Alinto

White paper
November 2022

DIGITAL SOVEREIGNTY: WHAT ARE THE CHALLENGES FOR BUSINESS E-MAIL?

Content

Introduction

Digital sovereignty is more than ever at the heart of companies' concerns. **It raises questions about data protection, confidentiality, and the independence of companies from American suppliers (particularly GAFAM)**.

This is a significant issue in a very tense geopolitical situation (war in Ukraine, crisis in Taiwan, etc.), and where the majority of cyberattacks originate from authoritarian countries such as Russia or China (according to the Carbon Black[1] report). European companies must protect their data and focus on sovereignty more than ever.

Open-source technologies provide some answers. Thanks to the transparency of the software, companies can see how the applications operate and therefore how the data is stored and used. Furthermore, several national and European initiatives are coming up to challenge the big companies in the industry:

Regulations (GDPR), awareness of sovereignty, and evangelization about open-source technologies...

Business email is also affected. Their exposure to cyberattacks makes them a priority in terms of security, while their operation, in terms of data routing and storage, remains complex. Digital sovereignty, European initiatives, and the potential of open source for the security of professional messaging systems are all evaluated in this white paper.

[1] https://www.developpez.com/actu/216086/La-Russie-et-la-Chine-sont-les-deux-principales-origines-des-cyberattaques-dans-le-monde-entier-d-apres-un-rapport-de-Carbon-Black/

Digital sovereignty challenges

There are debates on digital sovereignty at the centre of companies' digital strategies. Sovereignty is not just a protectionist buzzword to compensate for Europe's digital lag. It aims to **ensure the prosperity and independence of companies** by protecting their data, customers and fellow citizens.

Businesses can meet three major challenges by choosing a sovereign digital solution. Here are some explanations.

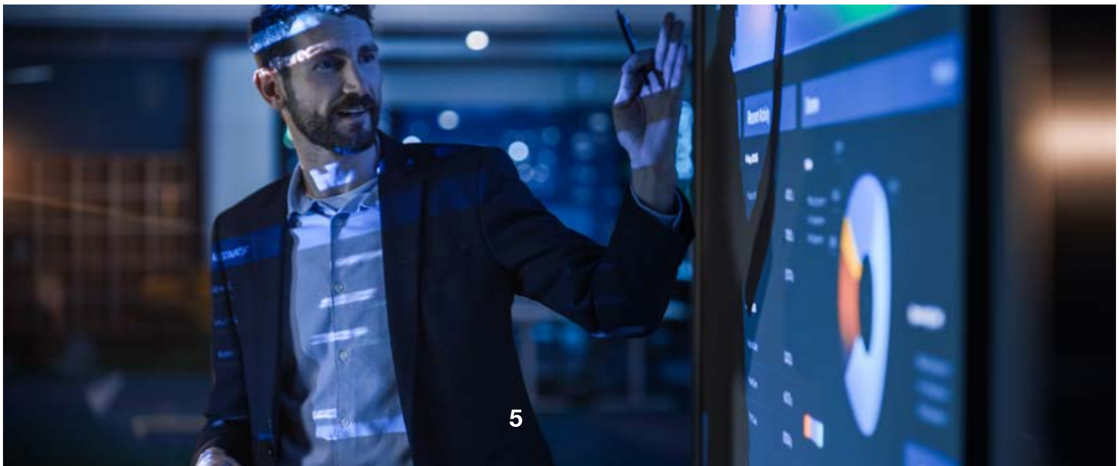
Sovereignty to keep control of your data

The topic of data privacy is on the agenda of most companies. The awareness in Europe has accelerated since the RGPD came into force in 2018. Indeed, not all countries and not all legislations offer the same level of data protection. It is necessary **to map them, to ensure that they are protected and inaccessible to malicious individuals**.

Organisations can use several solutions to protect their data.

- Host them on a **sovereign cloud** that is located in Europe and is managed by companies that follow European law. This can be certified by various labels, such as SecNumCloud, which is the most demanding certification for hosting in France.
- Opt for **open-source software** and/or European software
- Train employees in the various **data protection** regulations.
- **Raising employee awareness** of the importance of appropriate data management.

Sovereign hosting protects your data from hostile access legally. It is the foundation of a good control strategy for companies that want to capture value from their data while ensuring confidentiality for their customers.



