WHITEPAPER

ideals.

Customer due diligence checklist

The purpose and importance of a customer due diligence checklist

Businesses conduct customer due diligence (CDD) to verify client identities, assess risks, and monitor transactions to prevent money laundering and terrorist financing. In today's corporate setting, a systematic, well-documented CDD process is a legal requirement, not just a best practice.

Failures to conduct CDD thoroughly lead to severe multimillion-dollar fines from regulators such as the U.S. Financial Crimes Enforcement Network (FinCEN), loss of operating licenses, and lasting reputational damage. That's why following a strict CDD framework is crucial for good standing and regulatory compliance.

This whitepaper provides a framework for building a compliant customer due diligence checklist aligned with the FinCEN, the Financial Action Task Force (FATF), the EU's 6th Anti-Money Laundering Directive (AMLD6), and global Know Your Customer (KYC) standards. It includes adaptable templates, risk-based customization strategies, and technology solutions to mitigate exposure to illicit activities.

Disclaimer:

This material is for informational purposes only and does not constitute legal advice. Regulations vary by jurisdiction and industry. Consult qualified compliance professionals for specific guidance.

ideals.

Chapter 1

Why customer due diligence is a necessity

WHY CUSTOMER DUE DILIGENCE IS A NECESSITY

Mounting regulatory pressure

Regulatory bodies worldwide, led by the FATF, impose stringent requirements on customer due diligence. These are enacted through national legislation such as the EU AMLD and the USA PATRIOT Act.

Core obligations mandate a risk-based approach (RBA), requiring firms to identify customers and beneficial owners, understand business relationships, conduct ongoing monitoring, and perform enhanced scrutiny for higher-risk clients.

Disclaimer:

The AMLD6 is currently in force, but the EU has adopted a new AML Regulation (Regulation (EU) 2024/1624), which will become applicable across Member States starting July 2027. Organizations operating in the EU should begin aligning with this upcoming regulatory framework.

WHY CUSTOMER DUE DILIGENCE IS A NECESSITY

Expanding the scope of compliance

Financial services remain a central sector for CDD, encompassing banks, payment processors, money transmitters, insurers, and asset managers. However, anti-money laundering (AML) and counter-terrorist financing (CTF) obligations now extend decisively to designated non-financial businesses & professions (DNFBPs).

AML & CTF obligations for DNFBPs include:

- Law firms handling client transactions
- Accountants managing asset transfers
- Real estate agents facilitating property purchases
- Trust/company service providers
- Dealers in high-value goods (e.g. art, jewelry) transacting above €10,000

Virtual asset service providers (VASPs), including cryptocurrency exchanges and custodial wallet providers, also face intensified scrutiny. For example, FATF requires identity verification of VASPs to counter blockchain anonymity.

This expanding scope demonstrates a shift in the regulatory paradigm. Regulatory expectations now depend on activity risks, not just institutional labels. Therefore, any business that handles client funds or facilitates transactions (e.g. luxury car dealers and auction houses) may be subject to AML/CTF obligations under national laws.

ideals.

WHY CUSTOMER DUE DILIGENCE IS A NECESSITY

The core problem: Inconsistent execution

Lack of procedural standardization is one of the most common deficiencies flagged by AML regulators. This often leads to inconsistent application of procedures, critical oversights, poor documentation, and significant regulatory vulnerability.

Manual, ad-hoc processes are inefficient and prone to error, creating gaps exploitable by bad actors and increasing the likelihood of regulatory censure. Given the circumstances, a well-structured checklist is an indispensable tool for ensuring consistent, thorough, and defensible due diligence.

> Assessments conducted so far revealed that while technical compliance with the standard has improved, effective implementation of the AML/CFT framework continues to be challenging.

Source: International Monetary Fund (IMF)

Chapter 2

Core elements of a customer due diligence checklist

A comprehensive checklist systematically guides professionals through the following core due diligence items:

