Protelion SMC

Datenschutzrichtlinie

In diesem Abschnitt beschreiben wir die Maßnahmen zum Schutz personenbezogener Daten sowie Maßnahmen zum Schutz der Rechte betroffener Personen, die in der Software Protelion SMC umgesetzt sind, die folgende Module enthält:

- Protelion SMC VPN
- Protelion SMC Rollout
- Protelion SMC Monitoring
- Protelion SMC Policies
- Protelion SMC Enterprise Messenger Book

Personenbezogene Daten sind alle Daten hinsichtlich einer natürlichen Person, die zur direkten oder indirekten Identifizierung verwendet werden können.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Identität oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Protelion GmbH schützt die Grundrechte und Grundfreiheiten natürlicher Personen hinsichtlich ihrer personenbezogenen Daten. Zum Schutz der Rechte betroffener Personen sind in Protelion SMC die Maßnahmen vorgesehen, die für die Sicherheit personenbezogener Daten sorgen, sowie die Funktionen, die dem Schutz der Rechte betroffener Personen mitwirken.

Grundsätze für die Verarbeitung personenbezogener Daten

Bereits bei der Entwicklung der Produkte haben wir die nachfolgend genannten Maßnahmen getroffen, die dafür ausgelegt sind, die Grundsätze für die Verarbeitung personenbezogener Daten wirksam umzusetzen:

- **Grundsatz der Transparenz, Verarbeitung nach Treu und Glauben sowie Rechtmäßigkeit bei der Verarbeitung und Verwendung personenbezogener Daten.**

  Protelion GmbH stellt ausführliche Informationen über die Verarbeitung der Daten, die als personenbezogen gelten können, bereit. Dabei wird das Gleichgewicht zwischen den Interessen betroffener Person und des Produktinhabers berücksichtigt.

- **Grundsatz der Zweckbindung**

  Einschränkung der Verarbeitung personenbezogener Daten auf festgelegte, eindeutige und legitime Zwecke. Die Zwecke der Verarbeitung personenbezogener Daten werden eindeutig festgelegt (s. den Abschnitt „Wofür werden personenbezogene Daten verwendet?“) und die Verarbeitung der Daten durch die Produkte bleibt im Rahmen des für die Erreichung dieser Zwecke notwendigen Umfangs und erfolgt nicht für andere Zwecke.

- **Grundsatz der Datenminimierung**

  Die durch die Produkte erhobenen und gespeicherten Daten werden auf ein angemessenes Niveau beschränkt und überschreiten nicht das für die Zwecke der Verarbeitung notwendige Maß.

- **Grundsatz der Richtigkeit**

  Die Produkte von Protelion GmbH bieten eine Möglichkeit, bei Bedarf personenbezogene Daten zu aktualisieren, zu berichtigen oder zu löschen, soweit dies das angemessene Gleichgewicht der Interessen der betroffenen Person und des Produktinhabers nicht stört.

- **Grundsatz der Speicherbegrenzung**

  In den Produkten von Protelion GmbH ist ein Verfahren vorgesehen, das die rechtzeitige und regelmäßige Löschung von personenbezogenen Daten unterstützt, um eine unkontrollierbare Speicherung personenbezogener Daten zu verhindern.

- **Grundsatz der Integrität und Vertraulichkeit**

  Um eine angemessene Sicherheit personenbezogener Daten in den Produkten zu gewährleisten, werden Verfahren zur Entwicklung sicherer Software verwendet, die verschiedene Aspekte vom Design bis zum Betrieb und Nutzung des Produkts berücksichtigen um vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung von personenbezogener Daten zu schützen.

Was gilt als Verletzung des Schutzes personenbezogener Daten?

Eine Verletzung des Schutzes personenbezogener Daten ist „eine Verletzung der Sicherheit die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Im Falle einer Verletzung des Schutzes personenbezogener Daten ist die für die Datenverarbeitung verantwortliche Stelle verpflichtet,

- Die Verletzung unverzüglich der zuständigen Aufsichtsbehörde zu melden, wenn die Verletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Die von der Verletzung der betroffenen Person unverzüglich von der Verletzung in Kenntnis zu setzen, wenn diese voraussichtlich ein hohes Risiko für deren persönliche Rechte und Freiheiten zur Folge hat.
- Jede Verletzung ist von der verantwortlichen Stelle unabhängig von etwaigen Meldepflichten zu dokumentieren einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten (Anzahl betroffener Personen, Anzahl und Kategorien betroffener Datensätze), Auswirkungen und ergriffener Maßnahmen.

