ONLYOFFICE

# Sovereign collaborative infrastructures for government offices

Ascensio System SIA

February 2021

# Abstract

Collaborative technologies are being widely adopted in public organizations just as they are in the commercial sector. However, digital policies of such organizations rely solely on the limitations defined by public nature of organization's interests and the regulatory environment the organization operates within.

In this paper, we review the common challenges public sector faces when building an IT environment within its network to support collaborative processes and assume an effective model based on open, sovereign, and secure technologies.

# Contents

# Introduction

Most government bodies have somewhat similar operational models to common business practice, however, due to utterly different regulatory environments they face more harsh barriers to business automation and IT infrastructure building.

For this reason, the offices seek fully compliant associates that provide reliable solutions and offer sufficient options in customization, reliable assistance, and turn-key solutions. Same applies to business cloud apps for online document processing, sharing, and collaboration in particular. 2020 Digital Counties Survey by US Center for Digital Government (CDG) estimates that mid-size counties rank cloud computing as a top-10 technology priority over the next 12 to 18 months.

Despite governmental, financial, and structural differences between public organizations, some problems are commonplace in choosing the software for building the efficient collaborative environments:

- Regulations and standards for working with user data. Security of user data is a top priority for every public organization for a variety of well-known reasons, including the international and supranational requirements, protection from targeted attacks, need for establishing public trust, etc. The United States Government Accountability Office (GAO) found that 23 federal agencies lacked proper cybersecurity measures in their offices.
- Limited budgeting. In most cases the organization's IT budget creates a bottleneck in infrastructural improvements, for extending it's limit is a complex bureaucratic procedure since it may not be derived directly from the organization's income. According to Granicus's State of Digital report, 73% of government organizations lack budgeting sufficient to tackle the technology challenges.
- Purchasing process limitations. In some cases direct purchase of software is legally impossible and requires the presence of authorized subcontractors and government-certified procurement platforms.

Common procurement challenges, for example cause the US Department of Defence to have critically outdated and costly software procurement procedures according to Defence Innovation Board's Software Acquisition and Practices Study.

- Infrastructures of big scale. Scalability and clusterization of the software play key role for bigger organizations that need to provide essential tools for hundreds or thousands of users located in separate branches and departments.
- Need for interoperability with solutions in use. In most cases, addition or replacement of the software takes place within the environment where other connected services for working with the same data preexist.
- Specific functionality requirements. Besides the core offering itself, Customization opportunities of the solutions and special terms for functionality requests define the perspective for each particular contract.

In the following chapters, we will examine the principles of building a sovereign collaborative environment for a government office using open, interoperable technologies that cover the core data protection principles, and the applicability of ONLYOFFICE solutions in such an environment.

# New digital sovereignty

As cybercrimes thrive, businesses and organizations increasingly seek solutions to make their infrastructures more sovereign in terms of working with data. The role of the big cloud fades in favor of private and hybrid cloud ecosystems that give more control over the assets. This is specifically important to government offices that handle the most sensitive asset there is - personal data of citizens.

The breach of such data will lead to vast economic and, in some cases, political damage that will be hard to undo. And yet there's a chance to rethink the approach to data allocation.

First argument for reaching deeper digital sovereignty is the concern for privacy of the data stored in a public cloud environment. This data may be monitored by the provider for a variety of purposes, from gathering simple performance information to studying the usage of the service by its customers.

On the contrary, self-hosted data processing services with open code guarantee data independence, letting the full cycle remain within the organization's network. The vendor in this case doesn't act as a data controller, and only remains a producer of the system. This system can be examined end tested in the very conditions of the user environment and remains open in it's composition to the public. Data independence together with this transparency becomes the great condition for establishing public trust.

# Deficiencies of the universal approach

With agility of present-day data sharing methods come numerous related security issues that are not solved by most, if not any, of the existing solutions:

- Safe password creation requires knowledge in basic password strength standards. It also relies on manual safekeeping of these passwords.
- Insecure sharing of this data presents a direct threat to the information.
- Single-stage encryption and decryption necessarily limits the abilities such as group access and co-editing, forcing the users to restructure common workflows.
- Centralized key management schemes in storage encryption relocate the threat focus, but said model of encryption does not allow individual file protection.
- Basic training in data security is required to teach data safety principles and tools to the employees.

