

Häufig gestellte Fragen

- [Browser-Sicherheit](#)
- [garrioCOM Messenger-Dienst als App zur Taskleiste \(Windows\) hinzufügen](#)
- [Meine Benutzerkonten werden nicht mehr angezeigt](#)
- [Die Nachrichten der Patienten werden nicht angezeigt](#)
- [Remote-Support mit TeamViewer](#)

Browser-Sicherheit

Hintergrund: Sicherheitsfaktor

Damit garrioCOM nach der Ersteinrichtung weiterhin wie vorgesehen funktioniert und aufgerufen werden kann ist die korrekte Konfiguration des verwendeten Browsers entscheidend.

Bei der Ersteinrichtung wird zunächst die Administrations-Anwendung von garrioCOM (<https://admin.garrio.de>) mit einem PC der Praxis verbunden. Die so hergestellte Verbindung zwischen Praxis und den garrio-Systemen im garrio-Rechenzentrum wird mittels auf dem Praxis-PC gespeicherten Daten verifiziert. Gleiches gilt für die Verbindung der Praxis-Anwendung von garrioCOM (<https://praxis.garrio.de>) mit den Arbeitsplätzen der Praxis.

Damit diese Verifizierung und Absicherung auch bei späteren Verwendungen der Applikationen einwandfrei funktionieren und garrioCOM von der Praxis genutzt werden kann, muss die Speicherung dieser Daten vom Browser zugelassen werden und – entscheidend – vom Browser dauerhaft behalten werden. Eine automatische Löschung dieser Daten führt dazu, dass garrioCOM nicht genutzt werden kann.

Inkognito-/Privater-Modus

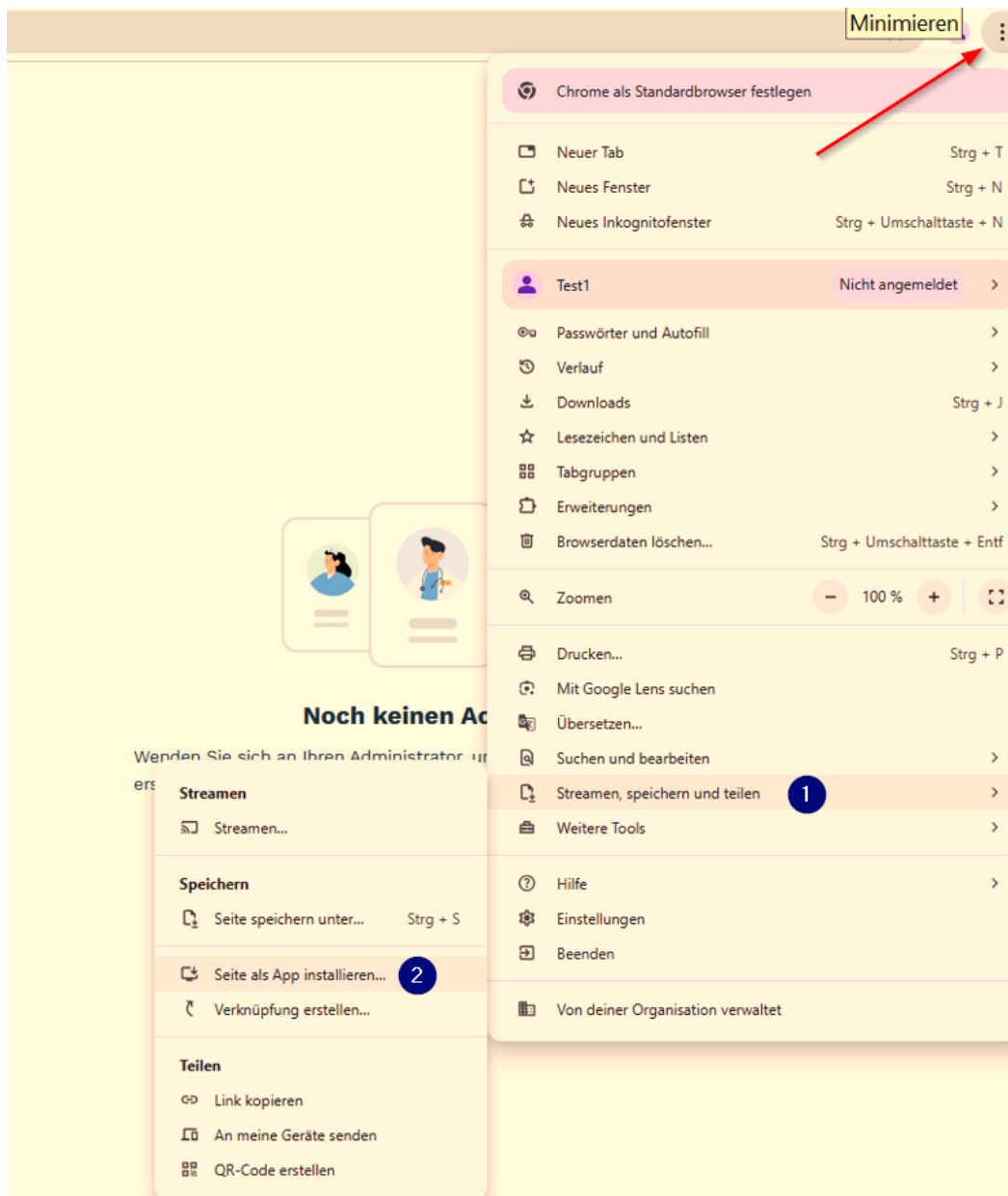
Da es im Inkognito-/Privat-Modus keine Möglichkeit gibt die Daten zur Verifizierung der Arbeitsplätze zu erhalten (in diesem Modus wird nach Sitzungsende immer gelöscht), ist dieser Modus für die sinnvolle Nutzung von garrioCOM nicht geeignet und nicht empfohlen.

