Secure file sharing

Supporting NIS2 compliance with Databeamer

Whitepaper - July 2025

Data Beamer

Summary

The NIS2 Directive (EU) 2022/2555 introduces stronger cybersecurity requirements for essential and important entities across the EU. As digital threats grow in complexity and impact, organizations must implement robust measures to protect their network and information systems, including secure communications with third parties.

NIS2 Key obligations

NIS2 applies to a wide range of sectors and imposes obligations such as:

- Risk management and security policies
- Secure data and system operations
- Incident detection and reporting (within 24 hours)
- Supply chain cybersecurity
- Business continuity and recovery planning
- Governance and accountability for senior management
- Use of encryption and MFA

Databeamer provides a secure, encrypted file transfer platform that helps organizations meet NIS2 compliance obligations. This whitepaper outlines how our platform contributes to the core requirements of the directive, particularly in the areas of secure data transfer, incident traceability, governance, and supply chain risk mitigation.

The following overview shows a summary of how Databeamer's capabilities help you to meet NIS2 requirements in relation to file transfer functionality.

NIS2 Requirement	Databeamer Capability
Ensure confidentiality and integrity of data in transit	End-to-end encryption
Incident response & audit logging	Real-time logging, SIEM integration
Access control & governance	RBAC, policy engine
Business continuity	High availability, DR, backups
Supply chain security	Integrity checks
Secure software development lifecycle (SSDLC)	Secure coding, vulnerability scans

Table of contents

1. Introduction - understanding NIS2

The growing complexity and interdependence of digital systems have made cybersecurity a critical concern across industries. In response, the European Union introduced the NIS2 Directive (EU) 2022/2555 (short: NIS2), an updated framework aimed at strengthening cybersecurity across essential and important entities. NIS2 mandates a higher level of risk management, incident reporting, and supply chain security, placing a renewed emphasis on visibility, control, and responsiveness in handling digital infrastructure.

A key but often overlooked area affected by NIS2 is file sharing. The exchange of files—internally or with external partners—remains a fundamental part of business operations. Yet, without the right safeguards, it also represents a significant vector for data breaches, ransomware, and compliance violations. NIS2 explicitly requires organizations to protect data flows, ensure access control, and monitor for unauthorized activity across all digital communication channels—including file transfers.

Databeamer is built with these evolving requirements in mind. It provides a secure and auditable platform for file sharing, enabling organizations to maintain full control over how, when, and with whom (sensitive) files are exchanged. Features such as encryption, access management, and activity logging support the traceability and risk mitigation measures mandated by NIS2. With Databeamer, file sharing becomes a secure, compliant, and transparent part of your broader IT ecosystem.

2. Challenging secure collaborative file sharing

In the digital era, organizations increasingly rely on collaborative tools and platforms to share sensitive files and data across internal teams, partners, and third-party vendors. While this connectivity accelerates productivity and decision-making, it introduces significant cybersecurity and compliance challenges. Under frameworks such as the NIS2 Directive, the protection of shared digital assets is no longer optional—it is a regulatory imperative.

The Complexity of Collaboration

Modern collaboration is not confined to internal networks. Files are shared across borders, devices, and ecosystems—via email, cloud drives, messaging apps, and third-party portals. These interactions frequently involve external suppliers and partners, remote and hybrid workforces or cloud-based applications. Each touchpoint increases the attack surface and poses risks such as data leakage, unauthorized access, and loss of data integrity.

Secure file sharing is vulnerable to a wide range of threats, like unauthorized access, insider threats or intercepted files because of unencrypted file transfers. Also collaborating with third party professionals or clients can attribute to extra risks as they may have weak cybersecurity postures themselves.

The NIS2 Directive emphasizes the need to address such vulnerabilities, especially as collaboration increasingly spans organizational and national boundaries.

Fragmented tools and lack of control

Many organizations rely on a patchwork of file-sharing solutions—some officially approved, others adopted informally—without consistent policies or centralized oversight. This fragmented approach often results in inconsistent encryption standards, limited or nonexistent auditing capabilities, and a lack of traceability in file activity. Once files are shared externally, organizations may have no effective way to revoke access. Furthermore, these disparate tools frequently fail to align with internal governance structures and regulatory requirements. As a result, such fragmentation significantly weakens risk management efforts, which are a core obligation under the NIS2 Directive.