The encryption scheme applied in ONLYOFFICE Private Rooms provides necessary technological basis to lift these limitations:

- Document encryption model in ONLYOFFICE allows reaching level of data protection highly tolerant to known methods of encryption hacking, while offering secure and convenient key management.
- Symmetric AES-256 encryption is ultimately resistant to brute force.
- There’s little to no chance users mishandle the passwords to documents because they are generated automatically and stored in encrypted form.
- Second-layer asymmetric encryption of document passwords allows single-action safe sharing of protected documents between users because no plain text password exchange is involved.
- This model allows real-time encrypted editing and collaboration.
- True end-to-end: the encryption is carried out on user’s machine and no centralized key management is involved.
- No training is required, as the users work with protected documents in the same way.

# Value of open source

The choice of the IT policy and strategy for a government does not rely merely on functionality and cost reduction. It’s a fundamental process of establishing sustainable, efficient, and secure flow and control of information. Open-source software implemented in governmental IT infrastructures opens an alternative strategy as both its production and usage are driven by the values of transparency, good faith and in many cases personal gains of the contributing community rather than simple accumulation of corporate wealth.

The pricing of open software is to a bigger extent derived from technical support services, involvement of the production team in the customer’s case (requested modifications and other supply of intellectual assets). This does not always allow the package to be free of charge or licensed with full transfer of rights.

But as opposed to traditional proprietary software, open source production is widely motivated by self-actualization and contribution to a bigger process and results in higher commitment of the individuals involved in the development labor. Motivational model built mostly on financial incentives results in higher cost of traditional software. Besides, the vendors that seek greater acquisition tend to lock their customers in the framework by implementing exclusive proprietary data formats and mechanisms of its processing, which doesn’t add any value to the product and only helps secure the extensive contracts.

When it comes to hosting the data in the hired proprietary infrastructure, there’s no chance to prove how the data is processed hands-on, without knowledge about its back-end. Open-source solutions, on the contrary, provide the opportunity to any data user to study each and every mechanism of its processing, not just from provider’s public statements and certifications. This consequently establishes better trust in the data processors and controllers (i.e. the government organization) and the services they provide that require submission and processing of personal information.

In a nutshell, open-source software not only allows for more efficient cost reduction, but thanks to different nature of producer’s motivation and alternative view on intellectual property helps establish transparent ans sustainable IT policies, therefore positively affecting the efficiency of the government.

## Principles of data control and protection

A public organization is always subject to the regulations that govern responsibility of the organization for lawful and limited processing of personal data of the government and its citizens to carry out the procedures with the data in public interest.

Therefore, one of the fundamental elements of every digital policy is privacy and security of the information. Regulatory laws, although diverse in each particular region and industry (e.g. GDPR in Europe, HIPAA for medical organizations in the US), define principles of data safekeeping, data processor and controller accountability, and technical safeguards that maintain core data protection mechanisms in the organization.

Generally, these regulations encourage data minimalism practice, define legal mechanisms of data storage and transfer and determine the rights of data owners. In some cases, clear instructions for technical data protection policy are introduced, including but not limited to data encryption technology, access control, data transfer, storage and erasure, data audit.

# Interoperability

The market of open-source solutions is very saturated and niche-based. The trend towards clear division of labor between the projects becomes more obvious: each developer focuses on what they do best, providing solutions ready to function in harmony with each other, while users are free to build custom, modular infrastructures choosing the best fit solution for each particular task.

Ability to build modular IT for an office gives great freedom in adapting, scaling and customizing the solutions in use, and significantly cutting the costs. The key to organize a smart modular workspace is the interoperability of the software of which the system is composed with other applications in the network, its architecture, external services, etc.

Today, it is possible to build a collaborative environment of any scale using custom architecture of components to satisfy each unique demand based on what collaborative processes need amplification, what means of communication are employed in the organization, what are the types of data each group deals with, etc.