Selbstverständlich funktioniert garrioCOM weiterhin in diesem Modus, die Verifizierung der Arbeitsplätze muss dann jedes Mal durch die Wiederherstellung der Verbindung neu erfolgen.

garrioCOM Messenger-Dienst als App zur Taskleiste (Windows) hinzufügen

Chrome Browser

1. Geben Sie **garrioCOM careprovider** in die Adressleiste des **Chrome Browsers** ein und rufen Sie die Seite auf.
2. Klicken Sie auf die drei Punkte im rechten, oberen Bereich des Fensters (siehe Pfeil im Bild).

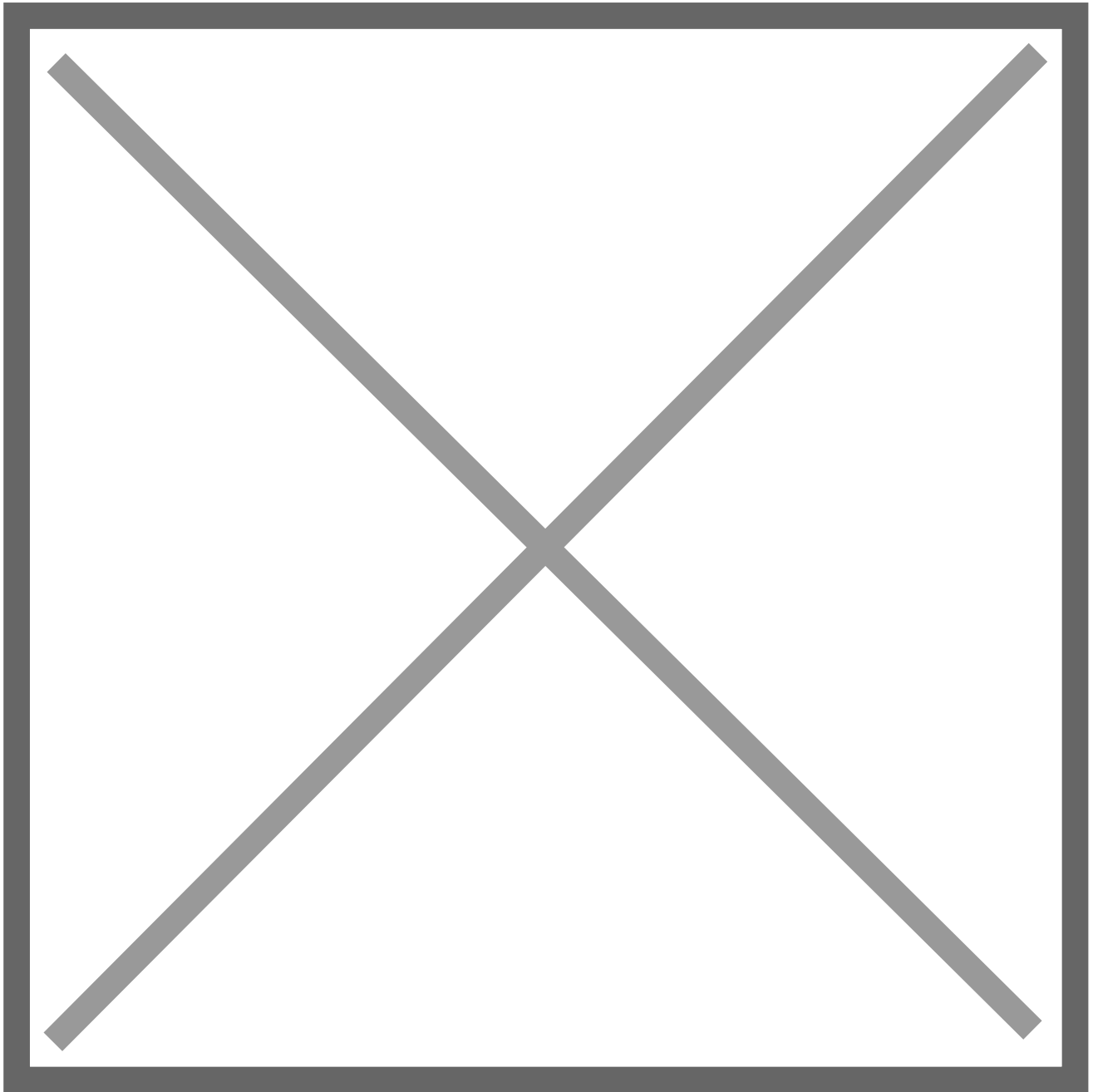


3. Klicken Sie nun auf **(1) "Streamen, speichern und teilen"** und anschließend auf **(2) "Seite als App installieren"**.