- **Customer identification and verification (IDV).** Verify the customer's legal identity using reliable, independent source documents (e.g. government-issued ID, passport, company registration documents).
- **Ultimate beneficial ownership screening (UBO Checks).** Identify the natural persons who ultimately own or control the customer (typically owning 25% or more shares/voting rights or exercising control through other means).
- **Risk profiling and risk-based approach (RBA).** Assess the inherent risk level associated with the customer, considering factors like their geographic location, business activities, transaction patterns, product/service complexity, and delivery channels.
- **Sanctions and politically exposed person (PEP) screening.** Screen the customer, their beneficial owners, and key controllers against relevant domestic and international sanctions lists, watchlists, and databases to identify PEPs and sanctioned entities and individuals. Matches against PEP and sanction lists require enhanced due diligence.
- **Adverse media checks.** Conduct checks for negative news or information from credible sources indicating potential involvement in financial crime, corruption, terrorism, or other illicit activities that pose a reputational or financial risk.
- **Ongoing monitoring requirements.** Establish procedures for regularly reviewing risk profiles and transactional behavior of customers to detect suspicious activity and ensure information remains current and accurate.
- **Recordkeeping obligations.** Maintain complete, accurate, and readily retrievable records of all CDD information collected, verification steps taken, risk assessments, and supporting documentation for the legally mandated retention period (typically five years after the relationship ends).

Chapter 3

Customer due diligence checklist template

The adaptable framework provides specific tasks under each core component, guiding professionals through the essential customer verification steps.

Core component	Purpose	Information and verification requirements	Notes
Customer identification & verification (IDV)	Confirm legal identity	**Individuals:** ☐ Full legal name + aliases ☐ Verified residential address ☐ Date/place of birth ☐ Government ID number ☐ Valid ID copy and authenticity verification **Entities:** ☐ Registered/trading names ☐ Legal/operational addresses ☐ Registration number ☐ Incorporation certificate ☐ Constitutional documents ☐ Entity status verification	Basic documentation suffices for low-risk clients. High-risk clients require biometric verification and source-of-funds checks.
Ultimate beneficial ownership (UBO)	Identify ultimate controllers	☐ ≥25% owners + control persons ☐ Ownership structure diagram ☐ UBO IDs + addresses ☐ UBO ID copies ☐ UBO identity verification ☐ Ownership change monitoring	Complex ownership structures may require deeper analysis, such as multi-source verifications and document forensics.

ideals.

Core component	Purpose	Information and verification requirements	Notes
Risk profiling (RBA)	Determine risk-appropriate measures	☐ Business purpose ☐ Risk-rated geographic locations ☐ Risk-rated industry sector ☐ Product/channel risk analysis ☐ Expected transaction patterns ☐ Screening results ☐ Documented risk rating + rationale	Enhanced due diligence is mandatory for high-risk cases, such as FATF-blacklisted countries, including Iran, North Korea, and Myanmar.
Sanctions and PEP screening	Detect prohibited connections	☐ Sanctions list matches ☐ PEP database matches ☐ Watchlist screenings ☐ Fuzzy matching evidence ☐ Match resolution documentation ☐ Screening audit trail	PEP matches always trigger enhanced due diligence.
Adverse media checks	Uncover reputational risks	☐ Credible negative reports (crime/corruption) ☐ Multi-source search methodology ☐ Jurisdiction coverage ☐ Severity assessment ☐ Search audit trail	Automated tools can be used for low-risk clients. Conduct manual multi-source investigations for high-risk profiles.

Core component	Purpose	Information and verification requirements	Notes
Ongoing monitoring	Maintain updated profiles and detect anomalies	☐ CDD review schedules ☐ Re-screening cycles ☐ Transaction monitoring reports ☐ Risk rating updates ☐ Change logs (ownership/activities) ☐ Event-triggered reviews	High-risk customers require continuous monitoring triggered by threshold events.
Recordkeeping	Demonstrate compliance	☐ Source documentation storage ☐ Verification evidence ☐ Risk assessment archives ☐ Monitoring logs ☐ Decision rationales ☐ Retrievable and complete records ☐ Retention period compliance	Maintain a minimum 5-year retention in audit-ready formats using secure digital repositories, such as virtual data rooms (VDRs).

ideals.

CUSTOMER DUE DILIGENCE CHECKLIST TEMPLATE

Customization recommendations

High-risk customers

High-risk customers need enhanced due diligence (EDD), including the following:

- Deeper source of funds/wealth verification
- More frequent and intensive ongoing monitoring
- Senior management approval for establishing/continuing the relationship
- Potentially lower UBO threshold (e.g. 10%)
- More rigorous adverse media checks

Jurisdiction/Industry specifics

Always consult local regulations. Specific requirements vary (e.g. exact UBO thresholds, precise recordkeeping duration, specific sectors needing licensing checks). For example:

- Cryptocurrency businesses (VASPs) have specific requirements for transaction counterparty information under FATF Recommendation 16, known as the “Travel Rule”.
- Real estate may involve specific title checks or agent verifications.
- Legal/accounting professions typically have specific ethical and regulatory obligations regarding client funds.

