

Privacy policy

Version 1.0 | Last updated on 01/01/2026 | Effective starting 01/01/2026

This Privacy Policy explains how Confidus Comm.V – SCS ("**Confidus**", "**we**", "**us**", or "**our**") collects, uses, stores, and protects personal data when you visit our websites, contact us, use our software-as-a-service products, engage us for IT management or custom software development services, or otherwise interact with our company.

1 Introduction

1.1 Data controller

The data controller for this Privacy Policy is Confidus Comm.V – SCS, with registered office at Rue de la Victoire 57/1, 1060 Brussels, Belgium, registered with the Belgian Crossroads Bank of Enterprises under registration number 0839.449.975. You can contact us at info@confidus.be or through the contact details listed at the end of this policy.

1.2 Scope of this policy

This policy covers:

- Visitors to our websites and online resources
- Customers and users of our software-as-a-service products
- Clients receiving IT management, consultancy, support, hosting, integration, or custom software development services
- Prospects, suppliers, partners, newsletter subscribers, and other business contacts
- Our general data processing activities as a controller and, where applicable, as a processor acting on behalf of our clients

Depending on the context, Confidus may act either as a data controller, for example when managing its own customer, supplier, marketing, billing, website, and support data, or as a data processor when processing personal data on behalf of a client in connection with managed IT services, hosting, support, integrations, SaaS products, or custom software development. Processor activities are governed by a separate Data Processing Agreement or equivalent contractual terms agreed with the client.

1.3 Our commitment to privacy

We are committed to protecting your privacy and ensuring compliance with the General Data Protection Regulation (GDPR), the Belgian Data Protection Act of July 30, 2018, and all applicable Belgian and European data protection laws.

Pagina 1 van 8

2 Personal data we collect

2.1 Data you provide directly

When you contact us, request a quote, enter into an agreement with us, create an account for one of our services, or receive support, we may collect personal information such as your name, email address, phone number, company name, job title, billing address, VAT number, contract details, and communication preferences. Where relevant for billing or payments, we may process invoice details, payment confirmations, purchase orders, and related accounting information.

In the context of IT management, SaaS delivery, integrations, hosting, support, or custom software development, we may process account settings, service configuration data, user roles and permissions, support tickets, project documentation, technical requirements, issue reports, logs, screenshots, diagnostic information, system inventory data, integration credentials, API keys, OAuth tokens, and other information you provide or authorize us to access. We only request and use such information to the extent necessary for the agreed services, security, troubleshooting, development, maintenance, or legal compliance.

2.2 Data collected automatically

We automatically collect certain technical data when you visit our websites, use our online services, or interact with systems we manage or support. This may include IP addresses, browser and device information, operating system details, access times, pages visited, referring sources, session identifiers, authentication events, audit logs, error logs, diagnostic information, usage statistics, and security events. This data helps us operate secure, reliable, and performant services.

Our use of cookies and tracking technologies supports various essential functions. Some cookies are required for session management and security purposes and cannot be disabled. We also use analytics cookies, such as those from Google Analytics, to monitor website performance. Marketing cookies, including those from HubSpot and Brevo, help us track the effectiveness of our campaigns. Preference cookies are used to remember your settings and enhance your experience.

2.3 Data from third parties

We may receive data from third-party sources when this is necessary to deliver or support our services. This can include information from identity providers, cloud platforms, hosting providers, payment processors, collaboration tools, monitoring tools, ticketing systems, analytics tools, CRM or marketing platforms, client systems, and other software or infrastructure that you ask us to connect, administer, integrate, maintain, or troubleshoot. We may also receive business contact information from public sources, referrals, events, or professional networks.

3 Legal basis for processing

We process your data under GDPR Article 6 based on:

- **Contractual necessity** (6(1)(b)): Account creation, service delivery, billing, support
- **Legitimate interest** (6(1)(f)): Security monitoring, fraud prevention, analytics, service improvement, business continuity
- **Legal obligation** (6(1)(c)): Tax compliance, accounting records, regulatory reporting
- **Your consent** (6(1)(a)): Marketing emails, non-essential cookies, case studies, public customer references

You may withdraw consent at any time without affecting prior lawful processing.

