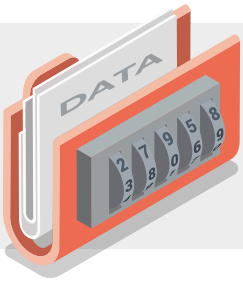
oplon®
SECURE ACCESS
GDPR compliance

Die Datenschutz-Grundverordnung (DSGVO) ist eine europäische Gesetzgebung, die am 25. Mai 2018 in Kraft getreten ist und den Schutz personenbezogener Daten von Bürgern der Europäischen Union (EU) regelt. Im Folgenden finden Sie eine kurze Beschreibung der wichtigsten Punkte der GDPR, gefolgt von einer Erläuterung der einzelnen Punkte der Oplon Secure Access-Konformität.

1. Umfang der Anwendung

Die Datenschutz-Grundverordnung gilt für alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, unabhängig vom Standort des Unternehmens.



Mit Oplon Secure Access werden persönliche Daten nur von dem Kunden, der sie nutzt, gespeichert und verwaltet und nirgendwo anders gespeichert.
Alle erfassten Daten werden in einer speziellen Datenbank und in einem klar definierten Strom von Videodarstellungen aufgezeichnet, die nur in bestimmten Fällen aktiviert werden können.

Grundprinzipien

TRANSPARENZ, FAIRNESS UND RECHTMÄSSIGKEIT DER DATENVERARBEITUNG

Wenn Daten, die personenbezogen sein könnten, aus Sicherheitsgründen (PAM) erfasst werden müssen, weist das System die Betreiber darauf hin, dass die Aktionen aufgezeichnet werden. In Fällen, in denen das Gesetz die Verarbeitung personenbezogener Daten nicht zulässt, zeichnet Oplon Secure Access diese Vorgänge nicht auf.

ZWECKBINDUNG

Daten dürfen nur für spezifische, ausdrückliche und rechtmäßige Zwecke erhoben werden.

Mit Oplon Secure Access werden persönliche Daten nur von dem Kunden, der sie nutzt, gespeichert und verwaltet und nirgendwo anders gespeichert.
Alle erfassten Daten werden in einer speziellen Datenbank und in einem klar definierten Strom von Videodarstellungen aufgezeichnet, die nur in bestimmten Fällen aktiviert werden können.
Es liegt daher in der alleinigen Verantwortung des Kunden, ein Tracking zu aktivieren, das nur in bestimmten Fällen personenbezogene Daten erfassen kann (z. B. PAM).

DATENSPARSAMKEIT

Die Verarbeitung muss sich auf die Daten beschränken, die für ihren Zweck unbedingt erforderlich sind.

Mit Oplon Secure Access ist es möglich, Tracking-Funktionen je nach Bedarf zu aktivieren und zu deaktivieren. Ihre Nutzbarkeit ist auf die Anzahl der Personen beschränkt, denen der Kunde von Oplon Secure Access die Möglichkeit gibt, sie zu nutzen. Da es an anderen Stellen keine Tracking-Daten gibt, sind die Daten ausschließlich für die zuständigen Personen verfügbar.

GENAUIGKEIT DER DATEN

Die Daten müssen korrekt sein und, falls erforderlich, aktualisiert werden.

Bei Bedarf und nach Freigabe durch den Kunden werden die Daten auf dem Weg durch die vom Kunden installierten Oplon Secure Access Virtual Appliances gesammelt und dann an der Quelle abgerufen. Nur vom Kunden autorisierte Personen können diese Daten einsehen und sie können daher nicht von anderen Personen geändert werden, da sie nur für die vom Kunden

ERHALTUNGSSATZUNG

Daten sollten nur so lange gespeichert werden, wie es für die Erfüllung des Zwecks erforderlich ist.

Mit Oplon Secure Access ist es auch möglich, gesammelte Daten zu löschen, indem Zeitfenster für ihre Aufbewahrung angegeben werden. Die Löschvorgänge sind einstellbar und erfolgen automatisch.
Die Zeitlichkeit der Daten ist wichtig, um einerseits das automatische Vergessen zu bewahren und andererseits dem Kunden ein Zeitfenster zu garantieren, um die Daten in den zulässigen und sammlungsfähigen Bereichen auswerten zu können.

3. Rechte der Betroffenen Parteien

Die Datenschutz-Grundverordnung gewährt den EU-Bürgern eine Reihe von Rechten, darunter das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit.

Alle Daten, die im Rahmen des Zwecks der Dienstleistung erhoben werden, werden in Dateien gespeichert, zu denen nur der Kunde Zugang hat.
Die Daten werden in einer relationalen Datenbank und, sofern möglich, in Form von Videomaterial gesammelt. Da es sich bei den erhobenen Daten um personenbezogene Daten handelt, die im Rahmen des Zwecks des betreffenden Dienstes ausschließlich vom Kunden und von den Personen aufbewahrt werden, die der Kunde für die Bearbeitung dieser Daten ausgewählt hat, gibt es keine Möglichkeit für Dritte, die Daten zu exfiltrieren.