Die Produkte von Protelion, wie z.B. Protelion TDA, Protelion NIDS, Protelion HIDS, verfügen bereits über Lösungen zur Unterstützung der Rechenschaftspflichten der verantwortlichen Stellen und zur Bewertung der Risiken und zur Erkennung von Verletzungen des Datenschutzes.

Welche personenbezogenen Daten werden von Protelion SMC verarbeitet?

Hinweis. Protelion SMC verarbeitet keine besonders sensiblen personenbezogenen Daten (sogenannte „besondere Kategorien personenbezogener Daten“), wie z.B. rassischer und ethnischer Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

In Protelion SMC werden personenbezogene Daten für zwei Benutzertypen bearbeitet: Benutzer von Protelion Server-Produkte und Benutzer von Protelion Endpunkt-Produkte, wie z.B. Protelion VPN und Protelion Enterprise Messenger.

Daten eines Benutzers von Protelion SMC

- Benutzername: Daten, die den Benutzer in der Benutzeroberfläche von Protelion SMC identifizieren.
- E-Mail-Adresse: falls Protelion SMC Monitoring angeschlossen ist, wird verwendet, um die Benutzer von Protelion SMC über Netzwerkprobleme im Protelion Netzwerk zu informieren.
- Beschreibung des Benutzers: zusätzliche Benutzerdaten, die die Verwendung der Benutzerliste erleichtern.
- Benutzerrolle: Daten über die Berechtigungen des Benutzers von Protelion SMC, die für die Kontrolle des Zugriffs auf die Funktionen erforderlich sind. Sehen Sie den Abschnitt „Abgrenzung von Rechten auf Basis von Administratorrollen“ in der Protelion SMC Dokumentation.
- Organisationsname: Informationen darüber, ob der Protelion SMC-Benutzer zu einer Organisation gehört. Erforderlich für die Kontrolle des Datenzugriffs innerhalb einer Organisation.
- Abteilung: Informationen darüber, ob der Benutzer zu einer Abteilung innerhalb der Organisation gehört. Erforderlich, um die Benutzer in logische Gruppen einzuteilen und den Zugriff innerhalb von Abteilungen zu kontrollieren.
- Login: Benutzername, der im Authentifizierungssystem von Protelion SMC verwendet wird.
- Benutzer-ID: interne eindeutige Benutzer-ID, die in der Oberfläche verwendet wird, um einen Benutzer eindeutig zu identifizieren, auch wenn sich der Benutzername ändert.

Daten eines Benutzers des Protelion Netzwerks

- Benutzername: Daten, die den Benutzer in der Benutzeroberfläche von Protelion SMC identifizieren. Wenn Protelion SMC Rollout angeschlossen ist, werden diese Informationen in Protelion SMC Rollout verwendet, um Einrichtungseinladungen und den Zugriff auf den Rollout-Dienst zu verwalten.
- Telefon und E-Mail-Adresse: Wenn Protelion SMC Rollout angeschlossen ist, werden diese Informationen in Protelion SMC Rollout verwendet, um die Einladungen zur Einrichtung der Protelion VPN-Software zu verwalten, Anmeldeinformationen und das Passwort für die VPN-Schlüsseldistribution zu übertragen.
- Beschreibung des Benutzers: zusätzliche Benutzerdaten, die die Verwendung der Benutzerliste erleichtern.
- Bild des Benutzers: falls das Adressbuchmodul Protelion SMC Enterprise Messenger Book angeschlossen ist, Informationen zur Identifizierung des Benutzers in der Benutzeroberfläche von Protelion SMC und Protelion Enterprise Messenger.
- Organisationsname und -ID: Informationen darüber, ob der Protelion SMC-Benutzer zu einer Organisation gehört. Erforderlich für die Kontrolle des Datenzugriffs innerhalb einer Organisation.
- Abteilung: Informationen darüber, ob der Benutzer zu einer Abteilung innerhalb der Organisation gehört. Erforderlich, um die Benutzer in logische Gruppen einzuteilen und den Zugriff innerhalb von Abteilungen zu kontrollieren.
- Interne Nummer: falls das Adressbuchmodul Protelion SMC Enterprise Messenger Book angeschlossen ist, virtuelle Nummer für private Anrufe über Protelion Enterprise Messenger.

