oplon®
SECURE ACCESS
GDPR compliance

Il **GDPR** è una legislazione europea che è entrata in vigore il 25 maggio 2018 e disciplina la protezione dei dati personali dei cittadini dell'Unione Europea (UE). Di seguito troverai una breve descrizione dei punti chiave del GDPR a cui seguirà una spiegazione per ciascun punto della compliance Oplon Secure Access.

1. Ambito di Applicazione

Il GDPR si applica a tutte le aziende che trattano dati personali di cittadini dell'UE, indipendentemente dalla sede dell'azienda.

Con Oplon Secure Access, i dati personali sono memorizzati e gestiti solo dal cliente che lo utilizza e non vengono memorizzati in nessun altro posto.
Tutti i dati raccolti sono censiti in uno specifico database e in un flusso di rappresentazioni video ben determinato e attivabile solo in specifici casi.

2. Principi fondamentali

TRASPARENZA, LEALTÀ E LICEITÀ NEL TRATTAMENTO DEI DATI

Quando per necessità di sicurezza (PAM) devono essere raccolti dati che potrebbero essere personali, il sistema avverte gli operatori che le azioni sono registrate. Nei casi in cui la legge non permette il tracciamento con dati personali Oplon Secure Access non registra queste operazioni.

LIMITAZIONE DELLA FINALITÀ

I dati possono essere raccolti solo per scopi specifici, espliciti e legittimi.

Con Oplon Secure Access, i dati personali sono memorizzati e gestiti solo dal cliente che lo utilizza e non vengono memorizzati in nessun altro posto.
Tutti i dati raccolti sono censiti in uno specifico database e in un flusso di rappresentazioni video ben determinato e attivabile solo in specifici casi.
È quindi a sola cura del cliente abilitare il tracciamento che può raccogliere dati personali solo in specifici casi (es.: PAM)

MINIMIZZAZIONE DEI DATI

Il trattamento deve essere limitato ai dati strettamente necessari per il suo scopo.

Con Oplon Secure Access è possibile abilitare e disabilitare le funzionalità di tracciamento in base a specifiche necessità. La loro fruibilità è limitata al numero di persone che il cliente Oplon Secure Access abilita alla consultazione. Non essendoci dati di tracciamento in altri luoghi i dati sono esclusivamente a disposizione delle persone incaricate.

PRECISIONE DEI DATI

Devono essere accurati e, se necessario, aggiornati.

Quando necessario e abilitato dal cliente, i dati vengono raccolti durante il loro passaggio attraverso le Virtual Appliance Oplon Secure Access installate dal cliente stesso, quindi prelevati alla fonte. Solo le persone abilitate dal cliente possono visionare questi dati e quindi non possono essere alterati da altre persone perché non disponibili a nessun altro che non sia abilitato dal cliente.

LIMITAZIONE DELLA CONSERVAZIONE

I dati devono essere conservati solo per il tempo necessario per il raggiungimento degli scopi.

Con Oplon Secure Access è anche possibile cancellare i dati raccolti dando delle finestre temporali di mantenimento degli stessi. Le operazioni di cancellazione sono impostabili e automatiche.
La temporalità dei dati è importante per preservare da un lato l'oblio automatico e dall'altro garantire al cliente una finestra temporale per poter analizzare i dati negli ambiti consentiti e abilitati alla raccolta.

3. Diritti degli interessati

Il GDPR conferisce ai cittadini dell'UE una serie di diritti, tra cui il diritto all'accesso, alla rettifica, alla cancellazione, alla limitazione del trattamento e alla portabilità dei dati.

Tutti i dati raccolti, nei limiti dello scopo del servizio, sono conservati in archivi che solo il cliente ha a disposizione. I dati sono raccolti in un database relazionale e in forma di filmato video, dove abilitato.

Essendo eventuali dati raccolti personali, nei limiti dello scopo del servizio assoggettato, mantenuti esclusivamente dal cliente e solo le persone elette dal cliente a operare sui questi dati, non vi è possibilità da parte di terze parti di esfiltrare dati.

4. Responsabilità e Accountability

Le aziende sono responsabili del rispetto del GDPR e devono dimostrare conformità attraverso la documentazione e la registrazione delle attività di trattamento dei dati.