4. Verantwortung und Rechenschaftspflicht

Die Unternehmen sind für die Einhaltung der DSGVO verantwortlich und müssen dies durch die Dokumentation und Aufzeichnung von Datenverarbeitungsaktivitäten nachweisen.

Oplon Secure Access zentralisiert alle Daten, die personenbezogene Informationen enthalten können, in zwei "Containern": die relationale Datenbank und alle Videoaufzeichnungen von Aktivitäten, die auf Fenstersystemen durchgeführt werden. Durch die Reduzierung der gesammelten personenbezogenen Daten auf diese beiden Container kann der Kunde die Zugriffsverfahren auf diese Daten aktivieren und die für die Verarbeitung erforderliche Dokumentation erstellen.

5. Ernennung des Datenschutzbeauftragten (DSB)

Einige Organisationen müssen einen behördlichen Datenschutzbeauftragten, einen unabhängigen Datenschutzexperten, bestellen, der die Einhaltung der Vorschriften überwacht.

Oplon Secure Access erleichtert Organisationen, die einen Datenschutzbeauftragten ernennen müssen, da alle personenbezogenen Daten, die im Rahmen spezifischer und ausdrücklich aktivierter Dienste erfasst werden, durch zwei Container, die relationale Datenbank und die Videos der Fenstergrafiksitzung, abgegrenzt werden. Auf diese Weise können die erfassten Daten jederzeit geschützt und überwacht werden. This way, the collected data can be protected and constantly monitored.

6. Benachrichtigung über eine Datenschutzverletzung

Unternehmen sind verpflichtet, die zuständigen Behörden über Datenschutzverletzungen innerhalb von 24 Stunden nach deren Auftreten zu benachrichtigen, es sei denn, es ist unwahrscheinlich, dass die Verletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.

Oplon Secure Access schränkt die Möglichkeit der Datenexfiltration ein, da sich die Daten nicht im Besitz einer dritten Partei befinden.
Sollte dies der Fall sein, ist es möglich, die zuwiderhandelnden Parteien sofort zu identifizieren und die Behörden innerhalb eines sehr kurzen Zeitrahmens und weit unter der gesetzlich vorgeschriebenen Frist von 72 Stunden zu benachrichtigen.

7. Internationale Datenübertragung

Die Übermittlung von Daten außerhalb der EU unterliegt Beschränkungen, und die Unternehmen müssen geeignete Sicherheitsmaßnahmen ergreifen.

Oplon Secure Access sammelt alle Daten für bestimmte, vom Kunden freigegebene Zwecke, nur und ausschließlich in den Archiven des Kunden, der als einziger Zugang hat, und an Orten, die im Rahmen seiner Dienstleistungen liegen.

8. Datenschutz-Folgenabschätzungen

In bestimmten Fällen müssen Organisationen eine Datenschutz-Folgenabschätzung durchführen, um die mit der Verarbeitung personenbezogener Daten verbundenen Risiken zu bewerten und abzumildern.

Die Datenerfassungsarchitektur von Oplon Secure Access, die sich ausschließlich im Besitz des Kunden befindet und von diesem verarbeitet wird, erleichtert die Durchführung von Datenschutz-Folgenabschätzungen erheblich.
Es werden keine personenbezogenen Daten außerhalb der Räumlichkeiten des Kunden und nur in zwei Archiven, relationalen Datenbanken und ggf. Videoaufzeichnungen von Fenstersitzungen gespeichert. Zusammen mit den internen Funktionen zur Auswahl der Personen, die Zugang zu diesen Daten haben, erleichtert dies die Datenschutzfolgenabschätzung.

9. Sanktionen

Die Aufsichtsbehörden können erhebliche Strafen für Verstöße gegen die DSGVO verhängen, darunter Geldbußen von bis zu 4 Prozent des weltweiten Jahresumsatzes.

