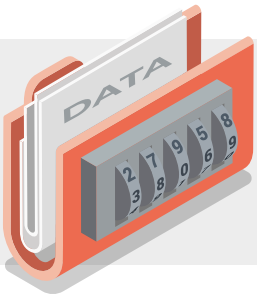
oplon® SECURE ACCESS

GDPR compliance

The **GDPR** is a European legislation that came into effect on May 25, 2018, governing the protection of personal data of European Union (EU) citizens. Below is a brief description of the key points of the GDPR, followed by an explanation of Oplon Secure Access's compliance with each point.

1. Scope

The GDPR applies to all companies processing personal data of EU citizens, regardless of the company's location.



With Oplon Secure Access, personal data is stored and managed only by the customer using it and is not stored anywhere else.
All collected data is recorded in a specific database and in well-defined video representations, which can be activated only in specific cases.

2. Fundamental Principles

TRANSPARENCY, FAIRNESS, AND LAWFULNESS IN DATA PROCESSING

When security needs (PAM) require the collection of potentially personal data, the system notifies operators that actions are being recorded. In cases where the law does not allow tracking with personal data, Oplon Secure Access does not record these operations.

PURPOSE LIMITATION

Data can only be collected for specific, explicit, and legitimate purposes.

With Oplon Secure Access, personal data is stored and managed only by the customer using it and is not stored anywhere else. All collected data is recorded in a specific database and in a well-defined video representation, which can be activated only in specific cases. It is, therefore, up to the customer to enable tracking that can collect personal data only in specific cases (e.g., PAM).

DATA MINIMIZATION

Processing must be limited to data strictly necessary for its purpose.

With Oplon Secure Access, it is possible to enable and disable tracking features based on specific needs. Their accessibility is limited to the number of people that Oplon Secure Access customer enables for consultation. Since there is no tracking data in other locations, the data is exclusively available to authorized individuals.

DATA ACCURACY

Data must be accurate and, if necessary, updated.

When necessary and enabled by the customer, data is collected as it passes through the Oplon Secure Access Virtual Appliances installed by the customer, thus sourced directly. Only individuals authorized by the customer can view this data, and it cannot be altered by others since it is not available to anyone other than those authorized by the customer.

STORAGE LIMITATION

Data must only be stored for the time necessary to achieve its purposes.

With Oplon Secure Access, it is also possible to delete collected data by setting retention time gaps. Deletion operations are configurable and automatic. The temporality of data is important to preserve automatic forgetting on one hand and to provide the customer with a time window to analyze data within the permitted and enabled collection areas.

3. Data subject rights

The GDPR grants EU citizens several rights, including the right to access, rectify, delete, restrict processing, and data portability.

All collected data, within the service's purpose limits, is stored in archives accessible only to the customer. Data is collected in a relational database and as video footage, where enabled.

Since any collected personal data, within the service's subject purpose limits, is maintained exclusively by the customer and only those elected by the customer to handle this data, there is no possibility for third parties to exfiltrate data.

4. Responsability and Accountability

Companies are responsible for GDPR compliance and must demonstrate compliance through documentation and recording data processing activities.

Oplon Secure Access centralizes any potentially personal data, only if enabled for specific purposes, into two "containers": the relational database and any video recordings of window system activities. By reducing collected personal data to these two containers, the customer can activate access procedures for this data and produce the necessary documentation for processing.

5. Data Protection Officer (DPO) Appointment

Certain organizations must appoint a DPO, an independent data protection expert, to monitor compliance.

Oplon Secure Access assists organizations that require a DPO appointment by ensuring that any personal data collected within specific and explicitly enabled services is confined to two containers, a relational database, and any graphical session videos.
This way, the collected data can be protected and constantly monitored.

6. Data Breach Notification

With the introduction of the Italian Cybersecurity Bill on 19/06/2024, public administrations, including central ones and local health authorities, are required to notify the competent authorities of data breaches within 24 hours of their occurrence.

Oplon Secure Access limits the possibility of data exfiltration because it is not accessible by third parties.
Should a breach occur, it is possible to immediately identify any compromised entities, notify the authorities in a very short time, well within the 72 hours required by European law, in full compliance with the new Cybersecurity Bill.

7. International Data Transfers

Transferring data outside the EU is subject to restrictions, and companies must implement adequate security measures.

Oplon Secure Access collects data for specific purposes and enabled by the customer, only and exclusively in the customer's archives, which are the only ones authorized to access them within their services.

8. Data Protection Impact Assessments (DPIA)

In certain cases, organizations must conduct a DPIA to assess and mitigate risks associated with personal data processing.

