

Privacy Policy

Version: 1.5 · Effective date: 2 March 2026 · Last updated: 11 October 2026

1. Controller

The controller of your personal data is:

WIDECLERK, LDA. · NIPC (legal-person number): 516 434 080 · Registered office: Praça das Flores, N.º 45, 1200-257 Lisboa, Portugal · Email: privacy@wideclerk.com

Data Protection Officer (DPO): to be appointed (in accordance with Article 37 of the GDPR, Wideclerk will assess the need for the formal appointment of a DPO).

2. Personal Data We Collect

2.1. Data provided directly by the user

CATEGORY	DATA	PURPOSE
Identification data	Name, email, telephone, job title	Account management and communication
Company data	Company name, tax number (NIF/NIPC), address, business sector	Provision of the Services
Access data	Authentication credentials (encrypted)	Access to the Platform
Financial data	Billing details, IBAN (for payment)	Subscription management

2.2. Data collected automatically

CATEGORY	DATA	PURPOSE
Usage data	Pages visited, features used, timestamps	Improvement of the Services
Technical data	IP address, browser type, operating system, screen resolution	Security and compatibility
Cookies	Session identifiers, preferences	See the Cookie Policy
Access logs	Login date/time, actions on the Platform	Security and auditing

2.3. Data processed on behalf of the Client (processing)

CATEGORY	EXAMPLES	LEGAL BASIS
Tax data	Suppliers' tax numbers, invoice numbers, amounts	Performance of the contract
Supplier data	Suppliers' names, addresses, contact details	Performance of the contract
Banking data	Statements, transactions, IBANs	Performance of the contract
e-Fatura data	Documents from the Portuguese Tax Authority portal (Portal das Finanças)	Performance of the contract

This data is the exclusive property of the Client. Wideclerk processes it only on the Client's instructions and under the terms of the DPA.

2.4. Advertising and campaign attribution

Wideclerk advertises its own services on Instagram and Facebook (Meta) and publishes posts on Instagram and LinkedIn, some of them scheduled with a publishing tool (Buffer). The links in our adverts, posts and emails lead to wideclerk.com and may carry campaign parameters in the address (utm_source, utm_medium, utm_campaign, utm_content, utm_term), which say which campaign and which advert the visit came from. The advertising platforms may add their own click identifier to the address (for example fbclid).

- **What we record.** When you book a call through our scheduling page (Cal.com) or submit a form on our website (for example, to receive the margin guide), we record with your contact details, in our record of business contacts, the campaign parameters, the address of the page you came from (*referrer*) and the page where you arrived or submitted the form. We do not record click identifiers.
- **What stays on your device.** While you browse the website, the campaign travels in the page address. It is remembered between visits only if you accept the *Advertising* category; see section 3.4 of the Cookie Policy.
- **What we do not do.** We do not install the Meta pixel, the Meta Conversions API, the LinkedIn Insight Tag or any other advertising tag on our website, and we do not send data about website visitors or about our Clients to Meta or LinkedIn.
- **Meta and LinkedIn.** When you see or click an advert or a post on Instagram, Facebook or LinkedIn, those platforms process data about you as independent controllers, under their own privacy policies: Meta (www.facebook.com/privacy/policy) and LinkedIn (www.linkedin.com/legal/privacy-policy). They are not sub-processors of Wideclerk.
- **Legal basis, retention and objection.** Recording which campaign brought a contact is based on our legitimate interest in knowing which marketing brings contacts (Art. 6(1)(f) GDPR). This data is kept with the contact record, for as long as that record is kept (see section 6). You may object at any time by writing to privacy@wideclerk.com (Art. 21 GDPR); we will then remove this data from your record.

2.5. Business outreach email

Wideclerk sends a small number of emails to businesses it believes could use its services, mainly hospitality groups with several sites. This section explains what we hold about the people we write to, and how those emails work.

- **Where the details come from.** We find businesses in Google Maps business listings and look them up on their own websites and in public web search results, including public LinkedIn pages. We may use an artificial-intelligence research tool (Claude, from Anthropic, through Google Cloud) to read those public sources. We may also obtain a person's work email address from a business-contact data provider, Apollo.io, which processes that data as an independent controller under its own privacy policy (www.apollo.io/privacy-policy). We did not collect these details from you directly.
- **What we record.** The business's name, address, website and telephone number; the name, job title, business email address and public LinkedIn page of the person we write to; the emails we send and whether they were delivered; whether an email was opened; and any reply or unsubscribe.