Sovereignty to counter the cloud act

The Cloud Act has been in effect in the United States since 2018. It states that US authorities can request communication service providers subject to US law to provide them with data under their possession, care or control, **regardless of the location of the data**. This poses a serious threat to the data of European companies that are hosted by US providers, including in data centres based in Europe. Under the Cloud Act, these service providers can exploit data, even confidential data, beyond the initial intended use.

Europe's digital sovereignty aims to put in place **safeguards against unlawful access by certain countries**, to regulate access requests by foreign authorities, and to prevent transfers of non-personal data.

Two European regulations are currently being considered for this

- **The data governance act**: adopted in May 2022, it will be applicable in September 2023. It aims to facilitate the sharing of personal and non-personal data by setting up intermediation structures.

- **The data act** was presented in February 2022 and aims to ensure a better distribution of the value from the use of personal and non-personal data between the players in the data economy, particularly in relation to the use of connected objects and the development of the Internet of Things.

Sovereignty to counter the expansion of GAFAM

The GAFAM[1] represents a major threat to digital sovereignty. There is a considerable economic weight to these American digital giants: "the cumulative stock market valuation of the GAFAM reached "5,853 billion dollars" in 2020, i.e. a value greater than the GDP of Japan, the 3rd largest economy in the world"[2].

This domination is not only economic, but also concerns digital dependency. These companies are, in fact, in a position to process and store the data of citizens and companies from all over the world (datacenters, messaging systems, clouds, etc.), which are "transferred" to them in a more or less conscious manner when using services or applications. Incidentally, it should be remembered that the GAFAM are subject to American legislation. They are subject to the Cloud Act, which allows them to transmit data in their possession to third parties.

Therefore, the rest of the world, and especially Europe, must counter this power by creating a truly sovereign ecosystem. How can this be done? By changing the regulations on this subject, encouraging the use of open-source software, and talking about the challenges of digital sovereignty.

[1] Google, Amazon, Facebook, Apple, Microsoft

[2] https://fr.countryeconomy.com/gouvernement/pib

Digital sovereignty: European initiatives

To achieve European digital sovereignty, it is essential to regulate the use, storage, and collection of data. This necessary data protection continues to provoke a complex debate among member countries. This has not stopped the European Union from taking several initiatives on this subject. Let’s take a look at some of them.

The General Data Protection Regulation (GDPR): the starting point

Coming into force in May 2018, the GDPR is a first step towards digital sovereignty. It regulates the access, storage, and use of personal data of European citizens. For this, companies holding such data must meet several requirements (deletion of data, consultation on request, appointment of DPO…). The same regulation stipulates that personal data from the EU may only be transferred to countries that offer similar protection and that the EU considers "appropriate"[1].

However, the US legislation, for example, is much less strict than the RGPD. The Cloud Act allows the US government to access data held by US companies. And culturally, Americans consider data to be an asset that can be traded. **Despite these differences, many European companies entrust their data to large American digital service providers, especially for hosting**. This has prompted the EU to take further initiatives to regulate the data market.

[1] Consultar https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Data Governance Act and Data Act : The way forward

These two regulations complement the GDPR. They aim to develop a single market for data that supports the access, sharing, and re-use of data, in line with EU values.

The Data Governance Act will be applicable in September 2023. It aims to promote the sharing of personal and non-personal data by setting up intermediation structures. The latter will clearly define the conditions under which data held by the public service can be reused, and thus compete on equal terms with international market players.

The Data Act aims to establish harmonised rules on access to data generated by connected objects and the various related services. The goal is to facilitate access, management, and sharing of this data.

The NIS2 directive : Sovereignty and Cybersecurity

The European Network Internet Security Directive, known as NIS2, aims to strengthen companies and organizations cyber risk management. It will result in new obligations, such as security measures, supervision rules, and the obligation to notify any attack to national cybersecurity agencies, such as ANSSI in France.

A risk analysis will allow each member state to draw up a list of the organizations covered by this directive. It is estimated that several thousand entities related to digital services, the space industry or research will be subject to this directive, which is currently being adopted.

CNIL and ANSSI: A French example of how local authorities ensure compliance in France

France has two bodies that are responsible for ensuring that data protection regulations are applied and for helping companies and citizens deal with the cyber threat.