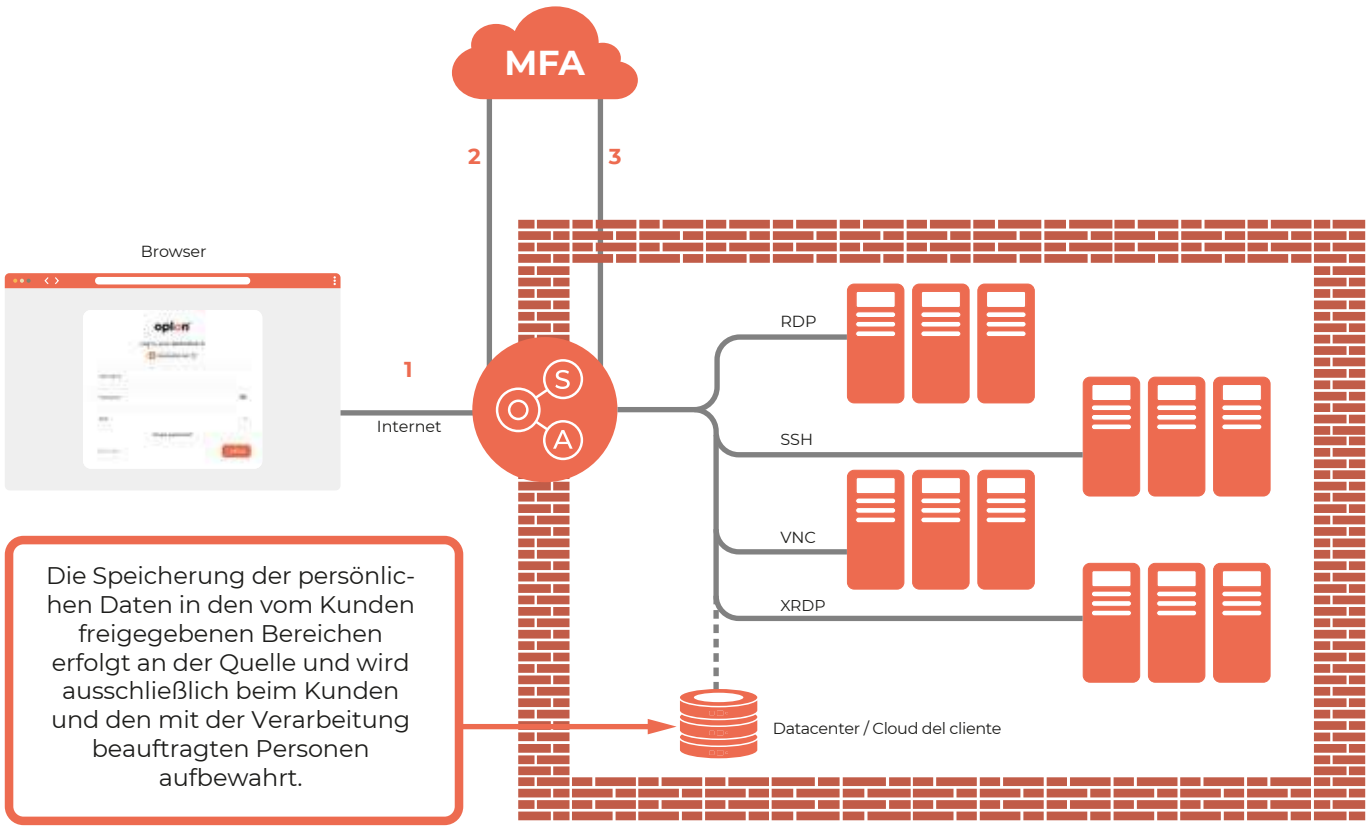
Mit Oplon Secure Access und einer Investition von sicherlich weniger als 4 % des Umsatzes kann diese Eventualität maximal gemildert werden. Oplon Secure Access vermeidet und minimiert diesen Fall durch seine Datenspeicherungspolitik und eine angemessene Auswahl der Personen, die auf die vom Kunden gesammelten Daten zugreifen können.

10. Zustimmung

Die Einwilligung in die Datenverarbeitung muss frei, in Kenntnis der Sachlage, ausdrücklich und unmissverständlich sein.
Die Nutzer müssen die Möglichkeit haben, ihre Zustimmung jederzeit zu widerrufen.