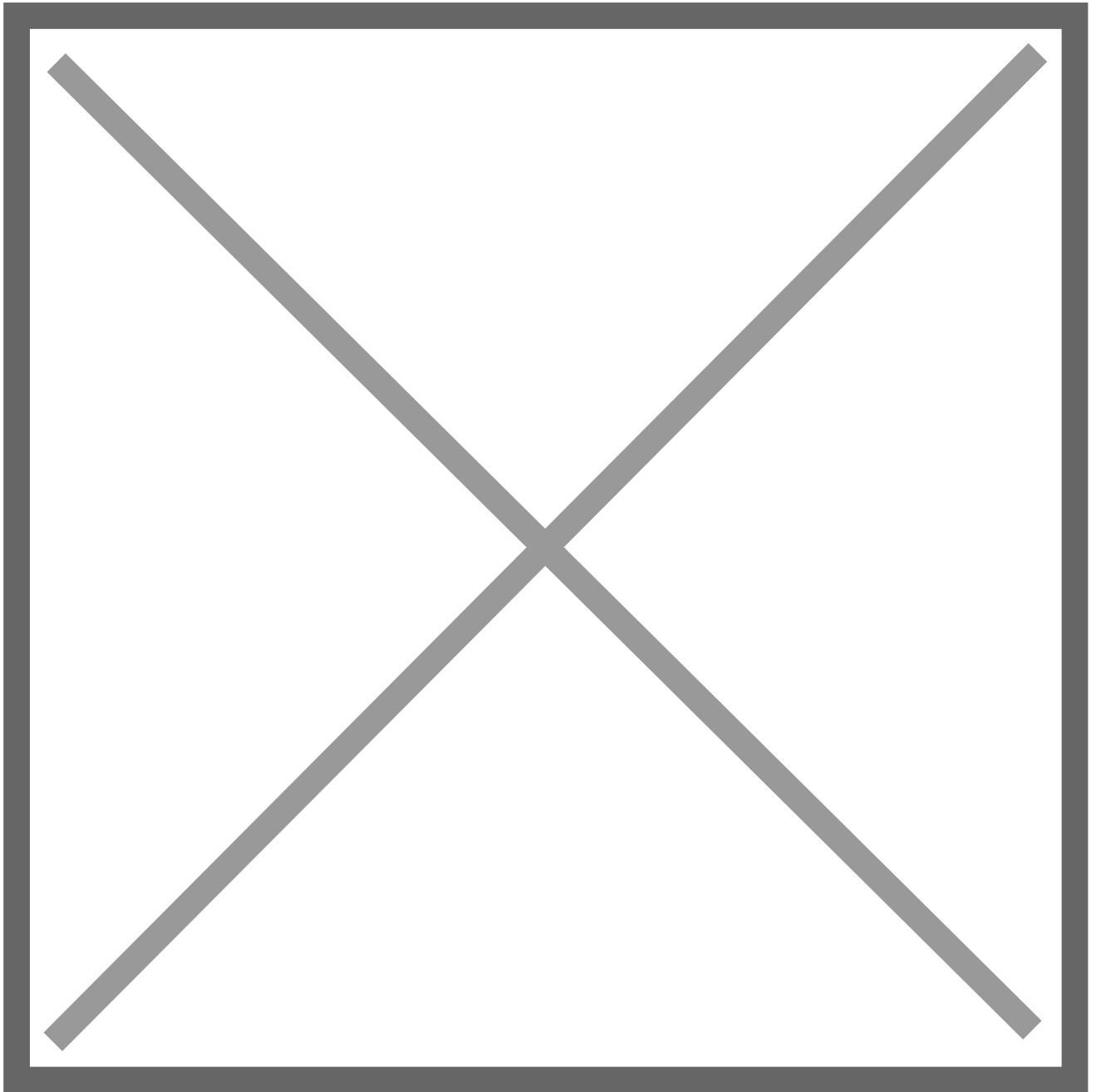
Edge Browser

Möchten Sie den garrioCOM Messenger zur Taskleiste hinzufügen, gehen Sie wie folgt vor:

1. Geben Sie **garrioCOM careprovider** in die Adressleiste des **Edge Browsers** ein und rufen Sie die Seite auf.
2. Klicken Sie auf die drei Punkte im rechten, oberen Bereich des Fensters (siehe Pfeil im Bild).



3. Nun klicken Sie auf **(1) „Apps“** und anschließend auf **(2) „Diese Seite als eine App installieren“**.



4. Es erscheint ein weiteres Fenster, in dem Sie erneut auf **„Installieren“** klicken.

Diese Site als eine App installieren



[Bearbeiten](#)

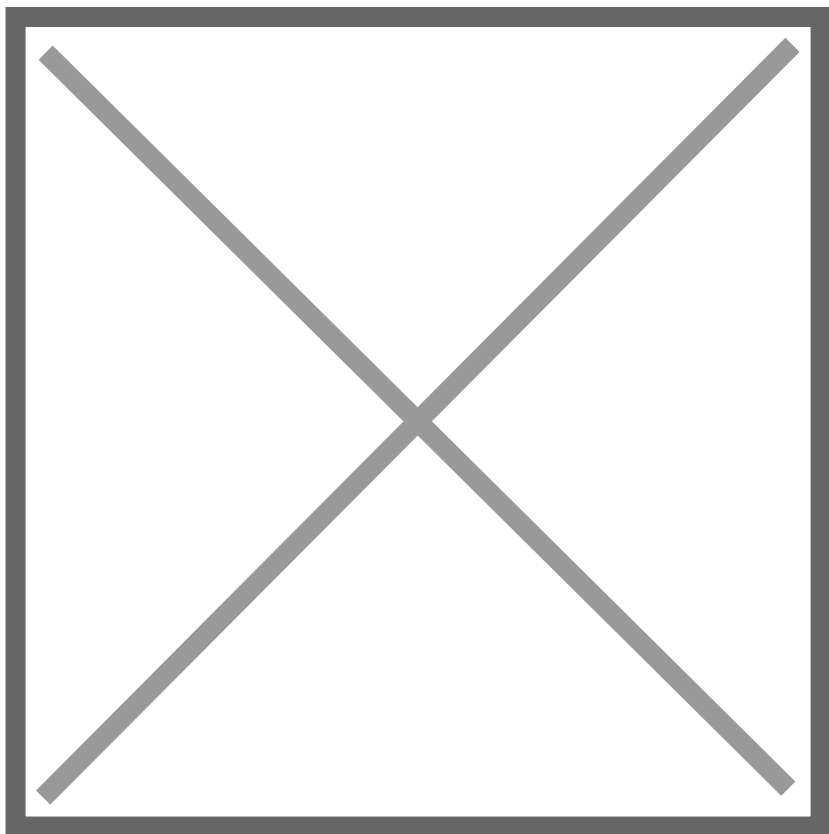
garrio - careprovider

Diese Website kann als Anwendung installiert werden. Sie wird in einem eigenen Fenster geöffnet und Sie können sie für einen schnellen Zugriff an Ihre Taskleiste anheften.

Installieren

Jetzt nicht

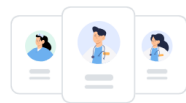
5. Im letzten Fenster wählen Sie den Bereich aus, an den die garrioCOM App angeheftet werden soll (siehe Bild)



Meine Benutzerkonten werden nicht mehr angezeigt

Beschreibung des Problems

Sie rufen die Praxis-Seite auf (<https://praxis.garrio.de/> bzw. <https://garrio.de/com/praxis/login>) und es werden keine Benutzerkonten mehr angezeigt (siehe Bild)?



