Security/Confidentiality

The security of the Gestan Cloud solution relies on a set of complementary elements: * infrastructure security * server maintenance * server protection against malicious actions by hackers * security of connection methods and data transmission * reliability of technical personnel with authorized access.



Infrastructure Security

Gestan Cloud servers are managed by Netsyst, an IT engineering services company based in Lyon and founded in 2011, comprising a team of systems, network, and data center consultants.

The company guarantees the security of its facilities through: * intrusion protection, * fire protection, * personnel access controls, * personnel authorization for handling confidential data.

Gestan Cloud production servers are located in a data center in Lyon, while backup servers owned by ICS-Informatique are located in another data center in Lyon, also managed by NetSyst.

Server Maintenance

Netsyst is also responsible for the technical maintenance of the physical servers and handles hardware upgrades whenever necessary.

When new machines offer a favorable cost-to-performance ratio, ICS may undertake a migration from one machine to another.

Currently, the standard profile for Gestan Cloud servers is:

Core-4-S-SSD 2 x Intel® Xeon E5 2620v4 128 GB 3 x 500 GB SSD 1 Gbit/sec 500 Mbit/sec RPNv2

Each server hosts approximately one hundred clients. ===== Server Protection =====

NetSyst’s server security monitoring ensures a high level of protection against malicious attacks. To this end, NetSyst implements:

- machine virtualization
- system snapshots with every software update

- additional data backups
- technical monitoring (CPU, disk space, etc.)
- security policy enforcement (firewall settings, proxy settings, etc.)
- antivirus alert monitoring

Brute-Force Protection

All Gestan Cloud servers are equipped with brute-force protection software.

DDoS Protection

DDoS protection is provided by NetSyst.

We have previously withstood several DDoS attacks that disrupted traffic for a limited time; these attacks were successfully contained within a few hours.

Secure Transmission

Communications between your computer and the Gestan Cloud servers use the HTTPS protocol—the same protocol used by your bank, for example.

This communication protocol, now a global standard, ensures the highest level of communication confidentiality.

Internal Security Procedures

Within ICS-Informatique, only Cloud technical support staff have access to your login credentials. All staff members have signed a confidentiality agreement.

The credentials we provide to you are randomly generated to ensure an adequate level of resistance against attacks.

All server access is logged and subject to verification.

Disaster Recovery Plan (DRP)

The fire at the OVHcloud data centers (March 2021) demonstrates that while major incidents are rare, the risk is not zero.

All Gestan Cloud servers are virtualized using VMware, allowing for rapid service restoration.

In the event of an OVH-style incident affecting the production data center—and barring any other simultaneous major incident impacting NetSyst's availability—service recovery will proceed as follows:

- provisioning a new server at another NetSyst site: approx. 15 minutes,
- restoring the virtual machine: approx. 15 minutes,
- restoring data: approx. 10 minutes per client (equating to 17 hours for 100 clients, the standard server load).

Note that data remains constantly available to clients for local backups via a compression tool built into Gestan, which generates a ZIP archive ready for immediate local use.

Legal Context

The Gestan Cloud solution is 100% French: the software is developed by ICS-Informatique (a French SARL), and the servers are managed by NetSyst (also a French SAS) in data centers located within mainland France.

French companies are subject to legal obligations that are often little-known, including the following:

- filing of documents accounting records outside the European Union is prohibited
- storing your electronic invoices outside the national territory requires a mandatory declaration to the tax authorities
- personal data processing must comply with French legislation, specifically the "Data Protection Act" (Loi Informatique et Libertés) No. 78-17 of January 6, 1978 as well as the GDPR.

France: The Intelligence Act's "black boxes"

A provision of the 2015 Intelligence Act, ostensibly aimed at combating terrorism, allows the State to install “black boxes” on hosting providers' infrastructure, operated by the DGSI and the DGSE.

The exact operation of these “black boxes” is currently unknown: while the State legally monitors Internet transmissions, it is unclear what data is actually transmitted to the DGSI and DGSE, let alone how that data is utilized.

USA: The Patriot Act

It should be noted that service providers based in the United States cannot guarantee the confidentiality of your data.

Indeed, since the introduction of the Patriot Act in 2001, US legislation has allowed security agencies to access all personal data. This applies to data belonging to:

- US companies, even if the data is physically stored within European territory
- their subsidiaries, even if they are located in another country
- servers hosted in the United States, even if the company owning the servers is of a different nationality

This intrusion into your data does not require judicial oversight, nor does it need to be made public: your information can be read, copied, retained, and disclosed to third parties without your knowledge.

i Other “Cloud” articles

Astuces pour Gestan Cloud
Avertissement de sécurité lors de la connexion à Gestan Cloud via rdp (avril 2026)
Bureau à distance Gestan Cloud
Connexion Gestan Cloud via RDP Windows
Connexion à Gestan Cloud
Double connexion
Etat des serveurs Gestan Cloud
Etat des serveurs Gestan Cloud (archives)
Imprimer avec Gestan Cloud
Problème de connexion à Gestan Cloud
Sécurité/Confidentialité
Transférer vos données dans le Cloud
Vérifier votre votre connexion Internet

From:
https://manuel.gestan.fr/ - **Le manuel de Gestan**

Permanent link:
https://manuel.gestan.fr/en/cloud/security

Last update: **2026/10/10 21:12**