- **Open measurement.** Our outreach emails contain a small image that our email provider (Resend) loads when the email is opened. It tells us whether and when the email was opened. Every outreach email says so in its footer, and turning off images in your email program blocks it. Our other emails, including invoices and account emails, do not contain this image.
- **How many, and how to stop them.** We send a person at most three emails in a sequence, and we stop when you reply, book a call or unsubscribe. Every email has a one-click unsubscribe link. When you unsubscribe, we keep your email address on a suppression list, only so that we never write to it again.
- **Legal basis, retention and objection.** Writing to businesses about a service relevant to their work is based on our legitimate interest in offering our services (Art. 6(1)(f) GDPR). These details are kept with the contact record, for as long as that record is kept (see section 6); the suppression list is kept for as long as we send outreach email. You may object at any time, through the unsubscribe link or by writing to privacy@wideclerk.com (Art. 21 GDPR), and you may ask what we hold about you and where it came from (Art. 15 GDPR).

3. Legal Bases for Processing

PURPOSE	LEGAL BASIS (GDPR ARTICLE)
Performance of the contract for the provision of the Services	Art. 6(1)(b) — Performance of a contract
Processing of data on behalf of the Client	Art. 6(1)(b) + Art. 28 — Processing
Issuing invoices and financial management	Art. 6(1)(c) — Legal obligation
Fraud prevention and security	Art. 6(1)(f) — Legitimate interest
Improvement of the Services and usage analysis	Art. 6(1)(f) — Legitimate interest
Recording the campaign that brought a contact (2.4)	Art. 6(1)(f) — Legitimate interest
Business outreach email, including open measurement (2.5)	Art. 6(1)(f) — Legitimate interest

4. Data Sharing

4.1. Sub-processors

Wideclerk uses sub-processors for the provision of the Services, in the following categories:

- **Infrastructure and hosting** — database, authentication, application hosting;
- **Payments** — card and SEPA Direct Debit payment processing;
- **Invoicing and tax obligations** — issuing certified documents and reporting to the Tax Authority;
- **Bank aggregation** — connection to the Client's bank accounts, with consent, under PSD2;
- **Communications** — transactional email and operational alerts;
- **Artificial intelligence and document reading** — classification, extraction and optical character recognition;
- **Documents and productivity** — document storage and sharing with the Client;
- **Business tools** — meeting scheduling and prospecting.

The complete and up-to-date list of sub-processors, identifying each entity, its purpose, its location and the applicable safeguards, is available at wideclerk.com/legal/en/subprocessors.html. Wideclerk notifies its Clients of any change to that list at least 30 (thirty) days in advance, and the Client may object under the terms of the DPA (Article 28(2) of the GDPR).

4.1-A. Access to the Client's systems

The Platform connects to systems contracted by the **Client itself** — namely point-of-sale (POS) systems, property management systems (PMS), certified invoicing platforms, accounting and ERP platforms, and bank accounts.

Wideclerk accesses those systems at the Client's request and with the Client's agreement, using credentials or authorisations supplied by the Client, and **exclusively to access the Client's own account** and read its data. Wideclerk does not create, contract or manage accounts on those systems, nor does it transmit personal data to them for processing on its behalf.

For that reason, **the providers of those systems are not sub-processors of Wideclerk**: the contractual and data-protection relationship concerning them is, and remains, between the Client and the respective provider. Wideclerk's sub-processors — those Wideclerk engages on its own account — are the ones identified in 4.1 and listed on the page indicated there. The Client acknowledges and accepts this access when accepting the Commercial Proposal.

4.2. International transfers

Some sub-processors may process data outside the European Economic Area (EEA). In those cases, we ensure the protection of the data through: Standard Contractual Clauses (SCCs) approved by the European Commission; adequacy decisions of the European Commission; approved certifications and codes of conduct.

4.3. We do not sell data

Wideclerk never sells, rents or trades the personal data of its users or clients to third parties.

4.4. Mandatory disclosure

We may disclose personal data where legally required by: a court order or an order of a competent authority; tax or regulatory obligations; the protection of the rights, property or safety of Wideclerk or of third parties.

5. Data Isolation (GDPR — Security by Design)

5.1. Wideclerk implements strict data isolation between Clients: each Client is identified by its tax number (NIF); all data is segmented by `client_id` at the database level; Row-Level Security (RLS) in Supabase guarantees isolation at the database level; each Client has its own storage space in Google Drive; no user can access another Client's data.

5.2. This isolation is guaranteed by design (*privacy by design*) and by default (*privacy by default*), in accordance with Article 25 of the GDPR.