- Login und Passwort: der Zugriff auf die VPN-Schlüsseldistribution erfordert eine Authentifizierung. Das Authentifizierungsverfahren unterstützt sowohl die Active Directory-Authentifizierung als auch Konten, die im Authentifizierungssystem selbst erstellt wurden. Beim Erstellen einer Einrichtungseinladung für einen Protelion Benutzer erstellt Protelion SMC Rollout ein Benutzerkonto auf der Seite des Protelion SMC-Authentifizierungsdienstes und liefert Login und Passwort in der Benutzereinladung per E-Mail oder SMS. Protelion SMC Rollout verarbeitet und speichert Protelion Benutzer-Login und Passwort in keiner Weise.
- Benutzer-ID: interne eindeutige Benutzer-ID, die verwendet wird, um einen Benutzer eindeutig zu identifizieren, auch wenn sich der Benutzername ändert.
- Verbindungen des Benutzers: in Protelion SMC werden im VPN-Modul die Verbindungen des Benutzers mit anderen Benutzern der Protelion Netzwerke oder mit Unternehmensressourcen, die die der Benutzer zum Arbeiten benötigt,verarbeitet.
- Benutzergruppe: Wenn Protelion SMC VPN angeschlossen ist, können Sie Protelion Netzwerkbenutzer in logische Gruppen einteilen, um die Verwaltung von Verbindungen zu erleichtern. Gruppennamen können auch personenbezogene Daten zur Identifizierung eines Benutzers enthalten.
- Zugriff des Benutzers auf die Schlüsseldistributionen: Wenn Protelion SMC Rollout angeschlossen ist, können Sie Informationen über die Zugriffsberechtigungen der Benutzer für die Schlüsseldistributionen auf den Benutzergeräten verwalten und verarbeiten. Bei der Authentifizierung des Benutzers im Benachrichtigungssystem Protelion SMC während der Bereitstellung des Protelion Endpunkts prüft Protelion SMC Rollout, ob der Benutzer über ausreichende Berechtigungen für den Zugriff auf die Schlüsseldistribution des Protelion Netzwerks verfügt.
- Ereignis-Logdatei: Enthält die Informationen über die Aktionen der Administratoren in den Funktionsmodulen sowie die Ereignisse von Protelion SMC.
- Nachrichten- und Anrufverlauf in Protelion Enterprise Messenger: der Protelion SMC Monitoring-Operator kann Logdateien aus Protelion Enterprise Messenger vom Gerät bekommen, die technische Daten über die App sowie Nachrichtenverlauf enthalten. Vom Gerät von Protelion Chat Server kann man den Anrifverlauf bekommen. Die Logdateien enthalten nur die Uhrzeit von Anrufen und Nachrichten sowie der Gerätename des Kontakts. Diese Logdateien helfen einem Support-Team bei der Fehlersuche im Protelion Enterprise Messenger. Der Inhalt von Anrufen und Nachrichten wird in keiner Weise gespeichert.
- Die Berechtigungsstufe des Benutzers in Protelion Enterprise Messenger definiert, falls das Adressbuchmodul Protelion SMC Enterprise Messenger Book angeschlossen ist, die Fähigkeit des Benutzers, einen anderen Mitarbeiter in Protelion Enterprise Messenger anzurufen oder ihm zu schreiben.
- Zusätzliche Parameter aus externer Datenquelle: falls das Adressbuchmodul Protelion SMC Enterprise Messenger Book angeschlossen ist, beliebige zusätzliche Informationen über den Benutzer oder seinen Arbeitsplatz. Beispiel: ausführliche Informationen über die Abteilung oder die Stelle, zusätzliche Kontaktangaben. Wird vom Benutzer der Protelion Produkte und dem Administrator von Protelion SMC zur einfachen Verwaltung des Unternehmensnetzwerks verwendet.