The National Commission for Information Technology and Civil Liberties (CNIL), sometimes called the digital policeman, is a government agency responsible for the regulation of personal data. It has several missions:

- **Informing and protecting rights**: it responds to information requests from professionals and individuals regarding data protection. It also handles their complaints.
- **Supporting compliance**: it offers a toolbox to help companies achieve compliance.
- **Anticipating and innovating**: it helps to develop privacy-protective solutions, advises companies, and helps to start a discussion about the ethical issues around data.
- **Control and enforce**: it ensures that the law is applied in practice.

The ANSSI (Agence nationale de la sécurité des systèmes d'information, the French information system security agency), provides expertise and technical assistance to organisations in the field of cybersecurity. It provides a monitoring, detection, alert, and reaction service to computer attacks.

Action by European governments : real recommendations

Governments have an important role to play in moving towards digital sovereignty. Their actions are influencing the choice of technological solutions. Their decisions contribute to the promotion of the know-how of the European digital players. **Local authorities and businesses have been pushed to turn to open-source solutions or software produced by local publishers for some time now**.

The development of Europe’s digital ecosystem gives people a real alternative to the GAFAM, and gives them control over their data.

Europeans are aware of the issues related to digital sovereignty. The attention of citizens has been awakened by regulations such as the GDPR. The media are reporting on the health data leaks or the opportunity provided by health data. Europe has taken some initiatives, but they are not enough to counter the power of the American giants. However, **these regulations show the way to more respectful ways of handling citizens’ data**.

Sovereignty and cybersecurity : Closely linked?

Cybersecurity is a prerequisite for digital sovereignty at a time when cyberattacks are increasing in number and sophistication. Information systems are increasingly complex, with public/private interconnections and often permeable borders. At the same time, the volume of email exchanges is constantly growing, providing a multitude of entry points for cyber threats.

When it comes to data protection, **cybersecurity and sovereignty are indissociable**. Here is why.

Digital sovereignty, the first step towards data protection

According to the article "Digital Sovereignty: European initiatives," sovereignty aims to better protect European organizations' and citizens' data. When a partner claims to be sovereign, one expects that he will only use the data for the specified purposes, and that he will not disclose them. This guarantee is obviously ensured by the control, storage, and processing put in place, the respect of regulations, and the technological solutions used (sovereign hosting, open-source software…)

The threat of cyber-attacks or data disclosure can be reduced by using a European service provider.

Cybersecurity: protection against external threats

By definition, cybersecurity is a set of measures aimed at ensuring the security of computer systems and data from malicious acts. Cyberattacks have a serious impact on companies. Consequently, they must be able to deal with such an event and implement IS security measures.

This includes deploying of protection software (antivirus, for example), system update plans (patches) and authentication systems, as well as training employees on good cybersecurity practices.

Many companies are unaware that they have sensitive data, or think that an attack only happens to others. Unfortunately, the number of cyberattacks is constantly increasing, and the techniques used by cybercriminals are becoming more and more sophisticated. **The consequences can be dramatic**.

For example, as a victim of a ransomware attack, the Corbeil-Essonnes hospital in the south of Paris had some sensitive data (computerised patient file, personal data, etc.) disclosed on the Internet[1] following its refusal to pay a ransom.

[1] https://www.liberation.fr/societe/sante/faute-de-rancon-les-donnees-volees-dans-un-hopital-de-lessonne-se-retrouvent-mises-en-ligne-20220925_PMF2MYWN5NAW3BLNDXF7Q34BZY/

No sovereignty without cybersecurity

Digital sovereignty alone isn't enough to protect data without also protecting it against cyberattacks.

Certainly, digital sovereignty makes it possible to better control one's data. However, if a software environment is too open or exposed, certain vulnerabilities will persist. It is not possible to separate sovereignty from cybersecurity. It is essential to promote good security habits within companies and to build a European cyber offer that is a real alternative to the solutions of American majors.

While they wait for a system like this to be put in place, companies should use cybersecurity solutions, such as antivirus software, back-up plans, experts who can help them, and follow the advice of reference organisations like the ANSSI in France and rely on as much as possible on solutions from local business experts working on open-source solutions.

There are dangers in business e-mail!

The evolution of remote working, the adoption of cloud solutions, the hybridisation of information systems, and other factors increase the vulnerability of companies to cyber threats. **While attackers targeted infrastructures a few years ago, today they target humans and rely on users' lack of vigilance**. And what better way to attack than with email?

Therefore, business email poses a risk to the protection of company data. Fortunately, there are sovereign solutions that provide better security. Here are some explanations.