## Reduction of the employee training cost

Adoption of new technologies as everyday tools drag along vital and sometimes costly employee training process. This is why the choice of collaborative software depends partly on learning curve it involves.

The value added of every core collaborative tool, talking about commonplace ground technologies like file management and sharing, document collaboration, is the ability to not only be interoperable but also user-friendly. The new interface shall provide easy transition from the software previously used to carry out the same tasks and minimize the need for additional training and learning.

## Budgeting challenges and smarter investment in collaborative tech

With accelerating pace of digitalization, the process of purchasing the elements of IT infrastructure within given budget has its dynamics that do not always come in favor of subject organizations.

Ability to adjust the spending to the exact current or planned scale of the infrastructure depends solely on the pricing model of the software vendor. Opting for more flexible plans based on technical support level and capacity (by number of users or other units) significantly cuts the expense and helps plan future spending based on the pace of infrastructure expansion.

Higher interoperability of the solutions means wider options for integration of compatible services to create a  custom ecosystem of sufficient scale that is at the same time cost-effective. Where each particular process is supported by corresponding unit of interoperable software, the approach results in efficient map of processes based on the network of applications.

# ONLYOFFICE solutions overview

ONLYOFFICE collaborative solutions, including online document editors called ONLYOFFICE Docs and the full-stack online ONLYOFFICE Workspace, offer an open-sourced, security-oriented alternative to public cloud office applications. ONLYOFFICE software can be deployed on private infrastructure to transfer the responsibility of data control and protection to the user, to provide an opportunity to follow own data protection protocol.

## Licensing model and commitment to open source

ONLYOFFICE sticks to double licensing model  where the code of the solutions is openly released for public under AGPL V3 (ONLYOFFICE Docs) and Apache 2.0 (ONLYOFFICE Groups) licenses, with certain protected components and scalability limitations in enterprise-grade editions.

The production of the software, technical support, QA, promotion and sales are carried out by an in-house team, while the contributing community freely takes part in the creation of extensions and apps, documentation and API writing, testing and other authorized activities.

## Data security policy

ONLYOFFICE security policy adheres to the principles of data minimalism and integrity, provides necessary tools for data protection in every possible aspect - document, storage and traffic encryption, access control, monitoring and audit, backup and migration functionality, user management with extensive controls for access rights and personalization. It is fully compliant with GDPR, and provides all required technical safeguards for compliance with HIPAA. ONLYOFFICE matches the requirements of ISO 27001 standard and HDS.

## Licensing model and commitment to open source

ONLYOFFICE sticks to double licensing model  where the code of the solutions is openly released for public under AGPL V3 (ONLYOFFICE Docs) and Apache 2.0 (ONLYOFFICE Groups) licenses, with certain protected components and scalability limitations in enterprise-grade editions.

The production of the software, technical support, QA, promotion and sales are carried out by an in-house team, while the contributing community freely takes part in the creation of extensions and apps, documentation and API writing, testing and other authorized activities.

## Data security policy

ONLYOFFICE security policy adheres to the principles of data minimalism and integrity, provides necessary tools for data protection in every possible aspect - document, storage and traffic encryption, access control, monitoring and audit, backup and migration functionality, user management with extensive controls for access rights and personalization. It is fully compliant with GDPR, and provides all required technical safeguards for compliance with HIPAA. ONLYOFFICE matches the requirements of ISO 27001 standard and HDS.

## Compatibility and interoperability

ONLYOFFICE editors are built to work with maximum compatibility with OOXML formats that make up to 99% of world's electronic documents. This makes it the only alternative to have full support for the formats that maintain complete interoperability with external sources of electronic data in the form of office type document.

Thanks to open API and the provided documentation, it is possible to integrate ONLYOFFICE editors with any existing environment either built on an enterprise sharing service or content management system, or use as a component for a custom web application. ONLYOFFICE already works in integration with over 30 well-known platforms and has been implemented in over 100 custom applications.