The Oplon Secure Access data collection architecture, which is exclusively owned and processed by the customer, greatly facilitates DPIA activities. No personal data is retained outside the customer's scope and only in two archives, a relational database, and video session recordings where applicable. This, along with internal functions for appointing who can access this data, allows for easier DPIA facilitation.

9. Penalties

Regulatory authorities can impose significant fines for GDPR violations, including fines up to 4% of global annual turnover.

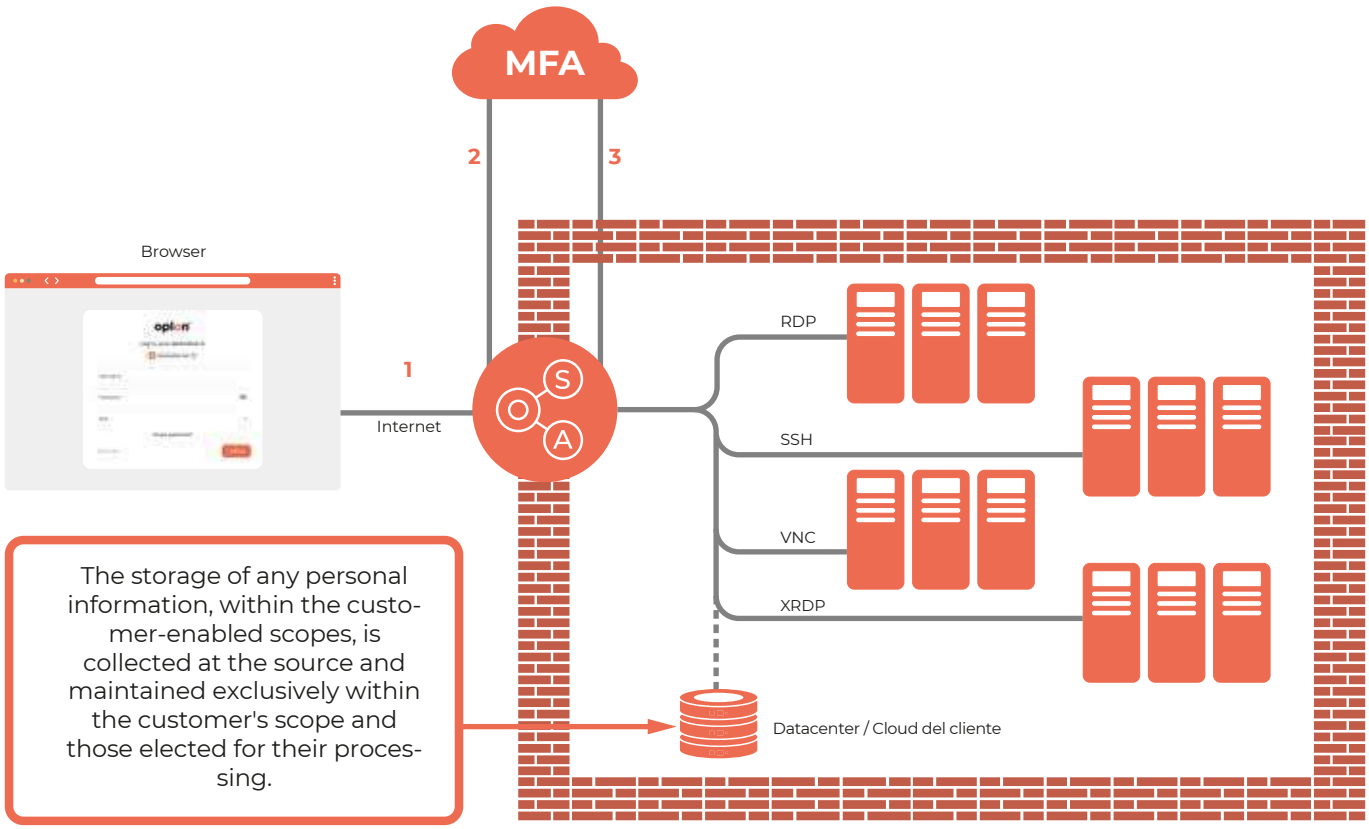
With Oplon Secure Access and an investment certainly less than 4% of turnover, it is possible to minimize this risk. Oplon Secure Access, through its data storage policy and the correct election of individuals who can access collected data by the customer, mitigates and minimizes this risk.

10. Consent

Consent for data processing must be freely given, informed, specific, and unambiguous. Users must be able to withdraw consent at any time.