Daten eines Geräts des Protelion SMC-Benutzers

- Online-ID: zur korrekten Arbeit mit Protelion SMC und allen angeschlossenen Modulen über die Webschnittstelle. Wird nach dem Ende der Sitzung oder nach 15 Minuten Inaktivität des Benutzers gelöscht.
- Geräte-ID im SMC-Kern: zur Identifikation im Modul Protelion SMC Monitoring, zu dem die Monitoring-Daten gehören.
- Geräte-Token: zur Authentifizierung im Modul Protelion SMC Monitoring, zu dem die Monitoring-Daten gehören.

Daten eines Geräts des Protelion Netzwerkbenutzers

- Der Gerätename des Protelion Netzwerkbenutzers wird in den Benutzeroberflächen von Protelion SMC und angeschlossenen Modulen Protelion SMC Monitoring, Rollout, Policies und VPN angezeigt und für die Verwaltung ausgestellter Schlüsseldistributionen, Geräteüberwachung und Konfiguration von Verbindungen verwendet. Er wird in Protelion SMC beim Konfigurieren oder Erzeugen einer Schlüsseldistribution erstellt und kann einen Benutzernamen enthalten. Er wird auch in Protelion SMC gespeichert.
- Gerätetyp des Protelion Netzwerkbenutzers: Daten über das Betriebssystem des Geräts zur Konfiguration des Geräts in Protelion SMC und dessen Modulen. Er wird vom Administrator zur Verwaltung des privaten Protelion Unternehmensnetzwerks verwendet.
- Login des Benutzers, der den VPN-Dienst auf dem Gerät gestartet hat: Für einige Produkte kann Protelion SMC Monitoring Informationen über das Login des Benutzers sammeln, der den VPN-Dienst auf einem Gerät gestartet hat.
- Protelion ID des Protelion Netzwerkbenutzers: Wenn Protelion SMC VPN angeschlossen ist, verarbeitet es auch die Protelion ID des Geräts, die in der Produkt-GUI angezeigt wird. Die ProtelionID erleichtert die Verwaltung in Protelion SMC und ist für die Funktion von Protelion Netzwerken erforderlich.
- Schlüsseldistribution: wird in Protelion SMC manuell erstellt und kann auf der Festplatte des Protelion SMC Servers oder der Arbeitsstation des Protelion Netzwerkadministrators gespeichert werden. Die Schlüsseldistribution kann auch auf Anfrage vom Protelion VPN über Protelion SMC Rollout erstellt werden. In diesem Fall werden die Schlüsseldistributionen im Speicher von Protelion SMC Rollout gespeichert und sind durch eindeutige Passwörter geschützt, die nur den Eigentümern der Schlüsseldistributionen bekannt sind. Die Schlüsseldistribution enthält die folgenden personenbezogenen Daten:
  - Protelion Name des Geräts des Protelion Netzwerkbenutzers, der den Benutzernamen enthalten kann
  - Protelion ID eines Geräts des Protelion Netzwerkbenutzers
  - Protelion Name eines Benutzers des Protelion Netzwerks
  - Protelion ID eines Benutzers des Protelion Netzwerks
  - Liste der Protelion Benutzergeräte, die mit dem Gerät verbunden sind (enthält die Protelion Gerätenamen und Protelion Geräte-IDs)
  - Liste der Protelion Netzwerkbenutzer, die mit dem Benutzer verbunden sind (enthält die Protelion Benutzernamen und Protelion Benutzer-IDs)
- Passwort der Schlüsseldistribution: Die Schlüsseldistribution ist zur Erhöhung der Sicherheit passwortgeschützt. Das Passwort wird automatisch auf Anfrage des Administrators oder bei der Generierung des Schlüsselsatzes in Protelion SMC Rollout erzeugt. Anschließend wird es an Protelion SMC übergeben, um erzeugte Schlüsseldistribution zu schützen. Gleichzeitig wird das Passwort dem Benutzer per E-Mail oder SMS oder direkt an die Protelion VPN-Software des Benutzers übermittelt. Das Passwort wird irgendwo anders weder verarbeitet noch gespeichert.
- Daten zur Netzwerküberwachung mittels Protelion SMC Monitoring:
  - Protelion Name des Benutzergeräts
  - Protelion ID des Benutzergeräts
  - Protelion ID des Benutzers
  - Name des Benutzercomputers
  - Name des angemeldeten Benutzers des Betriebssystems