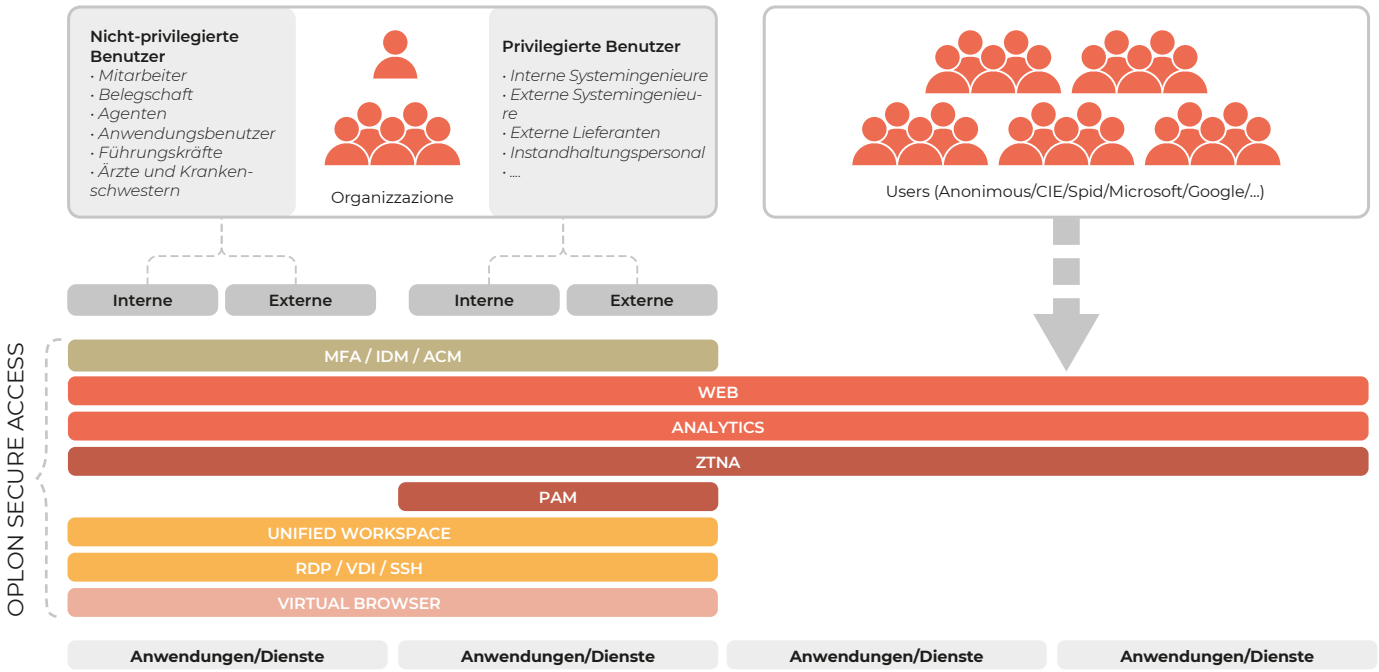
In Fällen, in denen es notwendig ist, Daten zu erheben, die auch personenbezogen sein können, ist es möglich, dem Nutzer die erhobenen Daten qualitativ und auch selektiv zu präsentieren.
Wenn der Nutzer mit diesen Bedingungen nicht einverstanden ist, ist es möglich, alle seine Daten dauerhaft zu löschen und den Nutzer, der dies beantragt, sofort zu sperren.

Oplon Secure Access: Architektur der Datenerhebung



Benutzerklassifizierung und -funktionalität

Die Nutzer und damit ihre Aktivitäten können in folgende Gruppen und Kontexte eingeteilt werden, die je nach Art der Aktivität oder Dienstleistung Dienstes unterschiedlich behandelt werden müssen. Das folgende Diagramm fasst die Funktionalitäten zusammen, die von der Oplon Secure Access-Plattform genutzten Funktionalitäten und damit auch den Grad der Protokollierung von Benutzerinformationen zusammen:



OSA Layers	BESCHREIBUNG
MFA / IDM / ACM	Benutzeridentifizierung und -berechtigung
WEB	Https reverse proxy
ANALYTICS	Zentralisiertes System zur Protokollierung von Benutzeraktivitäten
ZTNA	System zur Bereitstellung spezifischer Dienste für Nutzer, die von der Organisation eine Genehmigung erhalten haben
PAM	rotokollierungssystem und zeitliche Zugangsbeschränkungen für Nutzer mit Zugang zu Diensten mit sehr hohen Privilegien und zu kritischen Infrastrukture
UNIFIED WORKSPACE	System, das einen virtuellen Desktop mit einer Liste von Diensten präsentiert, auf die der Benutzer Zugriff hat
RDP / VDI / SSH	Typische Nicht-Web-Dienste, die mit Oplon Secure Access über den Browser bereitgestellt werden
VIRTUAL BROWSER	Interne, über einen Browser bereitgestellte http/s-Dienste, die innerhalb der Infrastruktur auf Windows- oder Linux-Plattformen aktiviert und über einen entfernten Bildschirm, wiederum über einen Browser, bereitgestellt werden. Es ist eine andere Option als das Reverse-Proxy-System zur Bereitstellung von Webdiensten

Hinweis zur Verwendung von VPNs und zum Datenschutz

Die Verwendung von Oplon Secure Access und die Eliminierung von VPNs ermöglicht es den Nutzern, private Informationen auf ihren Geräten nicht weiterzugeben, auch nicht versehentlich. Dieser Aspekt wird sehr oft übersehen. Oplon Secure Access stellt sicher, dass Benutzer, die keine Computertechniker sind, keine privaten Informationen auf ihren persönlichen Geräten weitergeben, ohne Vorsichtsmaßnahmen ergreifen zu müssen, die unangemessene technische Kenntnisse erfordern würden.

Oplon Secure Access ist das einzige System auf dem Markt, das die Privatsphäre der Bediener garantiert, auch wenn sie ihren eigenen Laptop oder persönlichen Computer benutzen.