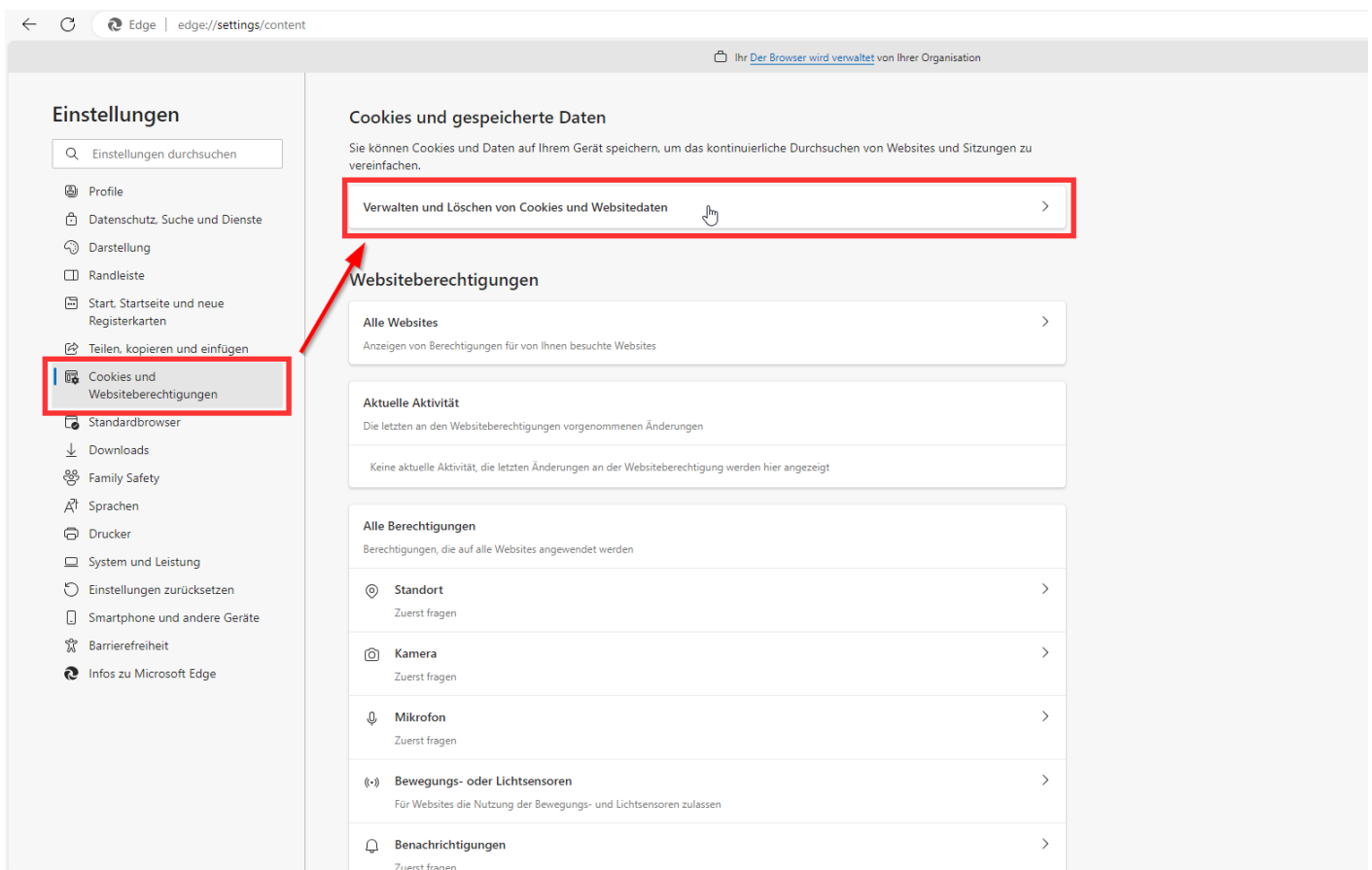
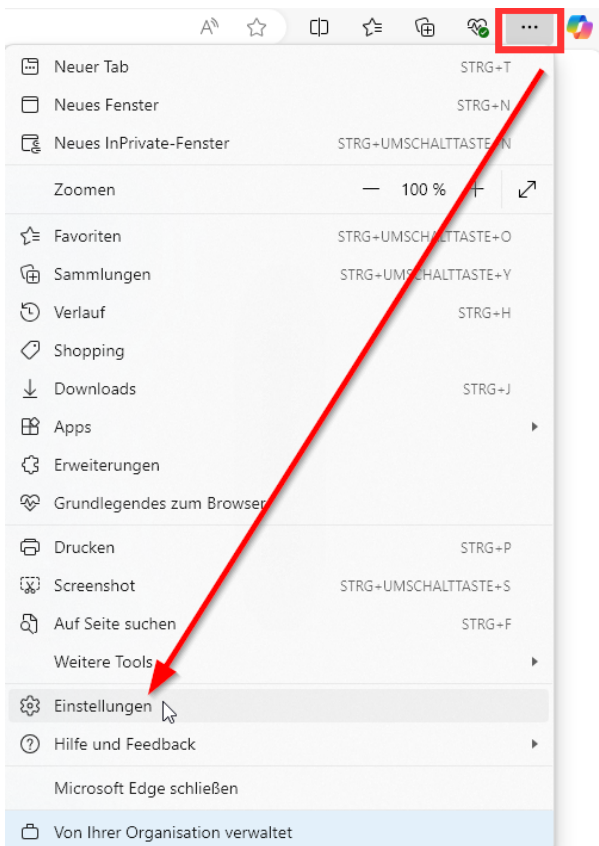
Noch keinen Account
Wenden Sie sich an Ihren Administrator,
um ein Konto für Sie zu erstellen