    - Betriebssystem-Aktivierungsschlüssel
    - IP-Adressen des Benutzergeräts
    - MAC-Adressen des Benutzergeräts
- Netzwerkaktivität auf dem Gerät: ein Protelion SMC Monitoring-Operator kann von einem Gerät mit installiertem Protelion VPN eine IP-Paket-Logdatei abrufen, die die Informationen über die Netzwerkaktivität auf dem Gerät enthält.
- Protelion VPN Logdateien: Wenn das Gerät, auf dem die Protelion VPN-Software installiert ist, zu Protelion SMC Monitoring hinzugefügt wird, kann ein Protelion SMC Monitoring-Operator die Protelion Logdateien des Geräts mit folgenden Daten erfassen:
    - Informationen zur Smartphone-Firmware und Einstellungen:
        - Smartphone-Modell
        - Prozessortyp
        - Mobilfunkanbieter
        - Firmware-Version
        - System-DNS-Server
        - Domänenname
        - Regionaleinstellungen
        - Zeitzone
        - Seriennummer
    - Informationen über die Netzwerkadapter des Telefons (Name, IP-Adresse, MAC-Adresse)
    - Liste installierter Apps
    - Liste laufender Vorgänge
    - Liste verbundener Protelion Geräte anderer Netzwerkbenutzer
- Zusätzliche Parameter aus externer Datenquelle: falls das Adressbuchmodul Protelion SMC Enterprise Messenger Book angeschlossen ist, beliebige Informationen über den Benutzer oder seinen Arbeitsplatz. Beispiel: ausführliche Informationen über die Abteilung oder die Stelle, zusätzliche Kontaktdaten. Wird vom Protelion SMC-Administrator zur einfachen Verwaltung des Unternehmensnetzwerks oder vom Benutzer zur Nutzung der Protelion Produkte verwendet.

Gerätedaten im Unternehmensnetzwerk

Protelion SMC Monitoring kann Geräte im Unternehmensnetzwerk finden, die keine Protelion Software besitzen und nicht in Protelion SMC enthalten sind. Es bearbeitet die IP- und MAC-Adressen der Geräte und sendet diese an den Protelion SMC Monitoring Server. Ermittelte Geräte können Sie zu Protelion SMC hinzufügen. Beim Hinzufügen der Geräte zu Protelion SMC werden die Informationen über diese Geräte zu Protelion SMC Monitoring automatisch hinzugefügt. Es werden folgende Informationen bearbeitet:

- Gerätename: Informationen, die das Gerät in Protelion SMC identifizieren.
- Gerätebeschreibung: alle zusätzlichen Informationen über das Gerät.
- Organisationsname: Informationen darüber, ob das Gerät zu einer Organisation gehört.
- Abteilung: Informationen darüber, ob das Gerät zu einer Abteilung innerhalb der Organisation gehört.

Daten über die Aktivität des Benutzers von Protelion SMC

Protelion SMC protokolliert alle Benutzeraktivitäten beim Konfigurieren von Protelion SMC, beim Verwalten des Protelion SMC Benutzerzugriffs, beim Erstellen von Protelion Benutzern und deren Geräten. Dies ist notwendig, um inkorrekte oder illegale Aktivitäten von Mitarbeitern zu erkennen, die schwerwiegende Auswirkungen auf die Organisation haben.

Protelion SMC VPN protokolliert alle Aktivitäten des Protelion SMC Benutzers in Protelion SMC VPN beim Konfigurieren von Protelion SMC VPN, beim Konfigurieren von Geräte- und Benutzerverbindungen und beim Erstellen von Benutzergruppen.

Protelion SMC Rollout protokolliert alle Aktivitäten des Protelion SMC Benutzers in Protelion SMC Rollout zum Konfigurieren von Protelion SMC Rollout, zum Verwalten des Zugriffs des Protelion Benutzers auf die Schlüsseldistributionen und zum Senden von Einladungen zur Bereitstellung von Schlüsseldistributionen.

