



beta systems



Garancy®

Garancy Data Access Governance

Secure Access to Unstructured Data – Transparent, Compliant, and Efficient

The volume of unstructured data – such as documents, spreadsheets, presentations, and emails – continues to grow rapidly. With it, the **complexity of file systems and access structures** increases. Accumulated authorizations, shared accounts, and outdated access rights assigned to former employees pose serious security risks.

To ensure long-term information security, companies need complete transparency and should know: Who has access to what data? Who controls that access? And where do structural weaknesses put sensitive information at risk?

With the Garancy Data Access Governance module, you **shift the responsibility for managing sensitive data directly to the business units** – where the knowledge of content, context, and access requirements actually resides.

How Secure Is Your Access Control?

To proactively identify risks and potential compliance violations in your data access processes, your organization should be asking:

- Who assigns access rights to your unstructured, sensitive data?
- Do you know who is ultimately responsible for that data?
- Do your Access Management processes meet internal policies and all relevant external compliance standards?

Empower Business Owners to Manage Access Independently

Garancy Data Access Governance provides the foundation for controlled, compliant self-service Access Management within business departments.

- Data owners define who can access which data, when, how and for what purpose – no deep technical expertise or IT involvement required.
- The solution supports granular access rights management below the Active Directory group level, down to the folder and file level – on file servers, in Microsoft SharePoint or other document management systems.
- Integrated approval workflows and self-service functions seamlessly involve responsible stakeholders in the access request and review process, ensuring transparency, auditability and full traceability.

Using a proven methodology, an initial authorizations audit can be conducted. This forms the basis for an automated consolidation of your file system structures with a focus on access control.

Seamless Integration with the Garancy Suite

The Data Access Governance module integrates seamlessly with the Garancy Suite – from light-weight connectivity to full integration. All relevant information is made available to the centralized IAM system.

- Data owners manage access rights independently through an intuitive interface and retain full control over their information.
- Administrators, operators and end users work in their familiar environments – there's no need to learn a new system. The solution blends smoothly into existing workflows and infrastructures.
- By integrating into existing self-service portals and reporting tools, you establish a centralized, efficient Single Point of Administration that combines transparency with ease of use.

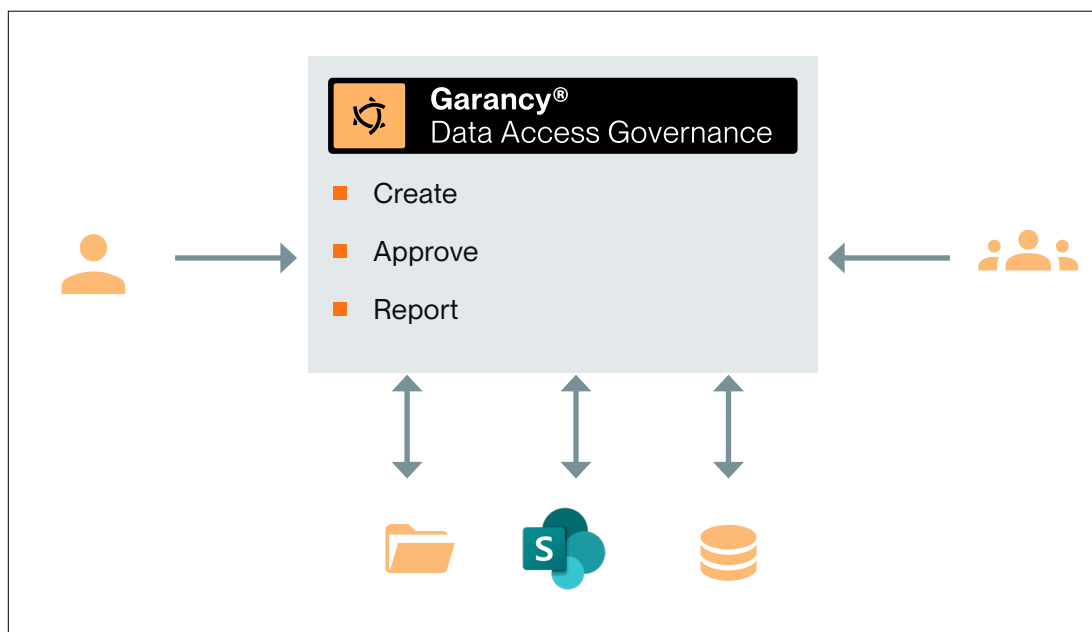


Figure 1 – Centralized Access Management with Garancy Data Access Governance

Three-Phase Model

1. Authorizations Audit – Analysis and Reporting

- Analysis of Access Rights: Automated identification and evaluation of access rights to unstructured data, including detailed reports answering key questions, such as “Who has access to what and who assigned which rights?”
- Security Assessment: Prioritization of identified risks based on defined KPIs
- Results and Recommendations: Evaluation of remediation efforts and concrete guidance to minimize risk

2. Clean-Up – Consolidation and Migration

- Software-supported restructuring of existing file and authorization structures
- Seamless migration of data and access rights without disrupting ongoing business operations

3. Data Access Governance – Control and Oversight of Access Rights

- Sustainable, secure management of access rights in environments with unstructured data
- Business units take control, managing permissions without direct IT involvement
- Prevention of uncontrolled access through business-oriented approval workflows, covering everything from initial requests to periodic recertifications and deprovisioning
- Built-in compliance checks ensure adherence to internal policies and regulatory requirements for critical data access, e.g. SOX, BDSG, MaRisk, GoBD and KonTraG
- Real-time comparison of access rights (target vs. actual) instantly highlight critical deviations and security gaps

Ready to Take the Next Step?



Contact us to learn more about our IAM solution – we look forward to hearing from you.

Email us at info-iam@betasystems.com or give us a call at **+49 (0) 30 726 118-0**.

www.betasystems.com/products/garancy