

Nutzungsbedingungen und Datenschutzrichtlinie – ASEM Pro

Mitarbeitende und beruflich befugte Personen

Letzte Aktualisierung : 2026-10-19

Vertragsversion : Im Ausgangsdokument nicht angegeben

[Vollständiges Dokument online](#)

Informative Übersetzung. Der französische Text ist das Referenzdokument; die rechtliche Gleichwertigkeit dieser Übersetzung muss noch geprüft werden.

1 Gegenstand und Zugang zur Anwendung

ASEM Pro ist eine private berufliche Anwendung, die Mitarbeitenden und ausdrücklich von ASEM befugten Personen (nachstehend „Unternehmen“) zur Verfügung gestellt wird.

Ihre Nutzung ist strikt auf die Ausübung der vom Unternehmen genehmigten beruflichen Tätigkeiten beschränkt. Die zugänglichen Funktionen unterscheiden sich je nach Aufgaben, Verantwortlichkeiten und Berechtigungen der jeweiligen Nutzerin bzw. des jeweiligen Nutzers.

Das Unternehmen behält sich das Recht vor, berufliche Zugänge zu verwalten, zu ändern, einzuschränken, auszusetzen oder zu widerrufen, insbesondere aus organisatorischen, vertraglichen oder sicherheitsbezogenen Gründen und im Einklang mit den anwendbaren Rechtsvorschriften.

2 Eigentum an Konten und beruflichen Ressourcen

ASEM-Pro-Konten werden unter der Verantwortung des Unternehmens eingerichtet und verwaltet. Sie stellen berufliche Zugangsmittel dar, die den Nutzerinnen und Nutzern zur Verfügung gestellt werden, und keine frei übertragbaren persönlichen Konten.

Berechtigungen, Zugänge, interne Ressourcen, berufliche Dokumente, Geschäftsinformationen und dem Unternehmen gehörende Daten bleiben unter dessen Kontrolle.

Jede Nutzerin und jeder Nutzer ist für die Vertraulichkeit der Zugangsdaten und für die über das eigene Konto vorgenommenen Vorgänge verantwortlich.

Die gemeinsame Nutzung von Konten, die Weitergabe von Zugangsdaten und jede Nutzung durch eine nicht befugte Person sind untersagt.

Diese Bestimmung beeinträchtigt nicht die Rechte, die Personen an ihren personenbezogenen Daten behalten.

3 Vertraulichkeit und Schutz der Interessen des Unternehmens

Sämtliche in ASEM Pro zugänglichen beruflichen Informationen unterliegen einer strengen Vertraulichkeitspflicht.

Sofern keine ausdrückliche Genehmigung oder gesetzliche Verpflichtung vorliegt, ist es untersagt:

- Interne Daten zu persönlichen, kommerziellen oder wettbewerbsbezogenen Zwecken zu kopieren, zu extrahieren, offenzulegen, zu übertragen oder zu verwerten.
- Dokumente, Kundeninformationen, interne Verfahren oder vertrauliche berufliche Kommunikation an Dritte weiterzugeben.
- Nicht genehmigte Aufnahmen, Aufzeichnungen oder Exporte geschützter Inhalte anzufertigen.
- Zugriffskontrollen zu umgehen, eine Identität anzunehmen oder auf Informationen außerhalb der eigenen Berechtigungen zuzugreifen.
- Informationen oder Systeme des Unternehmens zu verändern, zu zerstören, zweckzuentfremden oder missbräuchlich zu nutzen.

Diese Verpflichtungen gelten nach dem Ende der beruflichen Berechtigung im Rahmen der vertraglichen Verpflichtungen und des Gesetzes weiterhin.

Jeder Verstoß kann eine sofortige Aussetzung der Zugänge, anwendbare disziplinarische oder vertragliche Maßnahmen sowie zivil- oder strafrechtliche Schritte nach sich ziehen, wenn die Umstände dies rechtfertigen.

Das Unternehmen behält sich das Recht vor, seine berechtigten Interessen zu schützen und bei betrügerischer Nutzung, Offenlegung oder Zweckentfremdung von Daten die zuständigen Behörden einzuschalten.

