Sekur Private Data Launches Sekur.com in French in Preparation for Sales in the Democratic Republic of the Congo and Switzerland

French will facilitate sales in the Democratic Republic of the Congo and other French-speaking countries in Europe and Africa, such as Switzerland, Morocco, Algeria, and Côte d'Ivoire

---

MIAMI, FL — October 13, 2026 — Sekur Private Data, Inc., a Miami-based Swiss-hosted cybersecurity, private communications, and defense communications company serving enterprise, government, and defense clients, and a wholly owned U.S. subsidiary of Sekur Private Data (OTCQB: SWISF | CSE: SKUR | FRA: GDT0) ("Sekur" or the "Company"), today announced that it has launched its Sekur.com website in French, its third additional language after Spanish and Portuguese, with additional languages planned, in preparation for sales in the Democratic Republic of the Congo ("DRC").

As part of its Africa and International expansion, Sekur has begun translating its website, workflows, and onboarding into the local languages of its upcoming partners. French is the official language of the DRC, the largest French-speaking country in the world by population, where Sekur already has a team on the ground and expects to begin sales in the first quarter of 2027 or earlier. The French-language site can be viewed at https://sekur.com/fr.

"We are very pleased to be expanding Sekur internationally and to make our solutions available in multiple languages," said Alain Ghiai, Founder and CEO of Sekur Private Data. "French is the third additional language we have added, following Spanish and Portuguese, and it allows us to serve clients and partners in the DRC and across French-speaking Europe and Africa in their own language."

"Localization is not a cosmetic exercise for us. Our website, onboarding, and workflows need to work in the language our partners operate in every day. That is what makes an international expansion real, and it is how we intend to approach each new market we enter."

The Democratic Republic of the Congo: A Critical Minerals Hub Facing Security Challenges

The DRC is one of the world's most important commodity hubs. It produces around 70% of the world's cobalt, is one of the largest copper producers in the world, and holds significant reserves of other critical minerals, including coltan, lithium, and gold, that are essential to electric vehicles, electronics, and the global energy transition. Mining companies, commodity traders, financial institutions, and government agencies operating in and around the DRC handle highly sensitive information on production, exports, contracts, and pricing every day.

At the same time, certain regions of the country, particularly the eastern provinces of North Kivu and South Kivu, continue to face armed conflict and instability. In this environment, communications that can be intercepted, tracked, or disrupted put personnel, operations, and confidential business information at risk. Government agencies, defense and security forces, humanitarian organizations, and companies with operations in the field need secure communications that protect their identity, their location, and their information.

Sekur's solutions, including SekurOne, SekurMail, SekurMessenger, and SekurVPN, are designed for exactly these environments. They operate independently of conventional telecom infrastructure, do not location-track their users, and require no phone number, helping protect people and sensitive information in contested areas. With its team already on the ground and its French-language site now live, Sekur is positioned to serve government, defense, mining, and commodity clients across the DRC in their own language.

Switzerland: A Commodity Trading Hub and a High-Value Cyber Target

Switzerland is one of the world's leading commodity trading hubs, and Geneva in particular is home to some of the biggest commodity trading companies in the world. These firms handle highly sensitive information every day, including pricing, cargo and shipping data, counterparty negotiations, and trade financing arrangements. For these companies, secure communications such as Sekur are essential to protecting confidential corporate information from competitors, criminals, and state-sponsored actors.

Switzerland is also home to some of the wealthiest individuals in the world, as well as the family offices and wealth management firms that serve them. Their communications carry information about assets, investments, transactions, and personal security that is highly valuable to criminals. Sekur offers these individuals and their advisors protection with SekurOne, its fully encrypted voice/video, email, messaging, and VPN platform. With no phone number required and Call-by-Invite access only, SekurOne keeps private conversations private and guards against interception, tracking, and Pegasus-style malware.

Switzerland has recently been a target of hackers, and commodity trading companies, family offices, wealth management firms, and other high-value organizations remain prime targets. In October 2025, Swiss federal authorities reported that the Akira ransomware group alone had attacked around 200 companies in Switzerland, causing damage of several million Swiss francs, as reported by Swissinfo. According to the authorities, attackers typically gain access through outdated systems and remote access connections, such as VPNs, that lack two-factor authentication.

Sekur's Swiss-hosted solutions, built on proprietary architecture with no reliance on Big Tech, are designed to close these gaps. With its new French-language site, Sekur can now serve Geneva's commodity trading, family office, and wealth management communities, and the broader French-speaking business community in Switzerland, in their own language.

Sekur Core Communications Solutions

Sekur delivers secure communications that work within and beyond the Sekur network, operating independently of conventional telecom infrastructure to reduce exposure to interception, SIGINT collection, traffic analysis, metadata exploitation, and hostile surveillance in contested environments. No Sekur solution data-mines or location-tracks its users.

All solutions are built on proprietary architecture with zero reliance on Big Tech, meeting the privacy, security, and OPSEC requirements of intelligence agencies, defense and federal organizations, military commands, diplomatic missions, government agencies, executives, and professionals handling CUI and other sensitive, mission-critical information. Deployments are supported by on-premises infrastructure options for full data sovereignty, mission assurance, and sole control over keys and data.

SekurOne — Encrypted Voice/Video, Email, Messaging, and VPN

A fully encrypted communications platform engineered on proprietary HeliX data transfer architecture, purpose-built to defeat telecom network tracing, resist Pegasus-style malware intrusion, and support CUI handling requirements. SekurOne is designed for defense and federal officials, military commanders, government leaders, and executives conducting confidential, operational, or sensitive conversations where standard carrier-based voice and video platforms present unacceptable interception and exploitation risk.