Oplon Secure Access, accentra eventuali dati che possono avere delle informazioni personali, solo se abilitate per scopi specifici, in due "contenitori": il database relazionale ed eventuali videoregistrazioni delle attività eseguite su sistemi a finestre. Riducendo a questi due contenitori eventuali dati personali raccolti, il cliente è in grado di attivare le procedure di accesso a questi dati e di produrre la documentazione necessaria al trattamento.

5. Nomina del Responsabile della Protezione dei Dati (DPO)

Alcune organizzazioni devono nominare un DPO, un esperto indipendente di protezione dei dati, per monitorare la conformità.

Oplon Secure Access facilita le organizzazioni che necessitano della nomina del DPO in quanto eventuali dati personali raccolti, nell'ambito di servizi specifici e abilitati esplicitamente, sono delimitati da due contenitori, database relazionale e eventuali video di sessioni grafiche a finestre. In questo modo i dati raccolti possono essere protetti e monitorati costantemente.

6. Notifica delle Violazioni dei Dati

Le aziende sono obbligate a notificare alle autorità competenti le violazioni dei dati entro 72 ore dal loro verificarsi, a meno che la violazione non sia improbabile che comporti un rischio elevato per i diritti e le libertà delle persone interessate.

Oplon Secure Access limita la possibilità di esfiltrazione di dati perché non in possesso di terzi.
Qualora si verificasse, è possibile identificare immediatamente eventuali soggetti violati, darne comunicazione alle autorità in tempi brevissimi e ben al di sotto delle 72 ore previste dalla legge.

7. Trasferimento Internazionale di Dati

Il trasferimento di dati al di fuori dell'UE è soggetto a restrizioni, e le aziende devono adottare misure di sicurezza adeguate.

Oplon Scure Access raccoglie eventuali dati per scopi specifici e abilitati dal cliente, solamente ed esclusivamente in archivi del solo cliente che è il solo abilitato all'accesso e nei luoghi nell'ambito dei propri servizi.

8. Valutazioni dell'Impatto sulla Protezione dei Dati (DPIA)

In determinati casi, le organizzazioni devono condurre una valutazione dell'impatto sulla protezione dei dati per valutare e mitigare i rischi associati al trattamento dei dati personali.

L'architettura di raccolta dei dati Oplon Secure Access che sono di esclusiva proprietà e trattamento del cliente, facilita enormemente le attività di valutazione dell'impatto della protezione dei dati (DPIA).
Nessun dato personale viene trattenuto al di fuori dell'ambito del cliente e solo in due archivi, database relazionale e immagini di registrazione video delle sessioni a finestre lì dove previsto. Questo, unitamente alle funzioni interne di elezione a chi può accedere a questi dati, permettono di facilitare le valutazioni di impatto sulla protezione.

9. Sanzioni

Le autorità di controllo possono infliggere sanzioni significative in caso di violazioni del GDPR, comprese multe fino al 4% del fatturato annuo globale.

