Nextcloud

nextcloud.com

Why do governments use Nextcloud Enterprise?

Governments across Europe are increasingly moving away from foreign cloud providers due to growing concerns over digital sovereignty, regulatory compliance and control over sensitive public data. Nextcloud has become one of the most widely adopted private cloud solutions in the public sector. Governments choose Nextcloud for four key reasons:

Data sovereignty

Government digital infrastructure must remain independent of individual vendors and resilient against external influence, ensuring that sensitive public data remains under national or institutional control. As an open-source platform built around open standards, Nextcloud also reduces vendor lock-in and supports long-term interoperability.

Compliance with regulations and standards

Public institutions operate within demanding national and European regulatory frameworks. Nextcloud helps organizations implement collaboration environments that support requirements arising from the General Data Protection Regulation (GDPR/DSGVO), the German Federal Data Protection Act (BDSG), NIS2 and other applicable public-sector requirements.

Nextcloud Files has achieved the French ANSSI CSPN security certification, recognized by Germany's Federal Office for Information Security (BSI) as equivalent to its Accelerated Security Certification (BSZ). A Nextcloud deployment has also been certified according to BSI IT-Grundschutz, providing an important reference for German public authorities.

Protection of sensitive data

As digitalization increases, the challenges of privacy and security continue to grow. Governments cannot risk exposing sensitive citizens' data.

Digital transformation

Governments must modernize digital infrastructure to improve services for citizens while increasing efficiency across ministries, agencies and municipalities. Remote work needs real-time collaboration and fast but secure document exchange with other organizations.

Nextcloud Hub: A unified digital workspace



Nextcloud Hub brings all essential collaboration tools together in one platform, creating a secure and sovereign digital workspace for public sector organizations. It combines file sharing, chat messaging and videoconferencing, office collaboration, groupware, AI assistance, and workflow automation. Nextcloud Assistant enables organizations to use AI on their own terms, with options to run AI models locally so sensitive data stays within their controlled infrastructure.

Start with the tools you need and expand over time while maintaining full control over your data and infrastructure. As a fully open-source platform, Nextcloud Hub ensures transparency, flexibility, and independence from proprietary vendors.

Key capabilities include:

Collaboration

- Guest accounts for easy and secure external collaboration
- Teams and contacts – define once, reuse across the entire Hub
- Federation for secure cross-organization collaboration

Security and compliance

- Enterprise-grade security controls
- Full data sovereignty with on-premises deployment
- Extensive auditing and compliance capabilities
- Fine-grained access and sharing policies

Productivity

- Unified search across files, chats, emails, and calendars
- Integrated communication with Nextcloud Talk
- Collaborative document editing with support for Microsoft Office formats and OpenDocument Format (ODF)
- Workflow automation with Nextcloud Flow

Setup & infrastructure

- Custom branding and white label options
- Seamless integration with existing IT environments
- Accelerated Direct Access (ADA) reduces latency for large file transfers; critical for large-scale deployments

Flexible deployment options for a sovereign infrastructure

Nextcloud is designed as a private cloud solution, giving you full flexibility in how you deploy and operate your collaboration platform. This ensures that your organization always retains control over where data is stored and who manages the infrastructure. You can choose the deployment model that best fits your security, compliance, and operational requirements.

Deployment options include:

On-premises private cloud

Run Nextcloud in your own data center for maximum control and compliance.

Hosted private cloud

Deploy Nextcloud with a trusted hosting provider while retaining full control over your data and infrastructure. European and German hosting options enable public institutions to keep their data within the EU or Germany where required.

Hosted by a certified Nextcloud partner

Access Nextcloud as a fully managed service provided by certified partners. Depending on the provider, hosting is available in German or European data centers and can be tailored to public-sector requirements.

Procurement through established frameworks

Nextcloud solutions are also available through partners experienced in public-sector procurement. In Germany, for example, Nextcloud and Bechtle offer sovereign collaboration services that can be obtained by federal authorities and other public institutions through existing framework agreements.

Ecosystem, interoperability and open standards

Public administrations rarely operate in isolation. Nextcloud combines an open-source architecture with a broad ecosystem of extensions and integrations, making it easier to connect existing systems.

More than 600 apps extend the platform with functionality ranging from security features and productivity tools to infrastructure integrations. Federation enables organizations running separate Nextcloud environments to collaborate without first moving their data into one central cloud.

Nextcloud Enterprise integrates with existing enterprise infrastructure, including, but not limited to, Microsoft environments. This allows organizations to modernize their infrastructure step by step rather than replacing every existing system at once.

Open standards are equally important for long-term interoperability. Nextcloud Office supports OpenDocument Format (ODF) alongside common Microsoft Office file formats, helping public institutions keep documents accessible independently of a single proprietary office suite.



Protecting public-sector data

Nextcloud engineers every release around a security-first development process. Multiple layers of protection help public institutions control access, detect threats and protect sensitive administrative and citizen data.

Key security capabilities include:

Access control

- Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) authentication
- Two-factor authentication
- Fine-grained sharing and access policies

Threat protection

- Brute-force protection
- Remote wipe to protect data on lost or compromised devices
- Machine-learning-based suspicious login detection
- Ransomware protection and built-in security checks

Compliance and monitoring

- Extensive audit logs for monitoring and compliance
- External security reviews and penetration tests
- USD 10,000 security bug bounty program
- ANSSI CSPN security certification for Nextcloud Files
- BSI IT-Grundschutz-certified Nextcloud deployment

Nextcloud protects data both during transfer and while stored. Organizations can choose the encryption approach that matches their security model and infrastructure.

Encryption capabilities include:

- Transport Layer Security (TLS) encryption
- Server-side encryption
- Optional per-user encryption keys
- End-to-end encryption
- Enterprise-grade key management
- Protection against storage compromise or server theft

Take the next step toward digital sovereignty

Talk to our public-sector team about your infrastructure, migration or collaboration requirements.

MINISTÈRE DE L'ÉDUCATION NATIONALE
Liberté
Égalité
Fraternité

Bundesministerium
Arbeit und Wirtschaft

AMNESTY INTERNATIONAL

SH Schleswig-Holstein
Der echte Norden

Nextcloud

nextcloud.com

Get your free Sales consultation