4 Sicherheit und Verschlüsselung der Daten

ASEM Pro setzt technische und organisatorische Maßnahmen zum Schutz beruflicher Informationen um.

Die Kommunikation mit den Diensten der Anwendung nutzt sichere Protokolle und Verschlüsselungsmechanismen. Gespeicherte Daten werden durch Maßnahmen geschützt, die ihrer Art angemessen sind, insbesondere durch Zugriffskontrollen, Authentifizierungsmechanismen und anwendbare Sicherheitsmaßnahmen.

Der Zugang zu Informationen wird entsprechend den beruflichen Berechtigungen beschränkt.

Das Unternehmen wendet Maßnahmen an, die unbefugten Zugriff, Veränderungen, Datenverluste und missbräuchliche Nutzungen verhindern sollen. Kein IT-System kann jedoch absolute Sicherheit garantieren.

Jeder vermutete Sicherheitsvorfall ist dem Unternehmen unverzüglich zu melden.

5 Standortbestimmung und Achtung der Privatsphäre

ASEM Pro dient nicht der dauerhaften Überwachung der Bewegungen der Mitarbeitenden.

Die Anwendung führt keine kontinuierliche GPS-Ortung durch, die der Überwachung von Beschäftigten außerhalb ihrer beruflichen Aufgaben dient.

Die Standortbestimmung kann im Rahmen genehmigter beruflicher Tätigkeiten punktuell angefordert werden, insbesondere wenn ein Vorgang die Bestätigung einer Position oder die Nutzung einer Kartenfunktion erfordert.

Karten- und Routenfunktionen, insbesondere solche, die auf Google Maps zurückgreifen können, sind den befugten beruflichen Rollen vorbehalten.

Daher haben nicht alle Nutzerinnen und Nutzer Zugang zu denselben Standortbestimmungsfunktionen.

Die Nutzung des Standorts hängt von den erforderlichen Berechtigungen, dem funktionalen Kontext und den auf dem Gerät erteilten Genehmigungen ab.

Das Unternehmen verpflichtet sich, die Verarbeitung von Standortdaten auf die angegebenen beruflichen Zwecke zu beschränken, ohne eine kontinuierliche Erhebung vorzunehmen, die der Rekonstruktion privater Bewegungen der Mitarbeitenden dient.

6 Nachrichtenübermittlung und berufliche Kommunikation

ASEM Pro ermöglicht je nach Berechtigungen den beruflichen Austausch sowie die Weitergabe von Informationen oder Dateien, die für die genehmigten Tätigkeiten erforderlich sind.

Die Kommunikation kann Nachrichten, Dokumente, Fotografien, multimediale Inhalte oder andere berufliche Elemente umfassen.

Diese Informationen werden verarbeitet, um ihre Übermittlung und Einsichtnahme, die Koordinierung der Tätigkeiten und die Aufrechterhaltung des Dienstes zu ermöglichen.

Die in dieser beruflichen Umgebung erfolgende Kommunikation muss die Vertraulichkeits- und Sicherheitsverpflichtungen sowie die internen Regeln des Unternehmens einhalten.

Der Zugang zu Inhalten und Verlaufsdaten unterliegt den anwendbaren Berechtigungen. Ihre Einsichtnahme oder Speicherung durch das Unternehmen muss einem legitimen beruflichen Zweck dienen und die Rechte der betroffenen Personen achten.

Nutzerinnen und Nutzer dürfen keine personenbezogenen, medizinischen oder vertraulichen Daten übermitteln, die nicht mit den genehmigten Erfordernissen ihrer Tätigkeit zusammenhängen.

7 Personenbezogene Daten und Berechtigungen

Zur Sicherstellung des Dienstbetriebs kann ASEM Pro je nach genutzten Funktionen und erteilten Berechtigungen Folgendes verarbeiten:

- Identifikations- und berufliche Profildaten.
- Informationen über die durchgeführten Tätigkeiten und Vorgänge.
- Freiwillig im beruflichen Rahmen übermittelte Inhalte und Dateien.
- Technische Informationen, die für die Authentifizierung, die Sicherheit und den Betrieb erforderlich sind.
- Punktuelle Standortdaten, wenn ihre Nutzung erforderlich und genehmigt ist.
- Für die Kommunikation und Benachrichtigungen erforderliche Daten.