Chapter 4

Best practices and technologies for effective CDD

Implementing CDD efficiently and defensibly requires adopting strategic practices and leveraging modern technology. Here are the key best practices and enabling technologies:

BEST PRACTICES AND TECHNOLOGIES FOR EFFECTIVE CDD

Best practices examples

Automating identity verification and document capture

Modern platforms utilize optical character recognition (OCR) to extract data from passports, driver's licenses, and utility bills. This technology enables cross-referencing information against global databases. It reduces onboarding friction, minimizes human error in data entry, and provides a clear, timestamped audit trail of the verification process, essential for both low-risk volume onboarding and high-risk scenarios requiring enhanced scrutiny.

Utilizing centralized platforms for checklist management

Fragmented CDD processes across spreadsheets, emails, and shared drives create significant operational and compliance risks. Centralized compliance platforms, such as virtual data rooms, provide a single, secure environment to manage the entire CDD lifecycle.

These systems allow CDD professionals to enforce standardized checklists, automate task assignments and reminders based on risk ratings and timelines, and maintain version control for procedures. Virtual data rooms ensure that all supporting documentation and verification evidence are stored logically and securely in one place, accessible for audits or reviews.

Integrating third-party screening tools

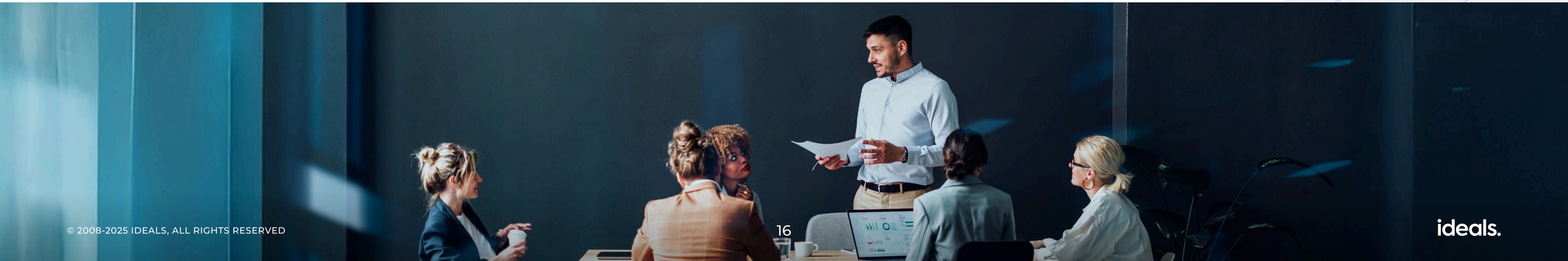
Effective sanctions, PEP, and adverse media screening demand access to vast, constantly updated datasets. Integrating specialized third-party screening providers (such as Dow & Jones Risk & Compliance Watchlist) via APIs directly into the CDD workflow is crucial. This enables real-time or batch screening against comprehensive global watchlists and reliable media sources directly during onboarding and ongoing monitoring.

Ensuring auditability and traceability

Every action within the CDD process, from document collection and verification to risk rating assignment, screening results, and ongoing monitoring alerts, must be meticulously logged. Best-in-class VDR systems provide immutable, timestamped audit trails showing who did what, when, and why. This includes maintaining full version histories of customer profiles and checklists, ensuring any decision or override is justified and documented within the system itself, ready for regulatory examination.

Training staff and aligning with internal compliance programs

Training must be practical, explaining the “why” behind tasks and how to escalate issues. The CDD process must be fully integrated into the organization’s broader AML/CFT compliance program, with clear reporting lines to the compliance officer, defined roles and responsibilities, and regular internal quality assurance reviews to ensure consistent application and identify areas for improvement.



ideals.