Business e-mail: the most common target for cyberattacks

Email is a privileged entry point for cyberattacks, with nearly 300 billion emails sent each day. This communication channel allows companies to share data and information that is more or less confidential. The opportunities for cybercriminals are especially high in these exchanges. This is shown by the numbers:

83 % **of respondents said their company had experienced at least one successful email phishing attack in 2021.**[1]

Sending harmful attachments, sharing malicious links, and requesting bank details are all techniques used to trap email recipients. Without greater awareness among employees and appropriate tools, companies are exposed to the risk of data breaches, which can have disastrous consequences.

[1] Informe «State of the Phish», 2022

E-mail and sovereignty: mission impossible?

How can we prevent cyberattacks? The answer is not so easy. The sophistication of hackers is increasing, and there is **no such thing as zero risk**. Nevertheless, it is possible to minimize the risk and improve the protection of your data by taking particular care when choosing a professional email provider.

The solutions managed by the GAFAM are not sovereign innately. They collect data and store it in datacenters not subject to European sovereignty rules. Therefore, it is not possible to ensure their confidentiality and maintain control of them as a company. Moreover, their messaging systems are closed code software, reinforcing the dependence on a supplier, with no transparency on the processing, contrary to the principles of digital sovereignty.

However, solutions exist and offer real alternatives: open-source messaging systems.

What is a good professional e-mail service?

Between the requirements of sovereignty and cybersecurity, what is the ideal business email solution?

The ideal business email solution is sovereign

It is obvious that it is an email messaging system developed by a European editor, or an open-source project. The latter provides more transparency as to how it works and the responsiveness of a community to fix potential weaknesses. Be careful, though. There's no point in having a local partner if your hosting company doesn't meet all the sovereignty requirements.

The ideal messaging system is therefore made up of software published in Europe, operated by a service provider under European law who hosts it on infrastructures in Europe, secured in accordance with European recommendations.

The ideal business email is secure

A well-designed business email system includes a complete security arsenal. The security solutions integrated in the standard versions of professional messaging systems (antispam, smtp relay…) are often not enough. Many companies do not invest in additional security solutions. **Until the day they are victims**.

A sound professional email system must therefore include the best technologies to ensure email filtering, but also the proper delivery of emails, while protecting the reputation of the email domain. This is something that few email systems offer by default.

To protect against email cyberattacks, the ideal messaging system must respect several criteria. First, choose a sovereign hosting partner, then a European email provider. To go further, companies can select an open-source solution, thus ensuring the transparency of the software code. Finally, additional security solutions should not be underestimated for a total protection of the messaging system.

Open source to the rescue of business email services

Email is an application that is part of everyday business life. The use of messaging goes beyond simple email exchanges. It is a real collaborative tool and a universal means of communication that saves time and dematerialises many communication exchanges.

It is important to have a good email system, that is intuitive to use, ergonomic, reliable, and safe. In the field, GAFAM dominate the market with messaging systems integrated into their office suites, such as Office 365 or Google Workspace. However, alternatives are available. These include open-source messaging systems.

The benefits of open-source e-mail systems

The huge advantage of open-source email solutions is that the software code is available freely . Their use is not conditional on the purchase of a licence, and **companies are not tied to a supplier**. Integration into the information system can be carried out internally or by an integrator, with no commitment to the latter. Moreover, the openness of the software code also makes it possible to adapt it to very specific needs, at a lower cost.

Choosing open-source means taking advantage of a community of users, who constantly enrich and improve the solution. Whether it is ergonomics, functionalities, or security, the contributors are full of ideas and bring their skills to make the solution evolve and adapt to the needs of organizations.

From the IT department's perspective, it is above all the technical sustainability that counts in the balance. For IT specialists, **open-source messaging systems are often better to implement than those of the tech giants because they call on their business know-how**.