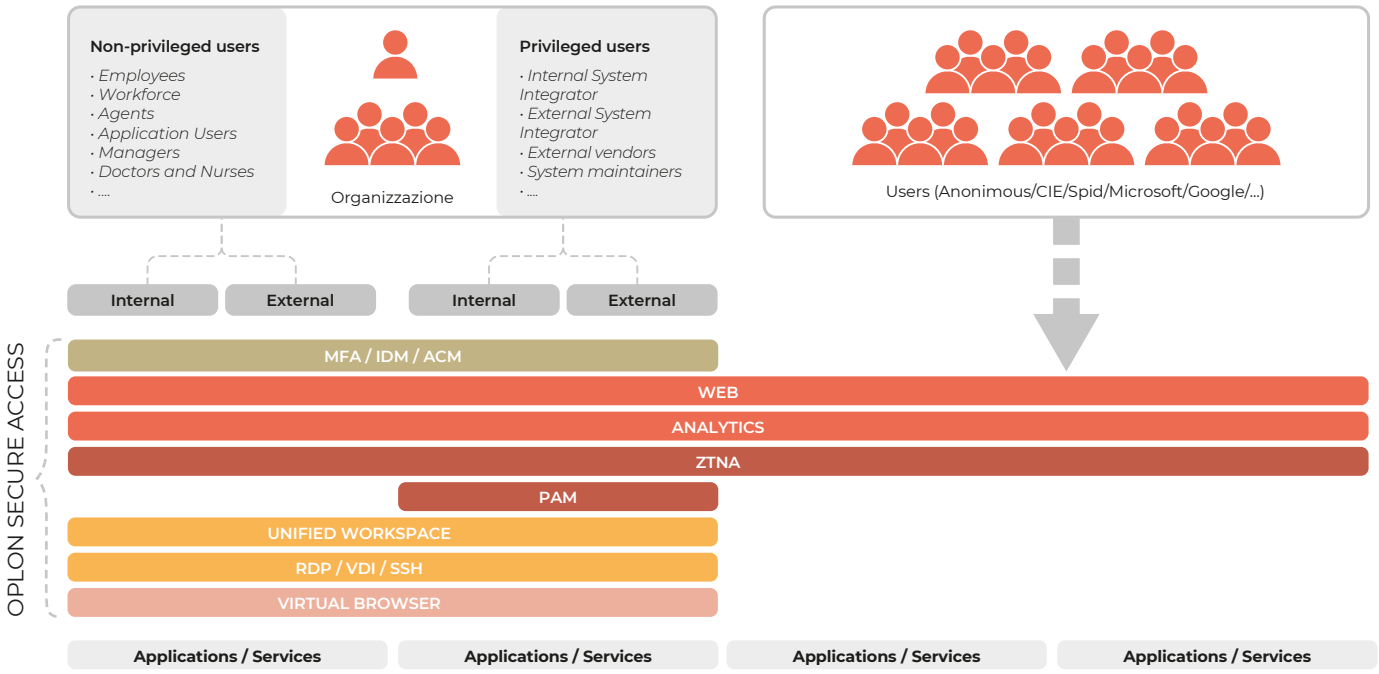
In cases where it is necessary to collect data that may be personal, it is possible to present the user with what is being collected both qualitatively and selectively. If the user does not accept these conditions, all their data can be permanently deleted, and the user can be immediately disabled upon request.

Oplon Secure Access: Data Collection Architecture



User Classification and Functionality

Users and their activities can be classified into the following groups and contexts, depending on the type of activity or service requiring differentiated treatment. The following scheme summarizes the functionalities used by the Oplon Secure Access platform and the level of information logging regarding users:



OSA Layers	Description
MFA / IDM / ACM	User identification and authorization
WEB	Https reverse proxy
ANALYTICS	Centralized logging system for user activities
ZTNA	System to provide specific services to users authorized by the organization
PAM	Logging system and temporal access limitations for users with high-privilege access to critical infrastructures
UNIFIED WORKSPACE	Virtual desktop presentation system with a list of services the user is authorized to access
RDP / VDI / SSH	Non-Web services typically provided with Oplon Secure Access via browser
VIRTUAL BROWSER	Internal HTTP/S services provided via browser activated within the infrastructure on Windows or Linux platforms and delivered through remote visualization via browser. This is an alternative option to the Reverse Proxy system for delivering web services

Note on VPN Usage and Privacy

Using Oplon Secure Access and eliminating VPNs allows users not to share, even accidentally, private information contained in their devices. This aspect of not sharing private information is often overlooked. Oplon Secure Access ensures that users, who are not IT technicians, do not share private information from their personal devices without needing to take precautions that would require undue technical knowledge.

Oplon Secure Access is the only system on the market today that guarantees operator privacy even when using their own laptop or personal computer.