Chapter 5

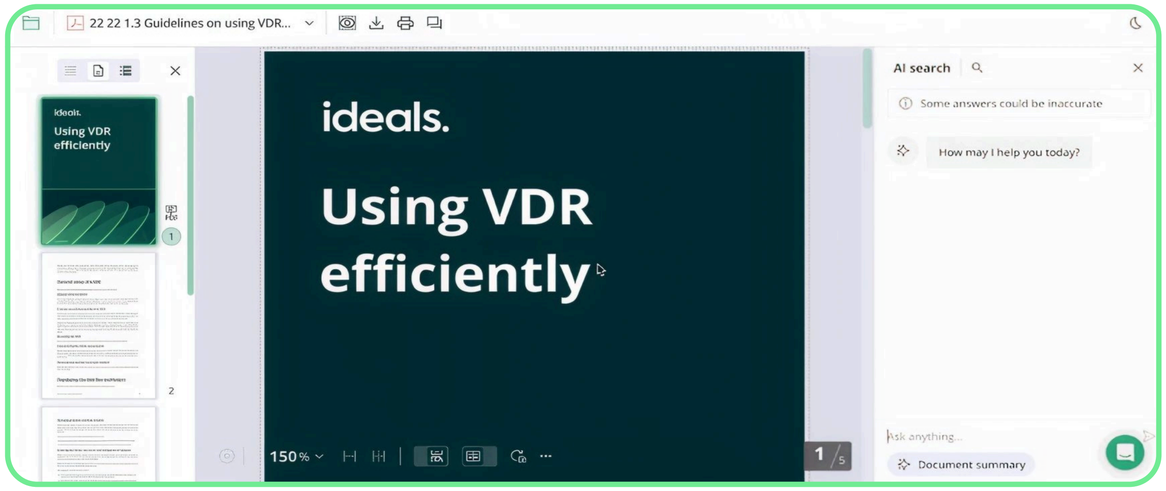
How Ideals VDR enhances customer due diligence

Ideals Virtual Data Room provides a secure, centralized platform for managing sensitive CDD documentation, transforming complex verification processes into auditable workflows.
As a purpose-built repository for confidential information exchange, Ideals ensures the integrity, traceability, and security essential for regulatory compliance.

HOW IDEALS VDR ENHANCES CUSTOMER DUE DILIGENCE

Secure document collection

Ideals' granular permission system enables risk-based access control for CDD documentation.



Ideals VDR AI search accelerates document reviews.

Key features:

- Tiered access controls with eight permission levels
- Dynamic watermarking and screen-capture protection for ID documents
- Excel-specific security toggles to hide formulas during audits
- AI-powered OCR for instant data extraction from global IDs and passports
- Automatic index numbering for seamless document referencing
- Real-time document translation across 100+ languages
- Semantic search to uncover hidden connections in CDD information
- Q&A module with query automation and question approval workflows

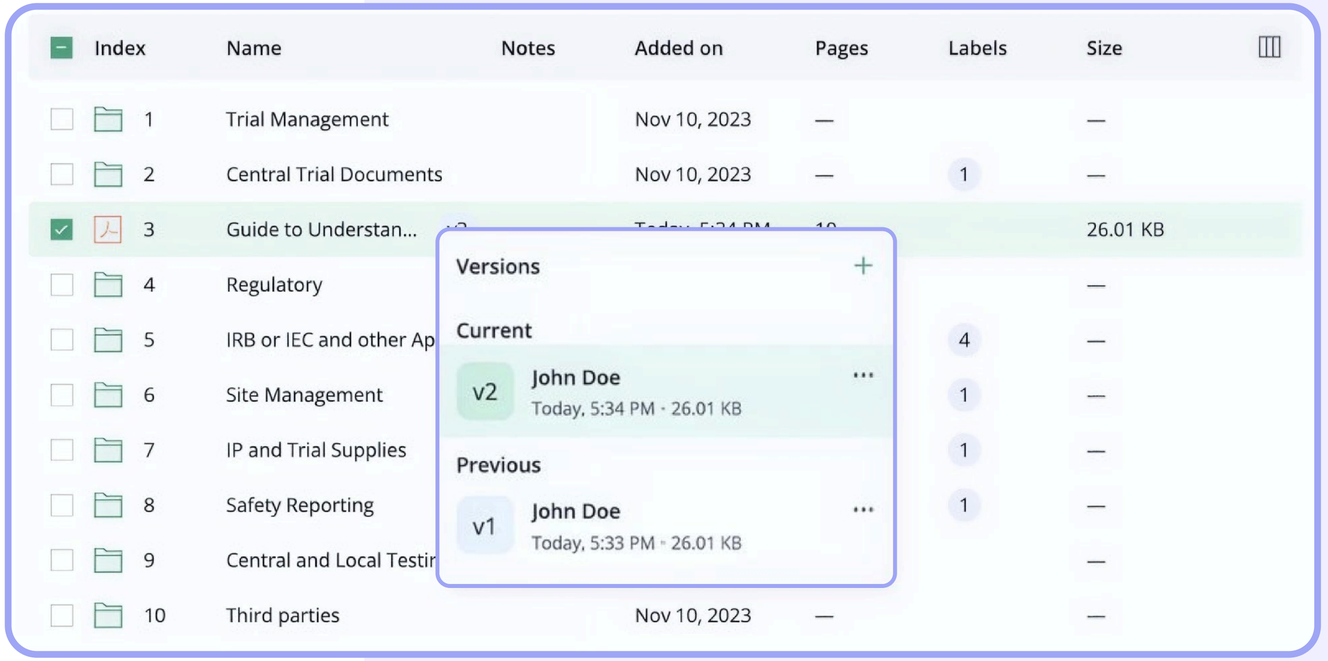
ideals.