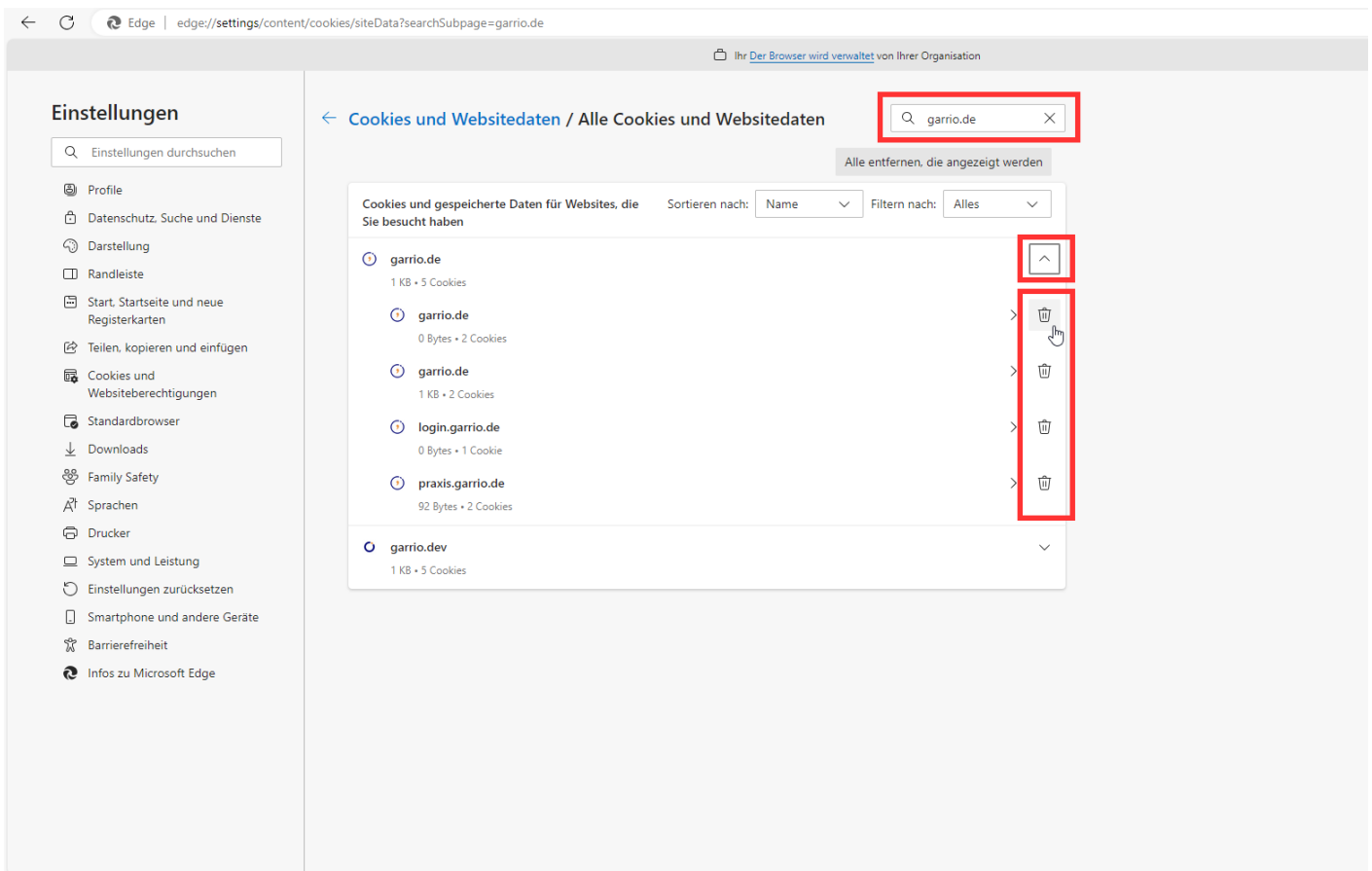
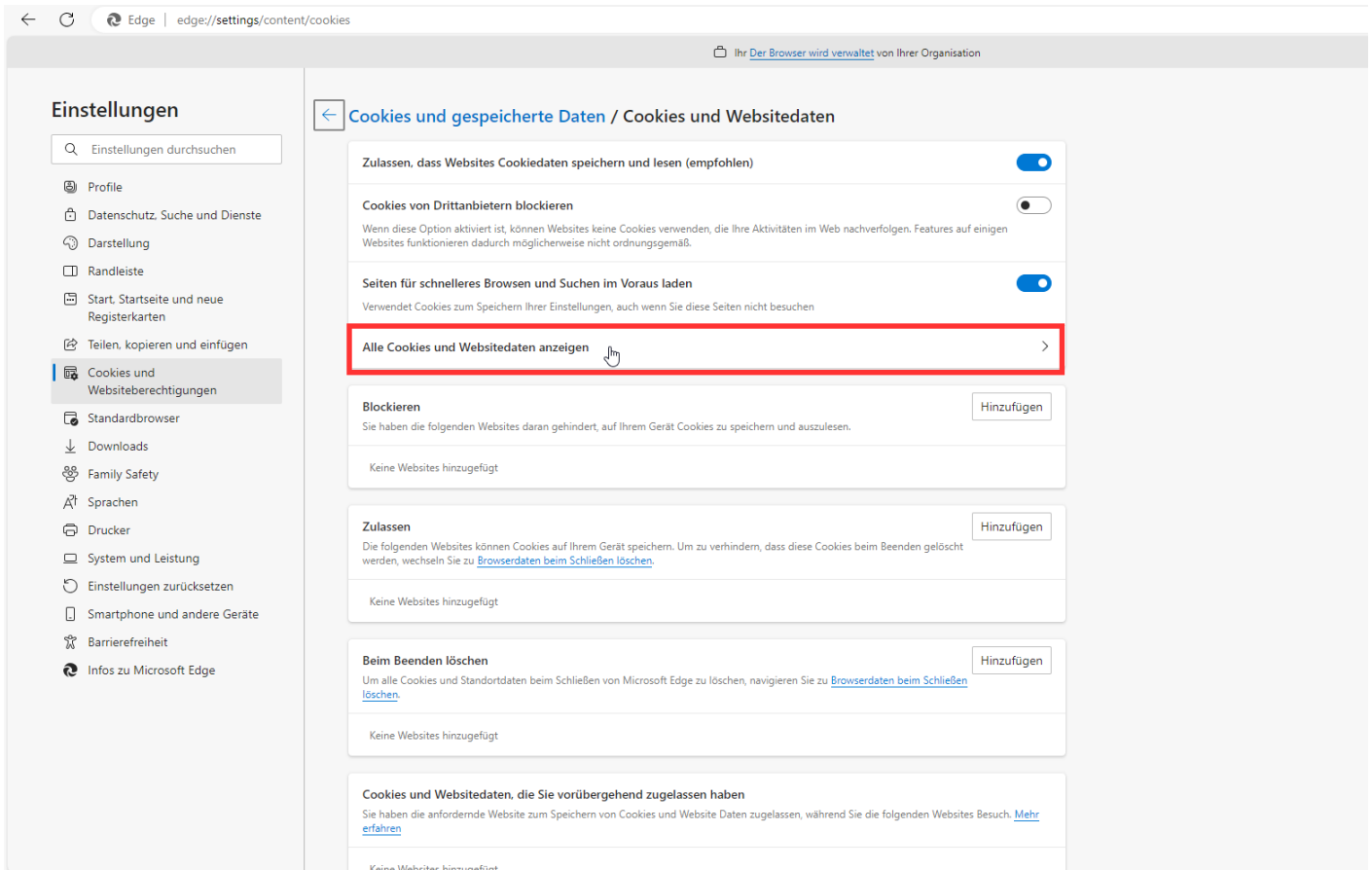
Lösung