6. Data Retention

TYPE OF DATA	RETENTION PERIOD	JUSTIFICATION
Account data	Duration of the contract + 30 days	Post-contract data export
Processed financial data	Duration of the contract + statutory period	Tax obligations (10 years, Article 123 of the Portuguese Corporate Income Tax Code — CIRC)
Access and audit logs	12 months	Security and compliance
Usage data (analytics)	24 months	Improvement of the Services
Marketing data	Until consent is withdrawn	Consent
Billing data	10 years	Portuguese tax obligation
Campaign origin of a contact (2.4)	For as long as the contact record is kept	Measuring which marketing brings contacts
Business outreach contacts (2.5)	For as long as the contact record is kept	Business outreach
Unsubscribed email addresses (2.5)	For as long as we send outreach email	Never writing to that address again

After the retention period, the data is securely and irreversibly deleted, or anonymised where technically feasible.

7. Rights of Data Subjects

RIGHT	DESCRIPTION	HOW TO EXERCISE IT
Access (Art. 15)	Obtain confirmation and a copy of the data processed	privacy@wideclerk.com
Rectification (Art. 16)	Correct inaccurate or incomplete data	Email or directly on the Platform
Erasure (Art. 17)	Request the deletion of the data	privacy@wideclerk.com
Restriction (Art. 18)	Restrict processing in certain circumstances	privacy@wideclerk.com
Portability (Art. 20)	Receive the data in a structured, machine-readable format	privacy@wideclerk.com
Objection (Art. 21)	Object to processing based on legitimate interest	privacy@wideclerk.com
Withdrawal of consent	Withdraw consent at any time	Email or Platform

7.1. Response time: 30 (thirty) days from receipt of the request, extendable by 60 days in complex cases, upon notice.

7.2. Identity verification: for security reasons, we may request proof of identity before responding to requests.

7.3. Complaints: the data subject has the right to lodge a complaint with the Portuguese supervisory authority, the Comissão Nacional de Proteção de Dados (CNPd): www.cnpd.pt.

8. Data Security

8.1. Technical measures: encryption of data in transit (TLS 1.2+) and at rest (AES-256); multi-factor authentication (MFA) for access to the Platform; Row-Level Security (RLS) for data isolation; continuous monitoring and intrusion

detection; regular backups with geographic replication; firewall and DDoS protection.

8.2. Organisational measures: least-privilege principle (*need-to-know*); staff training in data protection; security incident management policy; periodic review of access and permissions; confidentiality agreements with all staff.

For further details, see the Security Policy.

9. Data Breach

9.1. In the event of a personal data breach, Wideclerk will: notify the CNPD within 72 (seventy-two) hours of becoming aware of it, in accordance with Article 33 of the GDPR; notify the affected Clients without undue delay, where the breach is likely to result in a high risk to the rights of data subjects (Article 34 of the GDPR); document all breaches, their effects and the remedial action taken.

10. Cookies

The use of cookies on the Platform is governed by the Cookie Policy, which forms an integral part of this Privacy Policy.

11. Minors

The Platform is not intended for persons under 18 years of age. Wideclerk does not knowingly collect personal data from minors. If we become aware that we have collected data from a minor, we will delete it immediately.

12. Changes to the Privacy Policy

12.1. Wideclerk may update this Privacy Policy at any time, and changes will be communicated by: publication on the Platform; email to the address registered on the Client's Account; in-app notification.

12.2. Changes come into force 15 (fifteen) days after they are communicated, unless otherwise required by law. Changes to the list of sub-processors follow the 30-day period provided for in 4.1.

13. Contacts

Controller

Email: privacy@wideclerk.com

Address: Praça das Flores, N.º 45, 1200-257 Lisboa, Portugal

Supervisory Authority

Comissão Nacional de Proteção de Dados (CNPD)

Rua de São Bento, 148-3.º, 1200-821 Lisboa, Portugal · www.cnpd.pt

LEGAL REVIEW — PENDING

This Privacy Policy was drawn up in compliance with Regulation (EU) 2016/679 (GDPR), Portuguese Law no. 58/2019 of 8 August (the Portuguese GDPR implementation law) and other applicable Portuguese and European legislation. Review by a lawyer specialising in data protection is recommended before publication.

[PENDING] ☐ Formal appointment of the DPO (where applicable) ☐ Legal review by Dr. Samuel Oliveira (Portuguese Bar Association card no. 59720L, Lisbon district, registration no. 271667).

Binding version. This document was drawn up in the English language. Any translations into other languages are provided solely for the reader's convenience. In the event of any divergence or conflict of interpretation between language versions, the English-language version always prevails. This concerns the language of interpretation only: the applicable law stated in this document, and any forum it agrees, are unchanged.