HOW IDEALS VDR ENHANCES CUSTOMER DUE DILIGENCE

Precise version control

Maintain an immutable audit trail of document evolution with automated versioning:

- Auto-archiving of all historical versions without storage penalties
- One-click restoration of previous risk assessments
- Comprehensive change tracking with user/time stamps



Ideals' version log preserves a tamper-proof history of all document updates, complete with timestamps, authorship, and instant rollback options.

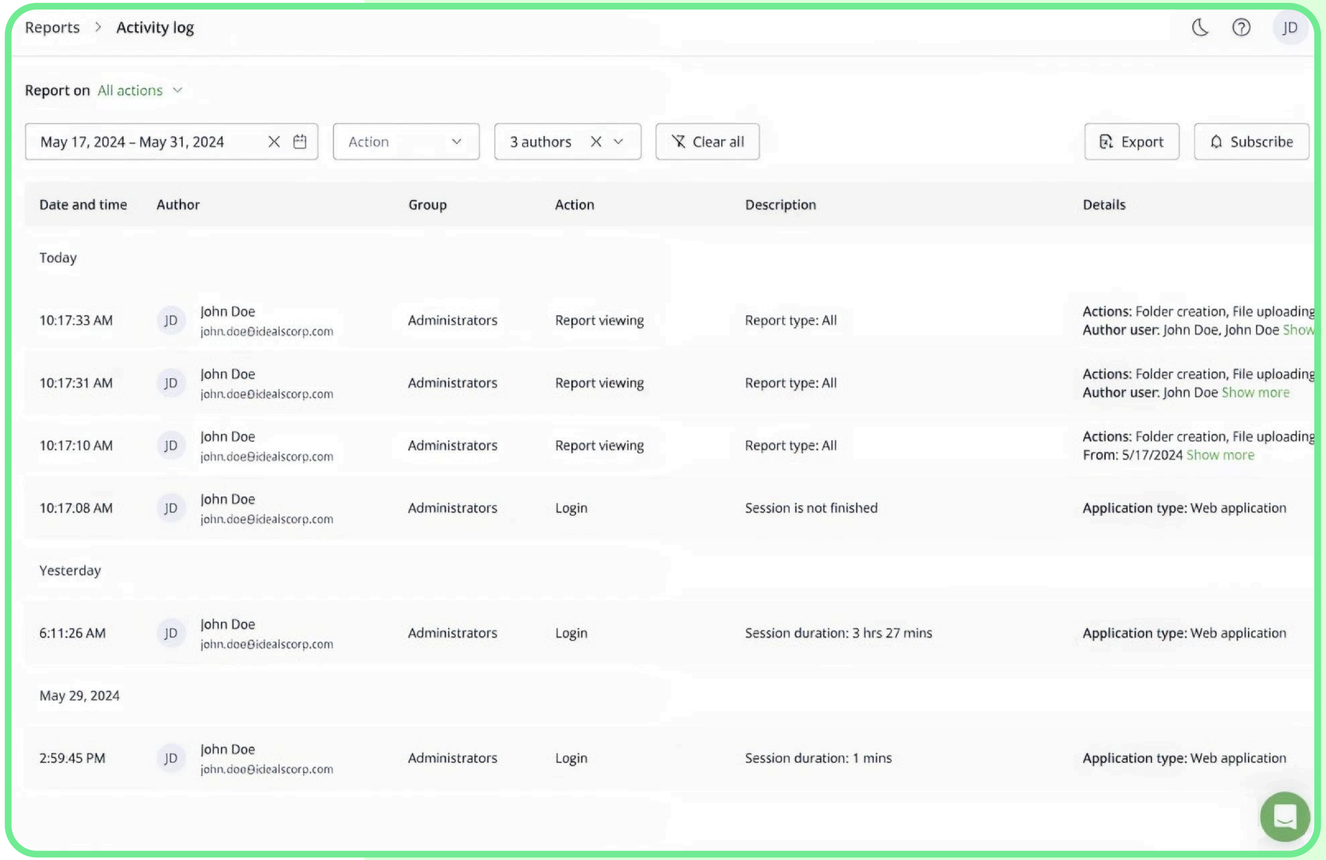
ideals.