Löschen Sie zunächst die Cookies in Ihrem Browser und aktivieren Sie den Browser dann wieder mittels Magischem Link.

Cookies löschen mit Microsoft Edge

Öffnen Sie die Einstellungen des Browsers und gehen Sie wie abgebildet zu den Cookie-Einstellungen:



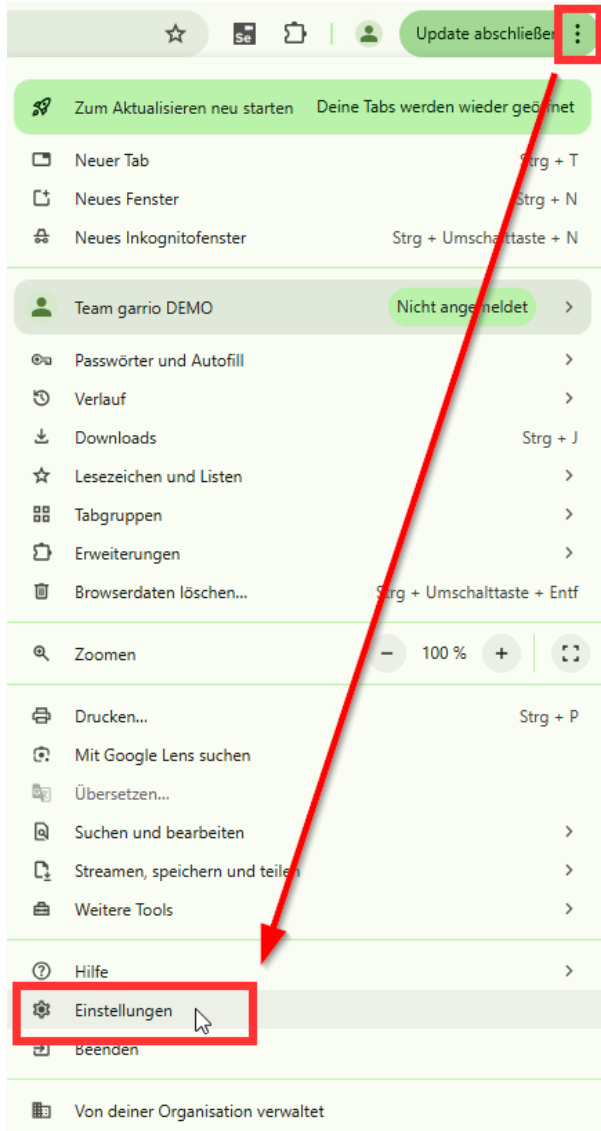


Alternativ können Sie auch direkt folgenden Link in Ihrem Edge Browser eingeben, sie gelangen dann direkt zu diesen Einstellungen:

<edge://settings/content/cookies/siteData?searchSubpage=garrio.de>

Hier löschen Sie alle zu den Seiten garrio.de, login.garrio.de, praxis.garrio.de und ggf. admin.garrio.de angezeigten Cookies.

Cookies löschen mit Google Chrome



← → ↻ Chrome chrome://settings/privacy

Einstellungen

Google und ich

Autofill und Passwörter

Datenschutz und Sicherheit

Leistung

Darstellung

Suchmaschine

Standardbrowser

Beim Start

Sprachen

Downloads

Bedienungshilfen

System

Einstellungen zurücksetzen

Erweiterungen

Über Google Chrome

In Einstellungen suchen

Dein Browser wird von deiner Organisation verwaltet

Sicherheitscheck

Chrome hat einige Sicherheitsempfehlungen gefunden, die du dir ansehen solltest
Passwörter, Chrome-Update, Berechtigungen [Zum Sicherheitscheck](#)

Datenschutz und Sicherheit

- Browserdaten löschen
Verlauf, Cookies und andere Daten löschen sowie Cache leeren
- Drittanbieter-Cookies
Drittanbieter-Cookies sind im Inkognitomodus blockiert
- Datenschutz bei Anzeigen
Du kannst die Informationen anpassen, die von Websites verwendet werden, um dir Werbung zu präsentieren
- Sicherheit
Safe Browsing (Schutz vor schädlichen Websites) und andere Sicherheitseinstellungen
- Website-Einstellungen**
Welche Informationen Websites nutzen und anzeigen dürfen (z. B. Standort, Kamera, Pop-ups)