Compliance pressure and governance gaps

The NIS2 Directive requires organizations to demonstrate that robust and secure information-sharing processes are in place. This includes implementing clearly defined access control policies, maintaining detailed audit trails, and ensuring that encryption is applied both during transmission and while data is at rest. Secure authentication mechanisms must be used to protect systems and data, and clear accountability must be established at the senior management level. Failure to implement and maintain these safeguards across collaborative environments can expose organizations to regulatory scrutiny, damage their reputation, and result in significant financial penalties.

Don’t forget the human factor

Even the most secure systems can be compromised by human error. Users often bypass official channels for convenience—using personal email, unsecured file-sharing services, or outdated methods—unknowingly exposing the organization to risk. Security awareness and user-centric design of secure collaboration tools are therefore essential.

3. Meet Databeamer

Databeamer is a secure file sharing platform designed to empower organizations in managing and governing all of their sensitive and large-scale file transfers. Whether collaborating with internal teams or external partners, Databeamer enables secure, controlled, and seamless file exchanges—without compromising usability or compliance.

At its core, Databeamer addresses one of the most critical aspects of digital infrastructure under the NIS2 Directive: the secure and transparent movement of data. File transfers are often a weak link in cybersecurity frameworks—vulnerable to breaches, unauthorized access, and regulatory violations. Databeamer closes that gap by offering a platform where every file exchange is encrypted, policy-controlled, and fully auditable.

Sovereign cloud

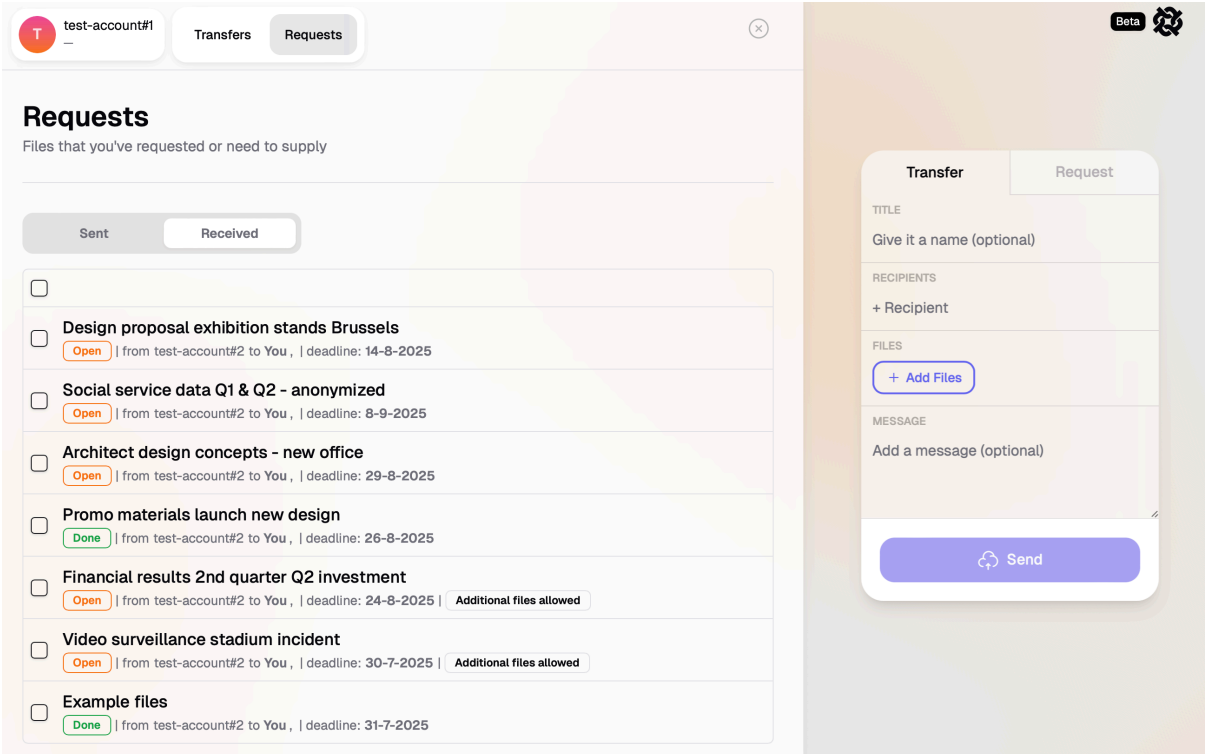
Databeamer is hosted entirely on European sovereign cloud infrastructure, with no reliance on U.S.-based providers, eliminating exposure to the U.S. CLOUD Act. This ensures organizations retain full control over their data and stay compliant with EU data sovereignty principles—an increasingly important requirement under both NIS2 and GDPR.

