as well as the French Data Protection Act of 6 January 1978, which ensures the protection of personal data contained in both paper and digital files and processing systems, whether public or private.

Hightekers is the data controller for the personal information we process, unless otherwise stated.

We are registered with the French Data Protection Authority (CNIL).

You can contact us by telephone, email or post.

Our main business/postal address: 1 Place des Saisons - 9E, 92400 Courbevoie.

Telephone: +33 1 86 65 31 10

Email: dpo@hightekers.com

Our Data Protection Officer is: Dr Louis Sanchez de Lozada

2. Who we are

This policy applies to processing carried out by Hightekers and Affiliates as an independent controller, unless stated otherwise.

It covers our commercial, contractual, marketing, support, compliance, security, relationship management and event administration activities.

3. Data subjects

- Customers and potential customers;
- Prospects;
- Candidates;
- Consultants;
- Contractors;
- Suppliers;
- business partners;
- Visitors;
- users of our platforms;
- company representatives;
- Signatories;
- Billing, procurement, support, compliance or legal contacts.

A person may fall within more than one category depending on the nature of the relationship.

4. Data we process

- **Identity and contact data:** name, surname, title, role, company, email, phone number, postal address, country, language, time zone, internal identifiers, signature.
- **Relationship data:** communication history, meetings, calls, requests, support tickets, contact preferences, consents, objections, feedback, event registrations.
- **Commercial and contractual data:** quotations, purchase orders, contracts, appendices, renewals, terminations, pricing terms, discounts, service levels, orders, deliveries, disputes.
- **Financial and billing data:** billing details, invoice numbers, accounting references, payment status, credit notes, anti-fraud checks, bank references where necessary.
- **Marketing and prospecting data:** lead source, campaign history, opens, clicks, event participation, preferred channels, segmentation, engagement measurement.
- **Technical and security data:** IP address, login logs, session IDs, browsing data, device settings, security logs, timestamps.
- **Compliance data:** proof of consent, proof of objection, KYC/AML checks where applicable, sanctions screening, audits, quality checks, incident files.
- **Special category data and criminal offence data** only where a specific legal basis exists and subject to appropriate safeguards.

5. Sources of data

We collect data directly from you through our forms, contracts, emails, calls, meetings, demos, trade shows, events, platforms, websites and business interactions.

We may also receive data from group companies, service providers, agencies, partners, professional directories, professional social networks, public sources and authorised third parties.

In some cases, data may be collected indirectly; in that case, the required information is provided as soon as possible and, at the latest, within the applicable time limits.

6. Purposes and legal bases

We process data to manage business relationships, qualify and track prospects, prepare, conclude and perform contracts, manage billing and collections, provide support, manage events and communications, administer accounts, secure our systems, prevent fraud, comply with legal obligations, handle complaints, checks and disputes, and improve our services and processes.

Legal bases may include contract performance, pre-contractual measures, legal obligation, our legitimate interests or your consent.

Our legitimate interests include business management and growth, security, evidence, fraud prevention, compliance, improving user experience and defending our rights.

Where we rely on legitimate interests, we carry out a balancing test to ensure your rights and freedoms are not overridden.

7. Special category data

As a rule, processing of special categories of personal data is prohibited. We process such data only if an Article 9 GDPR exception applies and the required safeguards are in place.

Special categories may include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, health data and data concerning a person's sex life or sexual orientation.

Depending on the case, we may process such data where: you have given explicit consent; processing is necessary for carrying out obligations and exercising specific rights in employment, social security or social protection law; processing is necessary to protect vital interests; processing is carried out in the course of legitimate activities by a non-profit body; the data has been manifestly made public by you; processing is necessary for the establishment, exercise or defence of legal claims; an important public interest justifies it; processing is necessary for occupational medicine or assessing working capacity; or another legal exception applies.

Where we rely on explicit consent, it is obtained separately, actively, specifically and in a documented manner; pre-ticked boxes do not constitute valid consent.

Where necessary, sensitive data is limited to what is strictly necessary, accessible only to a restricted number of persons and protected by enhanced confidentiality and security measures.

8. Marketing and right to object

Where we use your data for marketing purposes, we provide the required information and a simple way to object. In commercial prospecting matters, the right to object may be exercised at any time and without justification, and we stop the relevant processing as soon as possible, subject to applicable legal exceptions.

When we send emails, SMS, MMS or use automated calling systems, we apply the applicable rules on consent or objection depending on the type of recipient and the relationship context.

For consumers, commercial electronic marketing generally requires prior consent; for professionals, a simple and free opt-out mechanism may apply under the conditions set by law.

9. Telemarketing

In France, telemarketing to consumers is subject to the applicable rules, including the strengthened rules from 11 August 2026 and, where applicable, Bloctel before that date and for situations still subject to it.

From 11 August 2026, unsolicited commercial calls to consumers may only be made in cases permitted by law and, where required, on the basis of prior, free, specific, informed and unambiguous consent.

For business contacts, we may use a simple and free opt-out mechanism, subject to specific rules applicable to the sector or context.

10. Recipients

Data may be shared with group companies, internal teams, technical providers, hosting providers, CRM tools, marketing tools, payment providers, event partners, external advisers, public authorities and strictly necessary third parties.

Where providers act as processors, they are bound by contract, documented instructions and confidentiality and security obligations.

11. Transfers outside the EEA

Where data is transferred outside the European Economic Area, we use an appropriate mechanism such as the European Commission standard contractual clauses, binding corporate rules or an adequacy decision, as applicable.

Where necessary, we perform a transfer risk assessment and implement supplementary technical, contractual or organisational measures.

12. Retention

We retain data for as long as necessary for the purposes pursued and thereafter for the applicable legal or limitation periods in France.

More precise periods may be set out in our internal retention policy or in a dedicated annex.

13. Security

We apply appropriate technical and organisational measures: access controls, rights segregation, logging, encryption where relevant, backups, privilege management, staff awareness and incident response procedures.

Access is limited to those who need to know and are bound by confidentiality obligations.

14. Your rights

Subject to the conditions set out in the law, you have rights of access, rectification, erasure, restriction, objection and portability.

Where processing is based on consent, you may withdraw it at any time without retroactive effect on processing already carried out.

You may exercise your rights by contacting the contact point above and may also lodge a complaint with the CNIL.

15. Updates

We may update this policy at any time. The applicable version is the one published through our official channels.

In the event of a material change, we will take appropriate steps to inform you.