← → ↻ Chrome chrome://settings/content

Einstellungen

Google und ich

Autofill und Passwörter

Datenschutz und Sicherheit

Leistung

Darstellung

Suchmaschine

Standardbrowser

Beim Start

Sprachen

Downloads

Bedienungshilfen

System

Einstellungen zurücksetzen

Erweiterungen

Über Google Chrome

In Einstellungen suchen

Website-Einstellungen

Sicherheitscheck

Berechtigungen von 1 Website entfernt
Zum Schutz deiner Daten wurden einer Website Berechtigungen entzogen [Zum Sicherheitscheck](#)

Letzte Aktivität

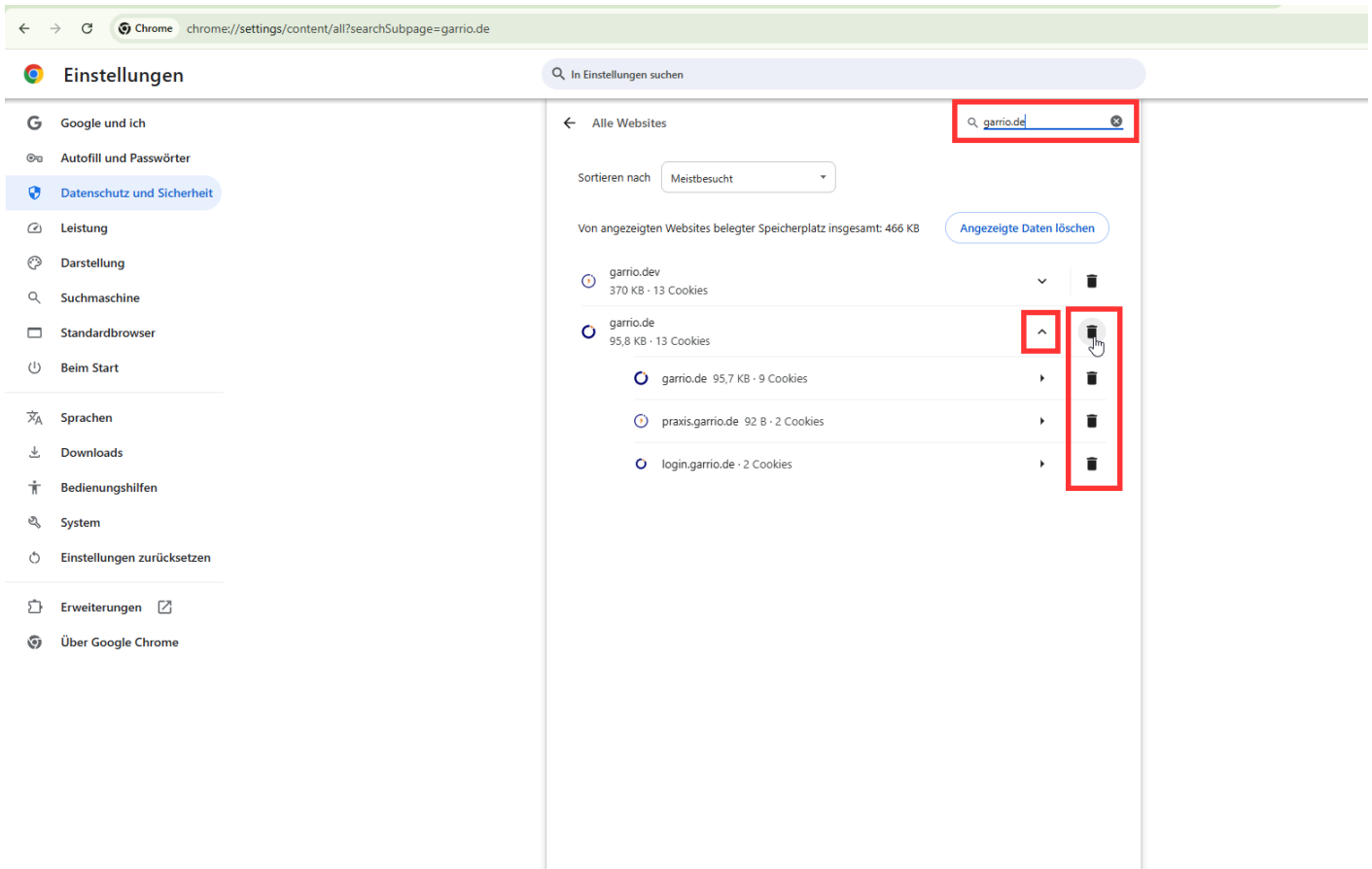
- garrio.de
Benachrichtigungen zugelassen
- staging.garrio.dev
Benachrichtigungen, Auto-Downloads zugelassen
- praxis.staging.garrio.dev
Kamera und 2 weitere zugelassen