Protelion SMC Monitoring protokolliert alle Aktivitäten eines Protelion SMC Benutzers in Protelion SMC Monitoring beim Konfigurieren der Überwachung und beim Abrufen von Logdateien aus den Protelion Benutzergeräten.

Protelion SMC Policies protokolliert alle Aktivitäten eines Protelion SMC Benutzers in Protelion SMC Policies, die mit zentraler Verwaltung von Richtlinien auf den Security-Gateways im Protelion Unternehmensnetzwerk verbunden sind.

Protelion SMC Enterprise Messenger Book protokolliert alle Aktivitäten eines Protelion SMC Benutzers in Protelion SMC Enterprise Messenger Book, die mit der Verwaltung des Adressbuchs von Protelion Enterprise Messenger Benutzern verbunden sind.

Aktivitätsdaten des Protelion Netzwerkbenutzers

Protelion SMC Rollout protokolliert die Benutzeranfragen auf die Schlüsseldistributionen. Protelion SMC Rollout speichert die protokollierten Ereignisse nicht und sendet sie an Protelion SMC.

Wofür werden personenbezogene Daten verwendet?

Beschreibung der Gründe, auf welche die personenbezogenen Daten verarbeitet werden	**Kategorien personenbezogener Daten**
Sicherer Datenaustausch zwischen den Benutzergeräten des Protelion Netzwerks	Daten eines Benutzers von Protelion SMC Daten eines Benutzers des Protelion Netzwerks Daten eines Geräts des Protelion Netzwerkbenutzers
Authentifizierung und Anmeldung des Protelion Netzwerkbenutzers	Daten eines Benutzers des Protelion Netzwerks
Primäre Bereitstellung der VPN-Schlüsseldistribution auf einem Host	Daten eines Benutzers des Protelion Netzwerks Daten eines Geräts des Protelion Netzwerkbenutzers Aktivitätsdaten des Protelion Netzwerkbenutzers
Erfassung von Benutzeraktionen, Sicherstellung der Nichtabstreitbarkeit	Daten über die Aktivität des Benutzers von Protelion SMC
Überwachung von Protelion Benutzergeräten zur Erkennung von Problemen im Protelion Netzwerk	Daten eines Geräts des Protelion Netzwerkbenutzers

Beschreibung der Gründe, auf welche die personenbezogenen Daten verarbeitet werden	Kategorien personenbezogener Daten
Verwaltung von Sicherheitsrichtlinien auf Protelion Netzwerkgeräten	Daten eines Benutzers des Protelion Netzwerks Daten eines Geräts des Protelion Netzwerkbenutzers

Wem wird der Zugriff auf personenbezogene Daten gewährt?

Im Rahmen der Datenschutzvorgänge, die Protelion SMC unterstützt, können personenbezogene Daten für folgende Kategorien der Empfänger verfügbar gemacht werden.

Kategorie der Empfänger	Grund für die Gewährung des Zugriffs
Protelion Netzwerkbenutzer	Notwendigkeit der Authentifizierung
Benutzer von Protelion SMC	Sicherer Datenaustausch zwischen den Benutzergeräten des Protelion Netzwerks Verwaltung der primären Bereitstellung der Protelion Schlüsseldistribution Monitoring von Benutzergeräten zur Erkennung von Problemen im Protelion Netzwerk Verwaltung von Sicherheitsrichtlinien auf Protelion Netzwerkgeräten
Protelion VPN	Anmelden bei Protelion SMC Erhalten einer Schlüsseldistribution
Protelion Enterprise Messenger	Gewährleistung einer sicheren Unternehmenskommunikation

Hinweis. Der Administrator von Protelion SMC kann sowohl ein Mitarbeiter des Unternehmens, das den SMC-Dienst verwendet, als auch ein Vertreter des Dienstanbieters sein, der diesen Dienst im Interesse des Unternehmens bietet.

Wie lange werden personenbezogene Daten gespeichert?

Protelion SMC unterstützt unten beschriebene automatische Löschvorgänge für die Daten, die von Protelion SMC erhoben und in der Anwendung gespeichert werden. Wenn die verantwortliche Stelle eine zusätzliche Speicherung braucht, sollte sie für angemessene Speicherung außerhalb der in Protelion SMC vorgesehenen Zeiträume und außerhalb des Produkts sorgen.