Security and privacy are built into every layer of the platform. Organizations can enforce granular policies, monitor all file activity, and maintain a clear audit trail, providing the transparency and accountability required by NIS2. Whether you're handling personal data, financial records, or confidential business information, Databeamer ensures that every transfer aligns with the highest standards of data protection, risk management, and incident preparedness.

Key features

Databeamer supports various features to enable safe and easy file transfers and meet compliancy demands. These features include:

- End-to-end encryption (in transit and at rest)
- Direct and scheduled data requests
- Workspace collaboration
- Agent workflows
- Client-side validation and anonymization
- Audit logging and traceability
- Policy-based acces controls and expiration rules
- Integration with identity providers (LDAP, SSO)
- Virus-scanning before transfer
- White-labelling personalization



Databeamers clean and user-friendly lay-out (depicting received data-requests)

Architecture & encryption technology

Databeamer is built on a modern, security-first architecture designed to meet the highest standards of data protection, scalability, and performance. Developed in Rust, a systems programming language known for its safety, speed, and memory efficiency, Databeamer delivers a highly reliable backend that is both resilient and secure by design.

At the heart of Databeamer's platform lies its robust end-to-end encryption model, engineered to protect sensitive files from the moment they are uploaded until they are accessed by the intended recipient. This encryption framework goes far beyond conventional TLS-based approaches, implementing AEAD streaming encryption that allows for secure handling of files of virtually any size—even streaming transfers of infinite length.

Key features of Databeamer's encryption architecture include:

- ChaCha20-Poly1305: A modern, high-performance cipher known for both security and speed
- HKDF-SHA256: A secure key derivation mechanism ensuring strong, consistent key management
- Multiple recipient support: Encrypted files can be securely shared with multiple authorized users without redundancy or re-encryption
- Streaming cipher: Designed to handle very large or continuous file streams securely and efficiently
- Private key handling: Leveraging Pedersen and Feldman commitment schemes, Databeamer ensures that private decryption keys are never accessible—even to us as the platform provider

For added security and resilience, users can recover access via a secure mnemonic phrase, eliminating the need to rely on centralized key storage or external key management systems. This architecture aligns directly with NIS2 principles of data confidentiality, integrity, and availability, while also supporting advanced governance and traceability.

This cryptographic design, combined with Rust's memory-safe development environment and Databeamer's scalable infrastructure, provides a strong technical foundation for secure file sharing in environments that demand both performance and strict compliance.

4. Example use cases

Case: **Strengthening Data Governance in Local Government**
Industry: Public Local Administration
Use Case: Interdepartmental and Interagency File Sharing

Local governments are responsible for managing and exchanging a wide variety of sensitive information—ranging from citizen records and social services documentation to infrastructure plans, procurement files, and legal contracts. These files are often shared between municipal departments, external consultants, national agencies, or EU regulatory bodies. Ensuring that these exchanges happen securely, traceably, and in full compliance with evolving regulations is a growing challenge—particularly under the scope of the NIS2 Directive.

A mid-sized Dutch municipality faced exactly this challenge. Their IT department was tasked with improving digital resilience and compliance posture following a cybersecurity audit. One critical gap identified was the lack of a secure and standardized method for exchanging sensitive personal data—especially large files—with external social services companies. The shared data was needed to check on citizens overlap and also anonymously used for accountability reporting.

By implementing Databeamer, the administration gains a centralized, secure platform for those specific file transfers. Employees can easily share encrypted files with the stakeholders within specific workpaces. The municipality acts as the central party with project responsibility and has full control over access rights, expiration dates, and download limits. Crucially, all file activities are automatically logged, enabling detailed audit trails to support internal oversight and NIS2 compliance reporting.

In addition to simplifying workflows, Databeamer helped the local government meet key NIS2 obligations and simultanously modernized its information governance and positioned itself as a digitally resilient organization ready to meet the demands of current and future EU cybersecurity directives.