4 How we use your data

We use personal data to respond to enquiries, prepare offers, manage contracts, deliver IT management and support services, develop, maintain, host, secure, and improve software products and custom applications, administer user accounts and access rights, process billing and accounting records, provide customer support, monitor service performance and security, detect and prevent fraud or misuse, manage suppliers and business relationships, send service-related communications, provide marketing communications where permitted, and comply with legal, tax, accounting, and regulatory obligations.

5 Who we share your data with

5.1 Subprocessors

We may use third-party services that have access to parts of your data. All service providers are contractually required to maintain GDPR compliance and process data only per our instructions. Data transfers outside the EU are protected by Standard Contractual Clauses (SCCs) and/or EU-US Data Privacy Framework.

Complete details about all subprocessors, including contact information and GDPR documentation links, are provided in Appendix A of our Data Processing Agreement.

5.2 Client systems, integrations, and external platforms

When we access, connect to, administer, integrate, or troubleshoot client systems, cloud environments, SaaS platforms, APIs, databases, networks, devices, or business applications, we do so based on the client's instructions and the agreed scope of services. These platforms and environments remain under the client's responsibility unless explicitly agreed otherwise. Clients are responsible for ensuring that they have the necessary rights and legal basis to allow us to access or process personal data in those systems.

5.3 Legal requirements

We may disclose your data when required by law (court orders, regulatory requests, law enforcement) or to protect our rights or prevent fraud.

5.4 Business transfers

In case of merger, acquisition, or asset sale, your data may transfer to the successor entity (with email notification).

5.5 No data sales

We do not sell or monetize your personal data to third parties.

6 Data retention

We retain personal data only for as long as necessary for the purposes described in this policy, unless a longer retention period is required by law or justified by legitimate business needs. Customer, supplier, contract, project, support, and account data are retained during the business relationship and for a reasonable period afterwards to manage follow-up, warranty, audit, dispute, compliance, and continuity requirements. Operational logs, audit logs, diagnostic data, and security records are retained for periods appropriate to security, troubleshooting, and legal needs. Invoices and accounting records are kept for seven years in accordance with Belgian accounting requirements, and tax-related records may be kept for ten years where required. Marketing-related data is retained until you unsubscribe, withdraw consent, object to processing, or after prolonged inactivity.

If you wish to have your personal data deleted or amended, you may submit a request by emailing info@confidus.be. We will respond to data subject requests within the applicable GDPR deadlines, unless legal retention obligations, contractual obligations, security requirements, or legitimate interests require us to retain certain information for a specified period.

7 Your rights under GDPR

You have several rights under the GDPR regarding your personal data. These include the right to access your data, correct inaccuracies, delete your information, restrict processing, receive your data in a structured and portable format, object to certain processing activities, and withdraw consent where processing is based on consent. You also have the right to lodge a complaint with the Belgian Data Protection Authority. To exercise your rights, you can email info@confidus.be with the subject line "Data Subject Rights Request." We will respond within one month, although this period may be extended to three months for complex requests. Where we process data on behalf of a client as processor, we may refer your request to that client as the relevant controller.

8 Confidentiality & security

8.1 Personnel obligations

Confidus ensures that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality. Employees, contractors, and service providers with access to personal data are required to follow confidentiality obligations, receive appropriate data protection and security guidance, comply with applicable policies and laws, and access personal data only where necessary for service delivery, support, development, security, or administration.

8.2 Technical and organizational security measures

Confidus implements and maintains appropriate technical and organizational security measures to ensure a level of security appropriate to the risk, taking into account the nature of the services provided, the systems involved, and the information processed. These measures may include:

- **Encryption:** TLS/HTTPS (min. 256-bit) for data in transit; AES-256 encryption for data at rest; encrypted connections to external platforms.
- **Access controls:** role-based access control limiting access to authorized personnel only; multi-factor authentication for administrative access; unique identification and authentication for each user; regular access reviews and revocation of unnecessary permissions.
- **Monitoring & detection:** audit logging of access to Personal Data; security monitoring and alerting; regular vulnerability scanning; regular penetration testing.
- **Infrastructure security:** firewall protection and network segmentation; DDoS mitigation and intrusion detection systems; regular security patches and dependency updates; physical access control to data centers under cloud provider responsibility.