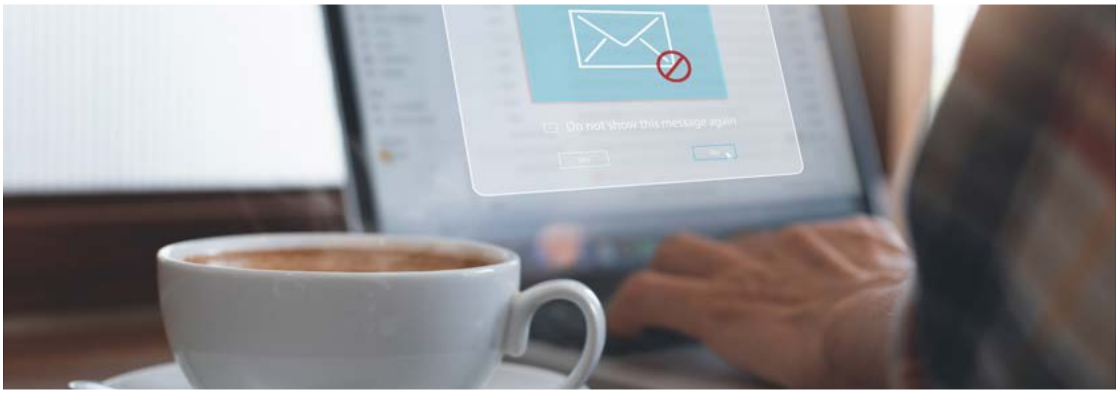
Open-source email systems and sovereignty

The security of business e-mail is addressed at different levels. When looking at the data, it is important to ask where it is being stored. How does it get accessed? Open-source solutions do not enforce any rules on companies. They are therefore free to select their data hosting provider and ensure that the data is processed properly.

To ensure continuity of service, companies can subscribe to a "business recovery plan" in the event of an incident, in accordance with the terms and conditions defined with their hosting provider. Selecting a European and open-source e-mail system, combined with sovereign hosting, provides an essential security base. The company's data is not covered by the Cloud Act, the American law that applies to GAFAM messaging solutions.

Even though there is no such thing as zero risk in terms of cybersecurity, hackers prefer to target large publishers, who have a large share of the market. With a comprehensive email security arsenal, this risk can be reduced.

It is also essential to ensure that the email system can interface with the company's IT architecture and communicates with other tools. **Here again, open source is an interesting alternative**.



The example of SOGo webmail

SOGo is an open-source webmail solution that allows to share calendars, address books and email within an organisation. The solution is completely open and freely available, if organisations choose to deploy it internally by themselves.

Based on AJAX, SOGo is a universal and responsive webmail. It is the front end component of the messaging infrastructure that provides users with a complete information access interface. It has a community of several thousand contributors who continually improve the solution.

For companies that want to have full integration and support, Alinto offers since 2022 a professional cloud version of SOGo, with dedicated support and 24/7 monitoring. **The solution, which is totally secure, relies on a sovereign hosting**.

Messaging has a role to play in the path towards digital sovereignty. Open source combined with European cloud hosting is a way to achieve this. Organisations are increasingly turning to these technologies. Although this transformation may take time due to the inertia of solution life cycles and market renewals, the trend is definitely there.

Conclusion

Organisations are increasingly focusing on digital sovereignty. There are many reasons for this:
Keeping control of data, promoting the use of European software, and keeping independence from large US and other global suppliers.

Europe’s governments are promoting open-source initiatives, and companies are becoming less reluctant to use them. It is in their interest to take advantage of this opportunity to keep control of their data. And this begins with business messaging and its security.

About us

Founded in 2000, Alinto is a company specialised in the email business: email and security services in SaaS or PaaS mode… through several products:

- **SOGomail** : a secure and collaborative email server that integrates the fully responsive SOGo webmail

- **Cleanmail** : a secure email relay that protects against cyber threats while providing continuous access to email.

- **Serenamail** : a SMTP mail relay that allows servers or applications to send emails to offer so-called “clean” traffic.

The European specialist in secure e-mail solutions, Alinto, is responding to the new expectations of the market by turning more actively towards open source. The editor took over the SOGo webmail and its community and the MailCleaner e-mail filtering.

But why turn to open-source? Above all, it is a question of digital sovereignty. With open source, the software code is available to users and companies can keep control over the hosting, storage, operation and especially the reversibility of the data. For the Alinto teams, open source offers the choice to their customers and partners of digital sovereignty. This is also the opportunity to offer a strong and sustainable alternative to GAFAM.

“In our opinion, open-source is essential to give users the freedom of choice. It’s an important element for diversity, and it’s a way for us to offer companies alternatives to the messaging tools of American cloud players,” says **Philippe Gilbert, CEO of Alinto**.

Lyon (Headquarter)
15 quai Tilsitt
FR-69002 Lyon
+33 481 09 01 10

Barcelone
Paseo de Gracia,101-4°1
SP-08008 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Lausanne
Rue des Jordils 40
CH-1025 St-Sulpice
Tel: +41 21 695 20 20

Alinto

www.alinto.com