Case: **Securing Operational Data Sharing in Public Transport**
Industry: Logistics – Public Transport
Use Case: Secure Exchange of Operational and Incident Data

Public transport operators manage a vast flow of information every day—ranging from real-time service reports and maintenance logs to surveillance footage, incident reports, and sensitive personnel records. This data is often shared with subcontractors, municipal authorities, law enforcement, and external maintenance providers. In this context, ensuring the confidentiality, integrity, and availability of shared data is not just good practice—it's a regulatory requirement under NIS2.

A local public transport authority faced challenges in securely exchanging large files, such as video recordings from onboard surveillance systems or diagnostic logs from connected vehicles. Previous methods—including physical media, unsecured cloud platforms, and inconsistent email practices—exposed the organization to unacceptable cybersecurity and compliance risks.

By adopting Databeamer, the transport authority is able to securely transmit and receive sensitive operational files while maintaining full control and traceability.

Accident reports and video evidence can now be securely shared with police and legal teams, with access restrictions and download tracking in place to ensure proper handling. Maintenance contractors receive encrypted diagnostic logs and are able to upload return documentation through the same secure channel—without being granted unnecessary access to internal systems. Additionally, incident investigations are significantly accelerated by enabling field agents and security staff to upload files directly via one-click links, minimizing delays and reducing the risks associated with manual file handling.

Databeamer's streaming encryption and multi-recipient capabilities ensure even the largest data files, such as high-definition video or telemetry logs, can be transmitted securely, quickly, and in compliance with NIS2's requirements for data protection, incident documentation, and third-party risk management.

5. Databeamer’s role in supporting compliance

Databeamer is designed with NIS2, cybersecurity and GDPR requirements in mind, providing the tools and infrastructure needed to meet modern security and transparency standards. This chapter outlines how Databeamer helps organizations fulfill key NIS2 compliance obligations while maintaining operational efficiency.

A. Encrypted data transfers

Requirement:
Ensure confidentiality and integrity of data in transit.

Our Contribution:
End-to-end encryption using AEAD streaming encryption ensures that sensitive data exchanged between organizations remains protected from interception or tampering.

B. Governance and Access Controls

Requirement:
Implement access control policies and enforce least privilege.

Our Contribution:

- Role-based access control (RBAC)
- Granular permissions
- Policy enforcement engines
- Full audit trail for every transfer and user interaction

C. Audit Logging and Incident Response

Requirement:
Maintain logs and respond to security incidents effectively.

Our Contribution:

- Timestamped, tamper-resistant logs
- Real-time alerts and monitoring
- Custom integration with SIEM platforms

D. Business Continuity & Resilience

Requirement:
Ensure service continuity during cyber incidents.

Our Contribution:

- High availability architecture
- Automated failover and backup systems
- Data replication and disaster recovery procedures

E. Supply Chain Security

Requirement:
Evaluate and mitigate risks from third-party services.

Our Contribution:
Our platform enables secure, trackable exchanges with external partners, reducing exposure to vulnerabilities introduced via third-party data transfers.

F. Secure Development Practices

Requirement:
Develop and maintain secure software.

Our Contribution:

- Secure SDLC processes
- Regular vulnerability scanning and patch management
- Pen testing and third-party code reviews

6. Partnering with Databeamer

In an era of increasing regulatory pressure and evolving cybersecurity threats, secure and compliant file sharing is no longer optional—it's essential. Whether you're operating in public safety, transportation, government, or another critical sector, the ability to protect sensitive data while enabling fast, efficient collaboration is vital to both operational success and regulatory compliance.

Databeamer provides a purpose-built platform that not only enhances your organization's security posture, but also significantly reduces risk exposure in regulated environments. By simplifying compliance documentation, supporting audit readiness, and ensuring full traceability of all file activity, Databeamer helps organizations align with frameworks like NIS2 and GDPR with confidence.

Ultimately, partnering with Databeamer means strengthening trust with customers, partners, and regulators—while gaining a secure, scalable solution for one of the most overlooked areas of digital infrastructure: file sharing.

Databeamer by Full Join

Databeamer is created and licensed by Full Join B.V. and is located in Eindhoven, The Netherlands. Full Join is a software and data development/consultancy agency. We develop applications and provide consultancy services, including advising organisations about data, privacy and development projects.

Protecting your privacy and securing your data is our top priority

Contact Us

To learn more about how Databeamer can support your organization’s NIS2 compliance, contact us at:
E: hello@fulljoin.nl
T: +31-402094163