8.3 Measures for Data Subjects' rights

Where Confidus acts as processor, and taking into account the nature of the processing, we will reasonably assist the client as controller in responding to data subject rights requests by implementing suitable technical and organizational measures. This assistance may cover requests for access, rectification, erasure, restriction, portability, and objection, subject to the terms of the applicable agreement and the client's instructions.

We will respond to reasonable requests for assistance within a commercially reasonable timeframe, taking into account the urgency of the request and the GDPR deadlines applicable to the controller.

9 Cookies

9.1 What are cookies?

Cookies are small text files stored on your device when you visit our website. They help us provide, protect, and improve our service.

9.2 Types of cookies we use

Confidus may use the following types of cookies and similar technologies on its websites and online services.

Essential cookies are always active and are required for the proper functioning of the service. These cookies handle key tasks such as session management, user authentication, security protection (including CSRF prevention) and maintaining account access and login status. The use of essential cookies is based on contractual necessity as outlined in Article 6(1)(b) of the GDPR, and they cannot be disabled.

Preference cookies are used to remember choices and settings, such as language preferences, interface preferences, and cookie consent decisions. The legal basis for preference cookies is our legitimate interest in providing a user-friendly service or, where legally required, your consent.

Analytics cookies help us understand how visitors interact with our websites and online services, including pages visited, navigation patterns, device and browser details, approximate geographic location, and traffic sources. Analytics cookies are used only where permitted by law and, where required, with your consent.

Marketing cookies support personalized marketing efforts and the tracking of campaign effectiveness.

10 Children's privacy

Confidus provides business-to-business IT, software, and related services and does not intentionally target children. We do not knowingly collect personal data from children through our websites or services.

11 Marketing communications

Confidus may communicate with customers, users, prospects, partners, and other business contacts through service-related and marketing communications. Service-related communications, such as support responses, security notices, invoices, contractual information, operational updates, and important service messages, may be sent where necessary for the business relationship. Marketing communications, such as newsletters, product updates, events, promotions, insights, or case studies, are sent only where permitted by law or where you have provided consent.

If you wish to stop receiving marketing communications, you can unsubscribe by clicking the "unsubscribe" link included in any marketing email, adjusting your preferences where available, or emailing info@confidus.be.

12 International data transfers

Where possible, we use service providers and hosting locations within the European Economic Area. Some providers, software tools, support processes, or cloud services may involve transfers of personal data outside the EEA. In such cases, we rely on appropriate safeguards, such as EU Standard Contractual Clauses, adequacy decisions, the EU-US Data Privacy Framework where applicable, encryption, access controls, and contractual commitments with our service providers.

13 Supervisory authority

If you have concerns regarding your data privacy, you may contact the Belgian Data Protection Authority at Rue de la Presse 35, 1000 Brussels, by phone at +32 (0)2 274 48 00, or via email at contact@apd-geb.be. Additional information is available on their website <https://www.dataprotectionauthority.be>. You have the right to lodge a complaint with the authority at any time without needing to contact us first.

14 Contact information

If you have any questions about privacy, you can contact us by email at info@confidus.be, by phone at +32 (0)2 315 30 20, or by mail at Confidus Comm.V – SCS, Rue de la Victoire 57/1, 1060 Brussels, Belgium. For requests related to data subject rights, please email info@confidus.be with the subject line "Data Subject Rights Request."

15 Changes to this policy

We may update this policy to reflect changes in our services, technologies, processing activities, supplier relationships, security practices, or legal requirements. Where changes are material, we will take reasonable steps to inform affected users or clients, for example by email, contractual notice, publication on our website, or another appropriate communication channel.