HOW IDEALS VDR ENHANCES CUSTOMER DUE DILIGENCE

Detailed activity logging

Ideals generates precise audit trails, allowing users to demonstrate a compliant CDD process:

- Granular tracking of 39+ actions, including document navigation paths
- Customizable reports filtered by project, user role, action type, and date
- Encrypted USB archives with PIN authentication



Ideals activity log demonstrates compliance with key CDD and AML regulatory requirements.

ideals.

HOW IDEALS VDR ENHANCES CUSTOMER DUE DILIGENCE

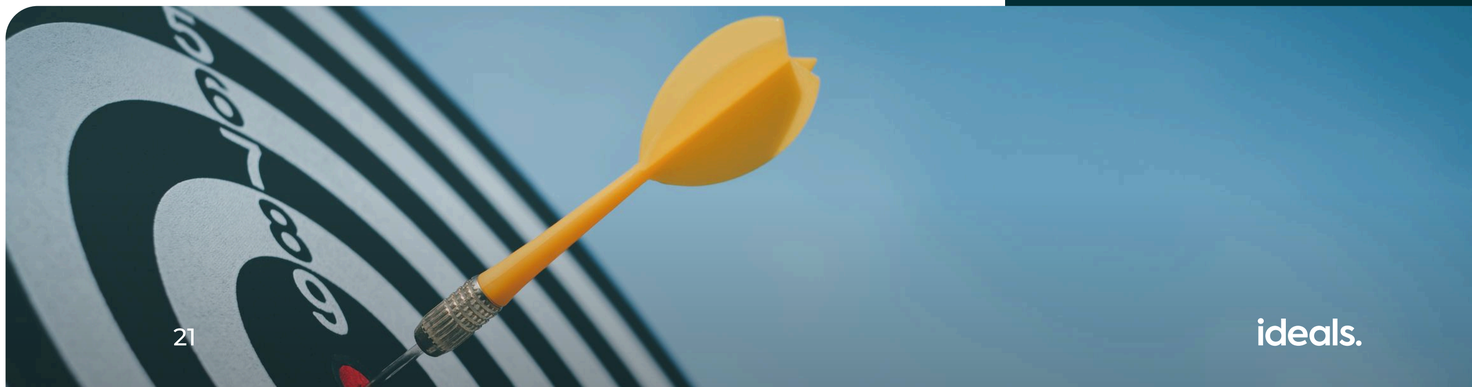
Case study: How Sagitta SGR streamlined due diligence with Ideals VDR

Sagitta SGR, a Milan-based asset manager specializing in illiquid and alternative investments, needed a robust solution to manage the increasing volume and sensitivity of client information involved in due diligence, underwriting, and investor relations. With multiple funds across real estate, renewable energy, and private debt, Sagitta sought a secure, auditable platform to handle confidential documentation and maintain regulatory standards.

Ideals Virtual Data Room met these demands with precision. The platform offered customizable landing pages and the ability to create separate, personalized environments for each client, ensuring clarity and confidentiality throughout the due diligence process. With multiple data rooms, user-friendly permission settings, and automatic document indexing, Sagitta gained complete control over how sensitive files were shared and accessed.

Granular access permissions, version control, and encryption features safeguarded critical due diligence files while supporting internal workflows and investor communications. Ideals enabled Sagitta to scale its operations without compromising due diligence scrutiny or data privacy.

As their investment analyst Luigi Lovisetto noted, “It’s the perfect way to securely show the same file to each party that needs to access it.”



ideals.

Want to manage customer due diligence as securely and efficiently as Sagitta?

Explore our data room plans and start your free trial — complete with onboarding and a dedicated success manager.

Trusted by 2M+ leading professionals globally

Deloitte. EY KPMG citi BDO accenture

ideals.

idealsvdr.com