Exhibit 3 - Technical and organizational security measures

Version 2.0

Retriever implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

1. Technical Security Measures

1.1 Access Control

Our security measures for access control encompass a comprehensive range of aspects, from safeguarding physical infrastructure to preventing unauthorized access and managing role-based data access rights.

Access to Facilities: We utilize both on-premises and cloud infrastructure providers to host our products. All our data center providers hold ISO-27001 certification and implement robust physical security measures. This includes round-the-clock operations, surveillance facilities, and strict access control procedures.

Protecting data on Physical Storage Devices: All storage devices containing personal data are protected by data-at-rest encryption using the AES-256 algorithm. Both production server and employee computer storage devices adhere to rigorous disposal procedures.

Access to Systems: Access to our production systems requires user authentication, either via username and password or through single sign-on (SSO). Anonymous access to any systems is strictly prohibited. When customers use passwords to log into our products, we do not store their actual passwords in our databases. Customers can also use their Active Directory (AD) for product access. Our company's AD is used to centrally manage employees' access to internal production systems, with approval required from IT administrators or department managers for all such access.

Access to Data: Customer data access is controlled through permissions that can be granted or revoked based on user duties. Our employees require explicit permissions to view and modify customer data in our internal administrative systems. Customers can also assign role-based permissions for their employees within our products.

1.2 Availability Control

Our availability control measures guarantee the safeguarding of data against accidental destruction or loss, while ensuring the continuous operation of our data processing services.

Redundancy and Failover: Our data centers provide uninterruptible power and network services, as well as other essential infrastructure. Various replication strategies are implemented to ensure redundancy and failover protection of our products and services in the event of a significant

infrastructure failure. For production databases, data replication is integral, with at least one primary and one secondary database.

Backups and Restoration: Scheduled backups cover all production data and employ AES-256 encryption. These backups are securely stored in geographically separated locations.

24/7 Operations: Our data centers provide continuous 24/7 monitoring and technical infrastructure troubleshooting. Additionally, we maintain a dedicated 24/7 Incident Response Team responsible for responding to any incidents affecting the performance of production services.

Disclosure control

Disclosure control measures are implemented to thwart unauthorized access, alteration, or removal of data during its transfer.

Transport Encryption: In our product, all production data is encrypted in transit over public networks. This encryption is accomplished using Transport Layer Security (TLS 1.2), ensuring the security and integrity of the data during transmission.

Private Networks: Most of our infrastructure operates on private networks, shielding data transfers from exposure to the Internet. Data transfers from these private networks necessitate secure VPN connections.

Security Testing: All new code undergoes thorough review by senior developers before deployment to production, with a strong focus on security. Additionally, static Security Analysers are employed to detect potential security issues in the code. Third-party companies are engaged to conduct penetration tests and simulate cyberattacks on our products.

1. Organizational Security Measures

Cybersecurity Policy: Our Cybersecurity Policy is designed to mitigate the impact of harmful disclosure, data corruption, or service interruptions on the organization's business, services, and information assets. It provides guidelines and procedures for safeguarding digital assets and data against cyber threats, ensuring data confidentiality, integrity, and availability while addressing security risks. This policy applies to all personnel with access to Retriever's internal systems or customer data.

Business Continuity and Disaster Recovery: We have implemented a suite of measures and procedures to guarantee the continuity of our most critical business functions in the face of unforeseen disruptions, thus maintaining essential operations and minimizing downtime.

Third-party (Sub-processor) Oversight: Retriever applies a structured, risk-based due diligence framework to select and oversee sub-processors, combining due diligence, contractual safeguards, and ongoing monitoring. Before engagement, we conduct due diligence assessments covering relevant security, data protection, and compliance aspects, including access controls, encryption, system architecture, certifications, and data retention and deletion practices. Relevant documentation, such as policies, certifications, and audit reports, is obtained and retained as part

of our compliance records. Retriever ensures that all sub-processors are bound by contractual obligations that provide an equivalent level of data protection and security, including appropriate rights of audit and inspection. Ongoing oversight is maintained through updates of relevant documentation and continuous risk-based monitoring. Where justified, including in cases of suspected non-compliance or elevated risk, Retriever reserves the right to conduct further assessments, including inspections or requests for additional evidence.

Personnel Security: Retriever implements personnel security measures to ensure that employees authorized to process personal data are reliable and act in accordance with applicable confidentiality and data protection requirements. Retriever performs an individual, risk-based assessment for each position. As part of the onboarding process, Retriever conducts reference checks and verifies relevant professional and educational qualifications. Where warranted by the nature of the role or where concerns arise, additional screening measures may be applied, including background checks where appropriate and permitted under applicable law. Access to personal data is granted on a least-privilege basis and is subject to confidentiality obligations. Access rights are assigned based on job responsibilities and are subject to approval and periodic review. These measures form part of Retriever's overall organizational security framework and support the protection of personal data in accordance with applicable data protection legislation.

Employee Training: Mandatory company-wide GDPR training is organized to emphasize the secure handling of customer personal data.