Native file management system incorporated in ONLYOFFICE Groups and consequently ONLYOFFICE Workspace allows interconnection with third-party storage services. At the same time, functionality of the platform and the editors can be extended with third-party addons, making ONLYOFFICE a highly interoperable host environment for additional software to use along with built-in functionality.

### Onboarding

ONLYOFFICE suite is built with ribbon-like tabular UI and similar feature naming code to those of other online suites, with intuitive user experience supported by thorough documentation and self-learning materials. At the same time, the technical guides for developers are available along with open API libraries and three levels of professional technical support.

### Pricing model

ONLYOFFICE provides double licensing model for enterprise solutions where ONLYOFFICE Docs suite is scalable based on the number of simultaneously edited files, while ONLYOFFICE Workspace plans are calculated by number of users. Developer Edition of the Docs suite is distributed with instance-based pricing. Enterprise-ready version comes with lifetime license meaning that it can be deployed and used for unlimited period of time with included professional service and update period limited by one year. The Develper Edition of ONLYOFFICE Docs provides licenses for one year of exploitation.

# Implementation examples of open collaborative technologies in government offices

### The General Secretariat of Economic and Financial Ministries of France

The General Secretariat of Economic and Financial Ministries employs ONLYOFFICE suite in integration with Alfresco Digital Workplace (ADW) to build an infrastructure for online collaboration on documents for its offices. The deployment and optimization was carried out by Atol CD, a French integrator of open-source solutions and a partner of Alfresco. Series of internal and external texts helped set up an operational solution in September 2020.

ONLYOFFICE in integration with ADW allows central administration of the Secretariat to collaborate on electronic documents within ADW among nearly 10,000 users - on MEF network infrastructures and in compliance with very advanced security policies.

The developers made the connector for ONLYOFFICE-Alfresco integration available to a wider number of users by opening its source code: it can be further compiled by third-party developers seeking custom ONLYOFFICE integration within their services.

### Government of Laos

In late 2020, Laotian software company SB LAB 856 Co., Ltd deployed the operational ONLYOFFICE instance with Nextcloud to create a collaborative environment with secure file sharing and collaboration for the government employees.

The existing IT infrastructure of Laotian government suffered from technological limitations, namely prevalent local file storage and no agile file sharing methods, need for real-time content collaboration and unavailability of authorized document editing tools on mobile devices.

Having paired online file sharing service provided by Nextcloud with ONLYOFFICE Docs, it was possible to assemble secure file storage in the private cloud with built-in online editing collaboration to automate paperwork and additionally protect data. The choice in favor of ONLYOFFICE as a primary editing suite was defined by being a cost-effective alternative to MS Office that could be deployed in the private network and provided necessary adjustments for working with required text font families.

**City of Hopewell, USA**

During the COVID-19 pandemic, the administration of Hopewell, Virginia, USA adopted ONLYOFFICE Workspace to establish a remote working environment for over 500 employees, including police officers, municipal workers, officials and other personnel.

The choice of ONLYOFFICE Workspace as singular collaborative environment was made in response to the administration's IT requirements and existing challenges. The solution provides secure remote access, sharing and co-editing documents in real-time, familiar user interface, compatibility with OOXML file types, and satisfactory plans for customer support.

On-premise file sharing model was chosen to avoid mass data migration to the public clouds provided by considered alternatives such as Microsoft 365, Box and Dropbox.

Opting for ONLYOFFICE Workspace also saved the budget of $30,000 if compared to similarly scaled alternative public cloud solutions.

# Conclusion

Government bodies seek fully compliant associates to provide collaborative software that will serve the tasks of an organization acting in public interest, limited by regulatory laws in data processing, the existing infrastructural conditions and heavy bureaucratic budgeting.

However, it is possible to retreat from default costly traditional solutions that assume risk of vendor lock-in and do not guarantee the desired level of data independence - in favor of open technologies that can help build custom sovereign infrastructures with transparent data flow.

Among present-day collaborative solutions of the open-source niche, ONLYOFFICE produces collaborative applications for working with documents that can be integrated or built into any existing environment with high level of compatibility with most used data formats and opportunities for customization and co-development of an effective collaborative solution within digital partnership.