Speicherort	Daten	Speicherfrist und -bedingungen
Protelion SMC	Schlüsseldistribution (falls Protelion SMC Rollout verwendet wird)	Sie wird höchstens einen Tag lang gespeichert, vom Erstellungszeitpunkt oder bis zum Erreichen der maximalen Anzahl von Anfragen auf die Schlüsseldistributionen für das Gerät. Um die Speicherbedingungen für die Schlüsseldistribution zu klären, wenden Sie sich an den Protelion SMC Administrator.

Speicherort	Daten	Speicherfrist und -bedingungen
	Einträge der Ereignis-Logdatei	Werden beim Löschen der Ereignis-Logdatei gelöscht und nicht länger als ein Jahr gespeichert und dann automatisch gelöscht.
	Geräte-Monitoringdaten, Protelion VPN-Ereignisse, Ereignis-Logdatei in Protelion Enterprise Messenger, Netzwerkaktivität auf dem Gerät (falls Protelion SMC Monitoring verwendet wird)	Standardmäßig werden sie maximal 90 Tage lang gespeichert und dann automatisch gelöscht. Um die Speicherbedingungen zu klären, wenden Sie sich an den Protelion SMC Administrator.
	Benutzerberechtigung für die Kommunikation in Protelion Enterprise Messenger	Explizit gelöscht oder wenn ein Benutzer, eine Organisation aus dem System entfernt wird.
	Bild des Benutzers, interne Nummer, zusätzliche Parameter aus externer Datenquelle	Explizit gelöscht oder wenn ein Benutzer, eine Organisation aus dem System entfernt wird. Wenn Daten aus Active Directory gelöscht werden, werden die Daten in Protelion SMC nach der nächsten Synchronisierung mit dem Active Directory gelöscht. Das Benutzerbild muss aus Active Directory gelöscht werden, sonst wird es nach der nächsten Synchronisation mit Active Directory unter Protelion SMC wiederhergestellt.
	Typ, Name und ID des Benutzergeräts	Werden gelöscht, wenn von Protelion SMC Gerät, Benutzer, Organisation entfernt werden. Beim Entfernen des Gerät aus dem VPN-Modul bleibt das Gerät im SMC-Kern mit angegebenem Namen. Der Typ und die ID des Geräts werden nicht gespeichert. In Protelion SMC Monitoring werden die Daten für die im Protelion SMC Monitoring definierte Zeit gespeichert, auch wenn sie aus dem VPN-Modul oder Protelion SMC gelöscht wurden.
	Benutzerverbindungen, Liste verbundener Protelion Geräte anderer Netzwerkbenutzer	Wird manuell vom Administrator entfernt, wenn der Zugriff auf Netzwerkobjekte eingeschränkt werden muss, und automatisch, wenn ein Benutzer aus Protelion SMC entfernt wird.
	Benutzergruppe	Das Löschen einer Gruppe oder eines Benutzers aus einer Gruppe erfolgt manuell durch den Administrator oder automatisch, wenn ein Benutzer oder eine Gruppe aus dem System entfernt wird.
	Andere Daten der SMC- und Protelion Netzwerkbenutzer	Explizit gelöscht oder wenn eine Organisation aus dem System entfernt wird.

Wie hilft Protelion GmbH beim Schutz der Rechte betroffener Personen?

Protelion GmbH bietet folgende Werkzeuge und Dokumente zur Unterstützung und Vereinfachung des Schutzes der Rechte betroffener Personen.

- **Auskunftsrecht**

  Betroffene Personen haben das Recht Auskunft zu erhalten, ob deren personenbezogenen Daten verarbeitet werden und wenn ja, auf Auskunft über diese personenbezogenen Daten und weitere Informationen, insbesondere über:

  - Verarbeitungszweck
  - Kategorie personenbezogener Daten
  - Empfänger oder Kategorien der Empfänger, für die personenbezogene Daten entdeckt wurden
  - Dauer der Speicherung

  Betroffene Personen können ferner Anspruch auf eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, erhalten.

  Die Schlüsseldistribution für ein bestimmtes Gerät wird dem Benutzer auf Anfrage während der Installation zur Verfügung gestellt und wird gelöscht, wenn die maximale Anzahl von Anfragen überschritten wird.