Der Zugriff auf die Kamera, das Mikrofon, Dateien oder den Standort erfolgt in den betreffenden funktionalen Kontexten und gemäß den erforderlichen Berechtigungen.

Bestimmte Funktionen können technische Dienstleister nutzen, insbesondere für Hosting, Benachrichtigungen, Kommunikation oder Kartendienste. Diesen dürfen nur die für diese Dienste erforderlichen Informationen unter den für ihre Nutzung geltenden Bedingungen übermittelt werden.

Die Daten sind nicht zum Verkauf an Werbetreibende bestimmt.

8 Speicherung, Rechte und Löschung

Die Informationen werden so lange gespeichert, wie dies für die betreffenden beruflichen Tätigkeiten, die Sicherheit der Systeme, die Nachvollziehbarkeit der Vorgänge und die Einhaltung der anwendbaren gesetzlichen oder vertraglichen Verpflichtungen erforderlich ist.

Sobald ihre Speicherung nicht mehr gerechtfertigt ist, werden geeignete Verfahren zur Löschung oder Anonymisierung durchgeführt.

Nutzerinnen und Nutzer können ihre anwendbaren Rechte auf Auskunft, Berichtigung, Widerspruch und Löschung ihrer personenbezogenen Daten ausüben.

Das Ende einer beruflichen Berechtigung führt zum Widerruf der betreffenden Zugänge. Dies bedeutet nicht zwangsläufig die sofortige Löschung sämtlicher beruflicher Dokumente oder Verlaufsdaten, die das Unternehmen berechtigterweise aufbewahren muss.

Anfragen zu personenbezogenen Daten oder zur Löschung eines Kontos können gerichtet werden an:

Die Anfragen werden im Einklang mit den anwendbaren Rechtsvorschriften geprüft, insbesondere mit dem algerischen Gesetz Nr. 18-07 zum Schutz personenbezogener Daten in seiner jeweils geänderten und ergänzten Fassung.

9 Verantwortung, Aussetzung und Weiterentwicklung des Dienstes

Jede Nutzerin und jeder Nutzer verpflichtet sich, ASEM Pro ausschließlich im Rahmen der eigenen beruflichen Berechtigungen und der anwendbaren Anweisungen zu verwenden.

Das Unternehmen kann einen Zugang im Fall des Ausscheidens einer Mitarbeiterin oder eines Mitarbeiters, eines Funktionswechsels, eines Sicherheitsrisikos oder eines Verstoßes gegen diese Bedingungen aussetzen oder entziehen.

Die Funktionen und Nutzungsmodalitäten können aus technischen, organisatorischen, sicherheitsbezogenen oder regulatorischen Gründen weiterentwickelt werden.

Wesentliche Änderungen der Bedingungen oder der Datenverarbeitungen werden gemäß den anwendbaren Rechtsvorschriften mit den erforderlichen Informationen bekannt gegeben.

Diese Bestimmungen gelten unbeschadet der zwingenden Rechte der Nutzerinnen und Nutzer und der gesetzlichen Verpflichtungen des Unternehmens.

10 Annahme und Kontakt

Die Nutzung von ASEM Pro ist befugten Personen vorbehalten und setzt die Einhaltung dieser Bedingungen sowie der anwendbaren beruflichen und vertraulichkeitsbezogenen Regeln voraus.

Berechtigungen in Bezug auf personenbezogene Daten und Gerätefunktionen werden, sofern dies gesetzlich erforderlich ist, getrennt eingeholt.

Bei Fragen zu den Nutzungsbedingungen, zum Datenschutz oder zur Sicherheit:

ASEM — direction@asem-medical.com
Offizielle Website: <https://asem-medical.com>

ASEM Pro — Sichere berufliche Umgebung, kontrollierter Zugang und Vertraulichkeit der Informationen.