Call-by-Invite capability via SMS or SekurSend email ensures controlled access and eliminates unsolicited contact. Each user is assigned a unique Sekur ID for identity management, with no phone number required — preserving user privacy across all voice and video communications.

SekurMail — Secure Business and Executive Email

An enterprise- and government-grade encrypted email platform designed for defense and federal agencies, military commands, senior government officials, C-suite executives, and organizations handling confidential and operationally sensitive communications, including CUI correspondence. Built on proprietary architecture with zero Big Tech dependencies and no metadata tracking, SekurMail keeps sensitive communications private between sender and recipient.

Key capabilities include SekurSend/SekurReply for secure delivery to non-Sekur recipients without exposing sender identity or message content; full message delivery control and audit capability; encrypted file transfer; custom domain support for organizational integration; and active protection against phishing, social engineering, and Business Email Compromise (BEC) attacks targeting corporate and administrative networks.

SekurMessenger — Secure Team Messaging and Collaboration

A secure messaging platform providing end-to-end encrypted text, file transfer, voice messages, and collaboration capabilities for defense, military, government, and executive teams coordinating operational and mission-sensitive information, including CUI material. Features include self-destructing messages, encrypted file transfers, and compliance-grade archiving for recordkeeping and audit requirements.

Cross-network secure communications with non-Sekur users are supported via Chat-by-Invite, enabling secure coordination with coalition partners, external agencies, and field elements without compromising the network. Each user is assigned a unique Sekur ID for identity verification and contact authentication, with no phone number required.

SekurVPN — Enterprise Network Security and Identity Protection

An enterprise-grade Virtual Private Network leveraging proprietary HeliX encryption technology, engineered to provide secure internet access, identity obfuscation, and traffic protection for defense organizations, military and federal personnel, government agencies, and executives operating across remote, traveling, deployed, forward, or untrusted network environments.

SekurVPN maintains zero data logging, ensuring no record of user activity exists that could be exposed through legal process, network compromise, or third-party collection. It is built for defense, government, and executive use cases — including protection of traffic associated with CUI and operationally sensitive workflows — where standard commercial VPN solutions present unacceptable privacy and security risk.

SekurRelay — Executive-Level Secure Email Integration

An enterprise-grade secure email relay solution enabling domain splitting, which allows organizations to establish secure communications at the executive, board, or senior staff level without requiring full organizational migration or infrastructure overhaul.

SekurRelay removes one of the most significant barriers to large-scale defense, government, and enterprise deployment, enabling phased adoption that protects command leadership, flag officers, and the highest-value personnel and communications immediately while broader organizational rollout proceeds. It is designed for defense and government organizations, regulated industries, and enterprises requiring rapid, low-friction elevation of communications security at the command and executive tier, including environments handling CUI communications.

About Sekur Private Data

Sekur Private Data is a Swiss-hosted cybersecurity, defense communications, and privacy solutions provider, offering a secure suite of tools to protect governments, defense and federal agencies, businesses, and individuals from unauthorized access and cyber threats. With capabilities such as SekurOne, SekurMail, SekurMessenger, and SekurVPN, Sekur provides a reliable and secure means of digital communication and data storage for Controlled Unclassified Information (CUI), classified-adjacent and civilian communications use, grounded in Swiss privacy standards with on-premises infrastructure for government agencies, allowing for data sovereignty. Sekur sells its solutions through its website **www.sekur.com**, approved distributors and telecommunications companies globally, and through the **U.S. General Services Administration (GSA) Multiple Award Schedule (MAS), Contract No. 47QTCA18D0089** serving governments, defense institutions, federal agencies, businesses, and consumers worldwide. Sekur's main sales operations are in Miami, USA.

Contact

Alain Ghiai
President and Chief Executive Officer
Sekur Private Data
Email: investors@sekur.com
Tel: +1.305.347.5114
https://sekur.com/en/company/investors

Follow Sekur on X and LinkedIn.

To find out more about Sekur, visit https://sekur.com

###

Forward-Looking Information

This news release contains certain forward-looking information within the meaning of applicable Canadian securities laws ("forward-looking statements"). All statements other than statements of present or historical fact are forward-looking statements. Forward-looking statements are often, but not always, identified by the use of words such as "anticipate", "achieve", "could", "believe", "plan", "intend", "objective", "continuous", "ongoing", "estimate", "outlook", "expect", "project" and similar words, including negatives thereof, suggesting future outcomes or that certain events or conditions "may" or "will" occur. These statements are only predictions. These statements reflect management's current estimates, beliefs, intentions and expectations; they do not guarantee future performance. Sekur cautions that all forward-looking statements are inherently uncertain, and that actual performance may be affected by a number of material factors, many of which are beyond Sekur's control. Such factors include, among other things: risks and uncertainties relating to the future of the Company's business; the success of marketing and sales efforts of the Company; the projections prepared in house and projections delivered by channel partners; the Company's ability to complete the necessary software updates; increases in sales as a result of investments in software development technology; consumer interest in the Products; future sales plans and strategies; reliance on large channel partners and expectations of renewals to ongoing agreements with these partners; anticipated events and trends; the economy and other future conditions; and other risks and uncertainties, including those described in Sekur's prospectus dated May 8, 2019, filed with the Canadian Securities Administrators and available on www.sedarplus.ca. Accordingly, actual and future events, conditions and results may differ materially from the estimates, beliefs, intentions and expectations expressed or implied in the forward-looking information. Except as required under applicable securities legislation, Sekur undertakes no obligation to publicly update or revise forward-looking information.