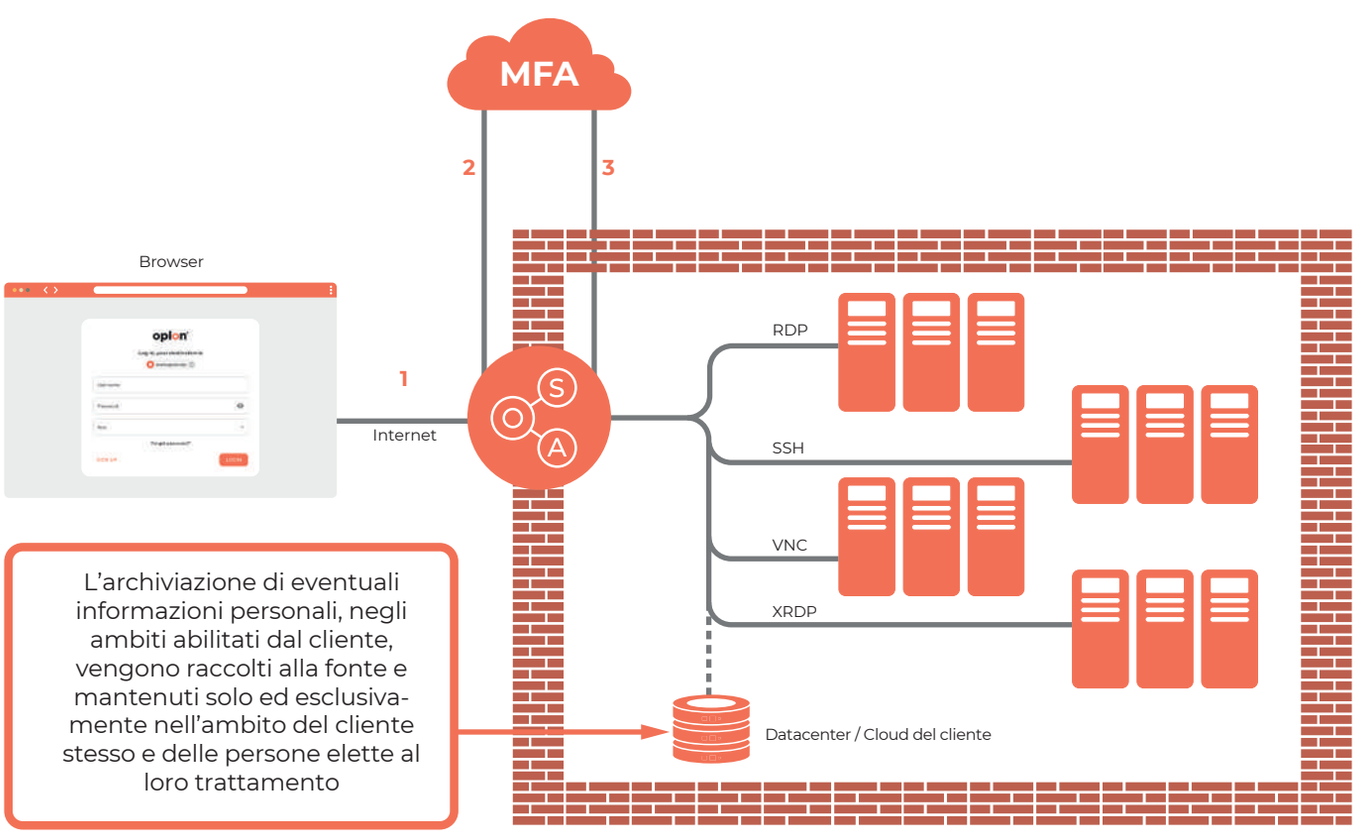
Con Oplon Secure Access e un investimento sicuramente inferiore al 4% del fatturato è possibile mitigare al massimo questa eventualità. Oplon Secure Access attraverso la sua politica di memorizzazione dei dati e una corretta elezione delle persone che possono accedere ai dati raccolti da parte del cliente, allontana e minimizza questa eventualità.

10. Consenso

Il consenso per il trattamento dei dati deve essere libero, informato, specifico e inequivocabile.
Gli utenti devono poter ritirare il consenso in qualsiasi momento.