  Die Ereignis-Logdatei kann jederzeit heruntergeladen werden; ein Protelion SMC Administrator kann es verwenden, um Details zu den betroffenen Personen zu erhalten. Sehen Sie den Abschnitt „Anzeigen der Logdatei" in der Protelion SMC Dokumentation.

  Die Logdatei-Einträge des Protelion VPN, das auf dem Benutzergerät installiert ist, die IP-Pakete-Logdatei mit den Informationen über die Netzwerkaktivität des Geräts und die Ereignislogdatei von Protelion Enterprise Messenger können Sie im Logdateispeicher finden. Sehen Sie den Abschnitt „Empfangen der Logdateien vom Gerät" in der Protelion SMC Monitoring Dokumentation.

  Protelion SMC Enterprise Messenger Book verfügt über keine Mechanismen zum Herunterladen von Netzwerkbenutzerdaten.

  Die Benutzerdaten von Protelion SMC Benutezrn und die Gerätedaten des Protelion Netzwerkbenutzers können von der Benutzeroberfläche von Protelion SMC kopiert werden. Protelion SMC verfügt über keine Mechanismen zum Herunterladen von benutzerspezifischen Daten in externe Systeme oder Medien.

- **Recht auf Berichtigung**

  Das Recht auf Berichtigung wird für den Benutzer als Recht auf Berichtigung der Benutzerbeschreibung, des Benutzernamens, der Telefonnummer und der E-Mail-Adresse, des Namens der Organisation und der Abteilung, der Benutzerrechte im Verwaltungssystem, des Logins und des Passworts für die Authentifizierung im Verwaltungssystem, der Liste der Benutzergeräte und deren Namen (wenn die Änderung der Geräteliste den Netzwerkbetrieb nicht stört). Andere Daten können nicht berichtigt werden.

  In Protelion SMC Policies kann der Administrator die vom SMC-Kern und dem VPN-Modul bereitgestellten Informationen verwenden. Sie können in bestimmten Regeln einen beliebigen Benutzernamen angeben. Auf diese Weise angegebene Benutzer werden nicht im SMC-Kern erstellt und verwendet, sondern als Teil der resultierenden Richtlinie an die Geräte weitergegeben.

- **Recht auf Löschung (Recht auf Vergessenwerden)**

  Die betroffene Person hat das Recht auf Löschung personenbezogener Daten ohne unbegründete Verzögerung im Falle, wenn die personenbezogenen Daten für die Zwecke, für die sie gesammelt wurden, nicht mehr notwendig sind, und im Falle, wenn die betroffene Person ihre Verarbeitungseinwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt.

  Die Löschung der Daten der betroffenen Person gilt für die Schlüsseldistribution und Überwachungsdaten des Geräts der betroffenen Person, sowie für die Ereignis-Logdatei durch Rotation. Die Löschung von Benutzerdaten erfolgt durch explizite Entfernung des Benutzers aus dem System oder bei Entfernung der Organisation, zu der ein Benutzer gehört.

- **Recht auf Datenübertragbarkeit**

  Das Recht auf Datenübertragbarkeit kann für Daten einer betroffenen Person bestehen, die sie einem Verantwortlichen bereitgestellt hat und deren Verarbeitung auf einer Berichtigungseinwilligung oder einem automatisierten Verfahren erfolgt. Protelion SMC beinhaltet keine Möglichkeit der Einholung einer Einwilligung für die mit Protelion SMC durchgeführte Datenverarbeitungsvorgänge. Ferner werden von den betroffenen Personen keine personenbezogenen Daten aktiv bereitgestellt werden. Dementsprechend wird eine Datenübertragbarkeit durch das Produkt nicht unterstützt.

- **Recht auf Widerspruch und Einschränkung der Verarbeitung**

  Das Recht auf Widerspruch und Einschränkung der Verarbeitung kann im Sinne von Protelion SMC nur durch das Entfernen des Benutzers aus dem System ausgeübt werden, wenn es den Netzwerkbetrieb nicht stört. Um die Datenverarbeitung durch Protelion SMC Monitoring einzuschränken, können Sie das Gerät vom Monitoring ausschließen und den Protelion SMC Monitoring Agent vom Gerät entfernen.