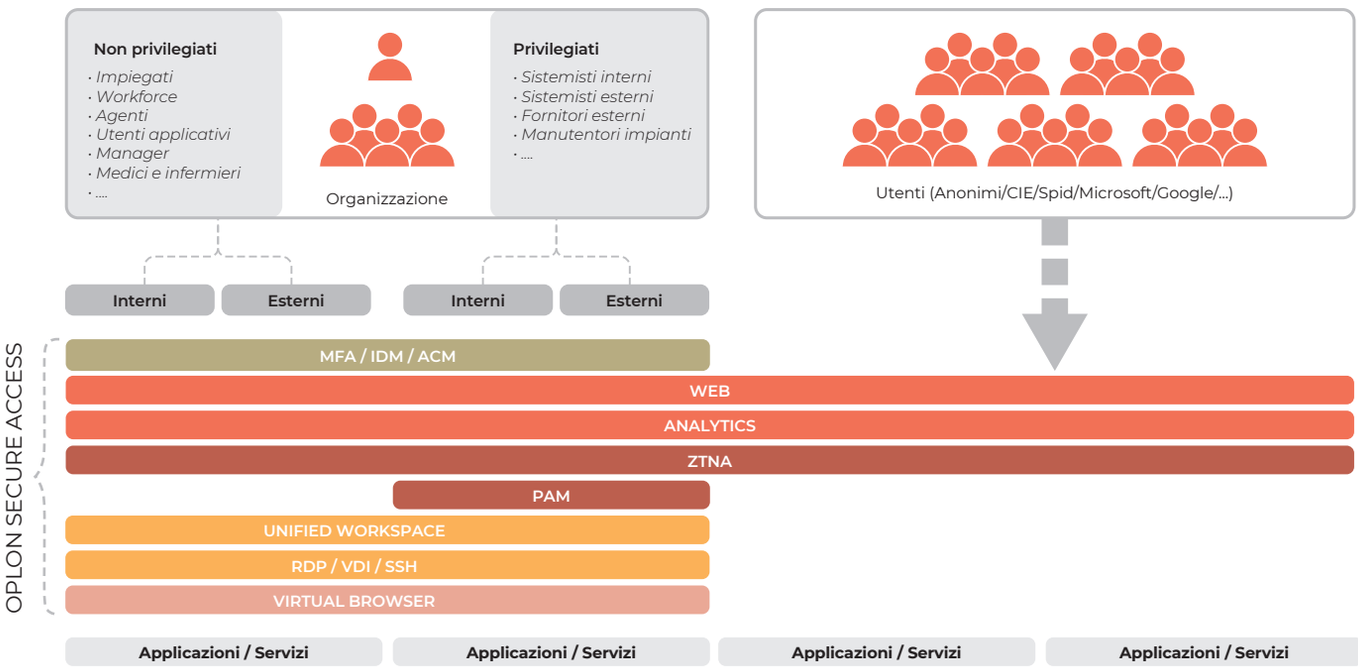
Nei casi in cui è necessario raccogliere dati che possono essere anche personali, è possibile produrre all'utente ciò che viene raccolto qualitativamente ed anche selettivamente.
Se l'utente non accettasse queste condizioni, è possibile eliminare in maniera definitiva tutti i suoi dati e disabilitare all'istante l'utente che ne facesse richiesta.

Oplon Secure Access: Architettura raccolta dati



Classificazione utenti e funzionalità

Gli utenti e quindi le loro attività, possono essere classificati nei seguenti gruppi e contesti, a seconda del tipo di attività o servizio devono avere un trattamento diversificato. Il seguente schema sintetizza le funzionalità utilizzate della piattaforma Oplon Secure Access e quindi il livello di logging delle informazioni riguardanti gli utenti:



OSA Layers	Description
MFA / IDM / ACM	Identificazione e autorizzazione utenti
WEB	Https reverse proxy
ANALYTICS	Sistema di logging centralizzato delle attività degli utenti
ZTNA	Sistema per erogare i servizi specifici agli utenti che hanno ricevuto l'autorizzazione da parte dell'organizzazione
PAM	Sistema di logging e limitazioni di accesso temporali per gli utenti che hanno accessi a servizi con privilegi molto alti e su infrastrutture critiche
UNIFIED WORKSPACE	Sistema di presentazione di un desktop virtuale con la lista dei servizi a cui l'utente è stato autorizzato ad accedere
RDP / VDI / SSH	Servizi tipicamente non Web che erogati con Oplon Secure Access tramite browser
VIRTUAL BROWSER	Servizi http/s interni erogati tramite browser che sono attivati all'interno dell'infrastruttura su piattaforme Windows o Linux ed erogati tramite una visualizzazione remota sempre tramite Browser. È una opzione diversa al sistema Reverse Proxy di erogare servizi web

Nota sull'utilizzo delle VPN e privacy

L'utilizzo di Oplon Secure Access e l'eliminazione delle VPN, permette agli utenti di non condividere, anche accidentalmente, informazioni private contenute nei propri device. Questo aspetto di non condividere informazioni private è molto spesso trascurato. Oplon Secure Access garantisce agli utenti, che non sono dei tecnici informatici, di non condividere le informazioni private dei propri personal device senza dover prendere precauzioni che dovrebbero presupporre delle conoscenze tecniche non dovute.

Oplon Secure Access è l'unico sistema oggi sul mercato che garantisce la privacy degli operatori anche se utilizzano il proprio laptop o personal computer.