Nach Websites sortierte Berechtigungen und gespeicherte Daten aufrufen

Berechtigungen

- Standort
Websites dürfen nach meinem Standort fragen

Kamera

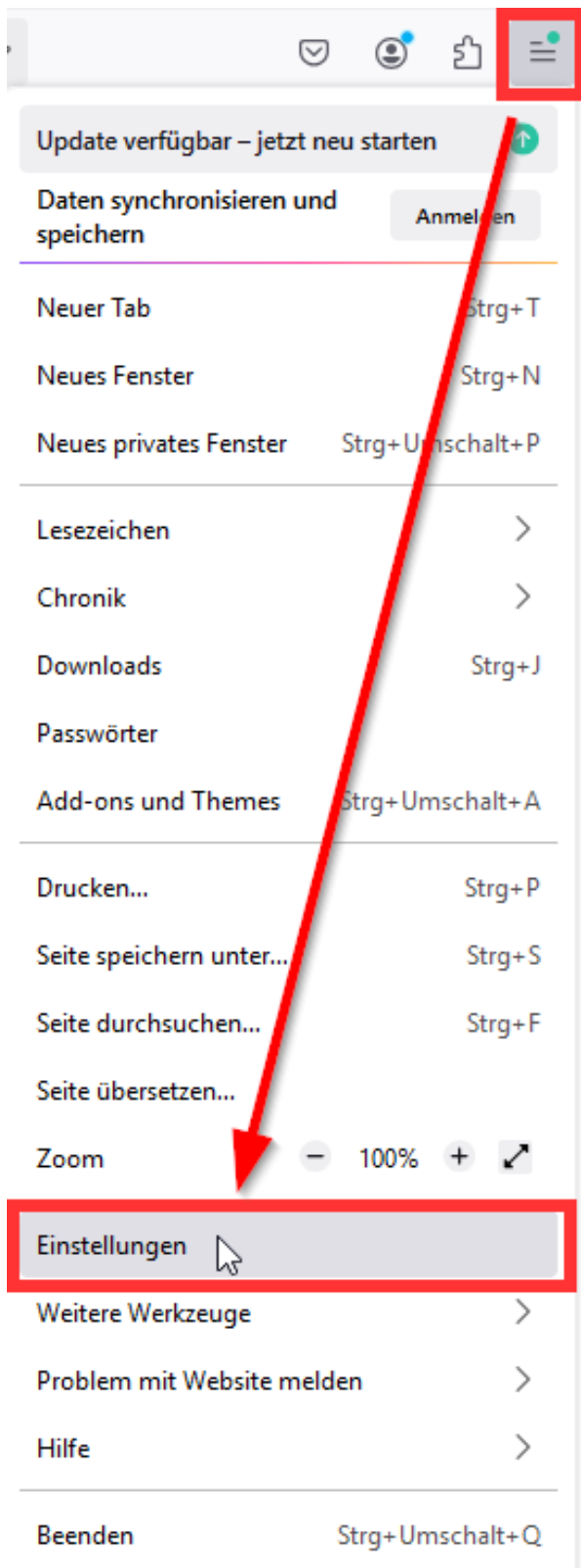


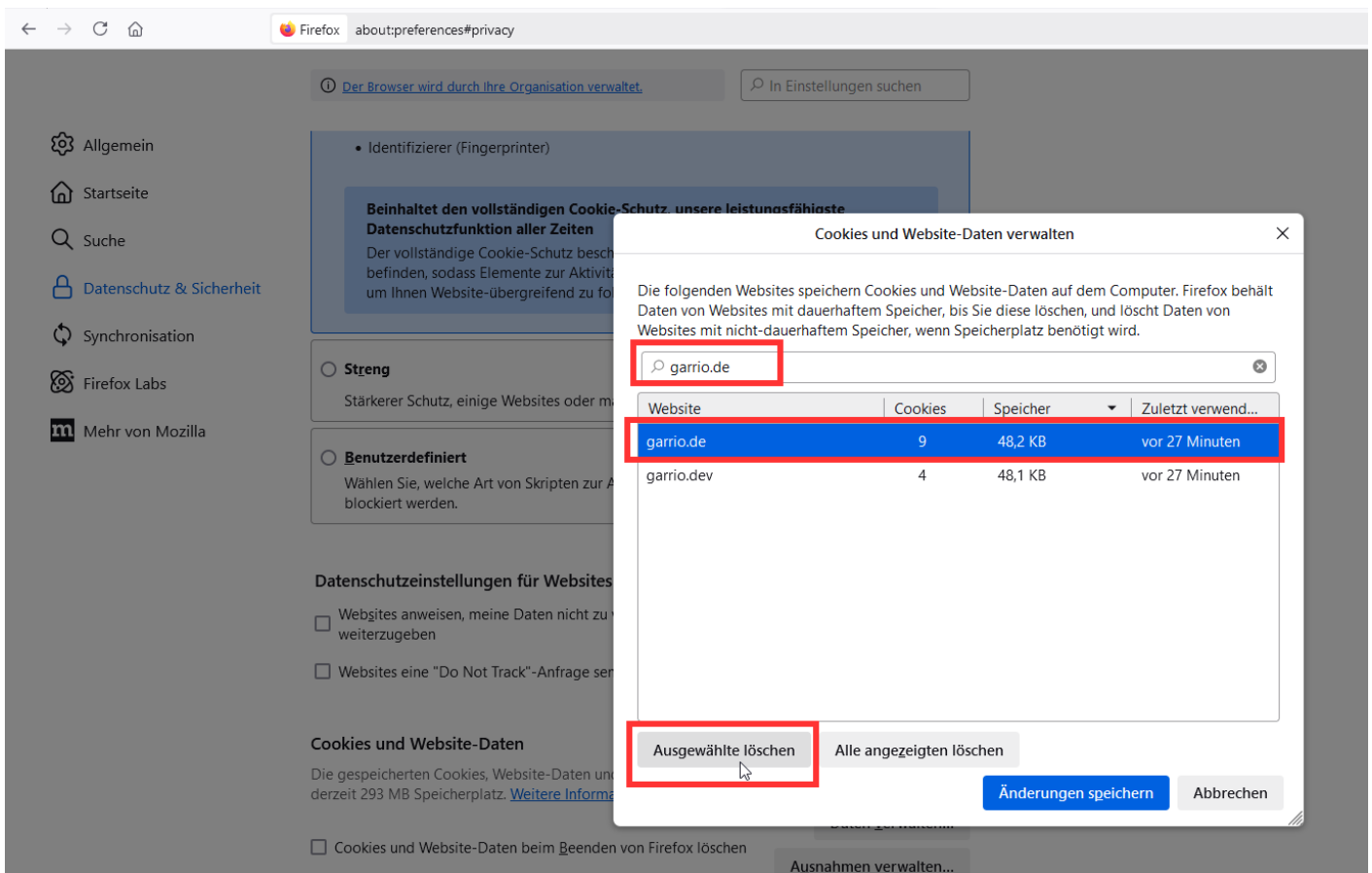
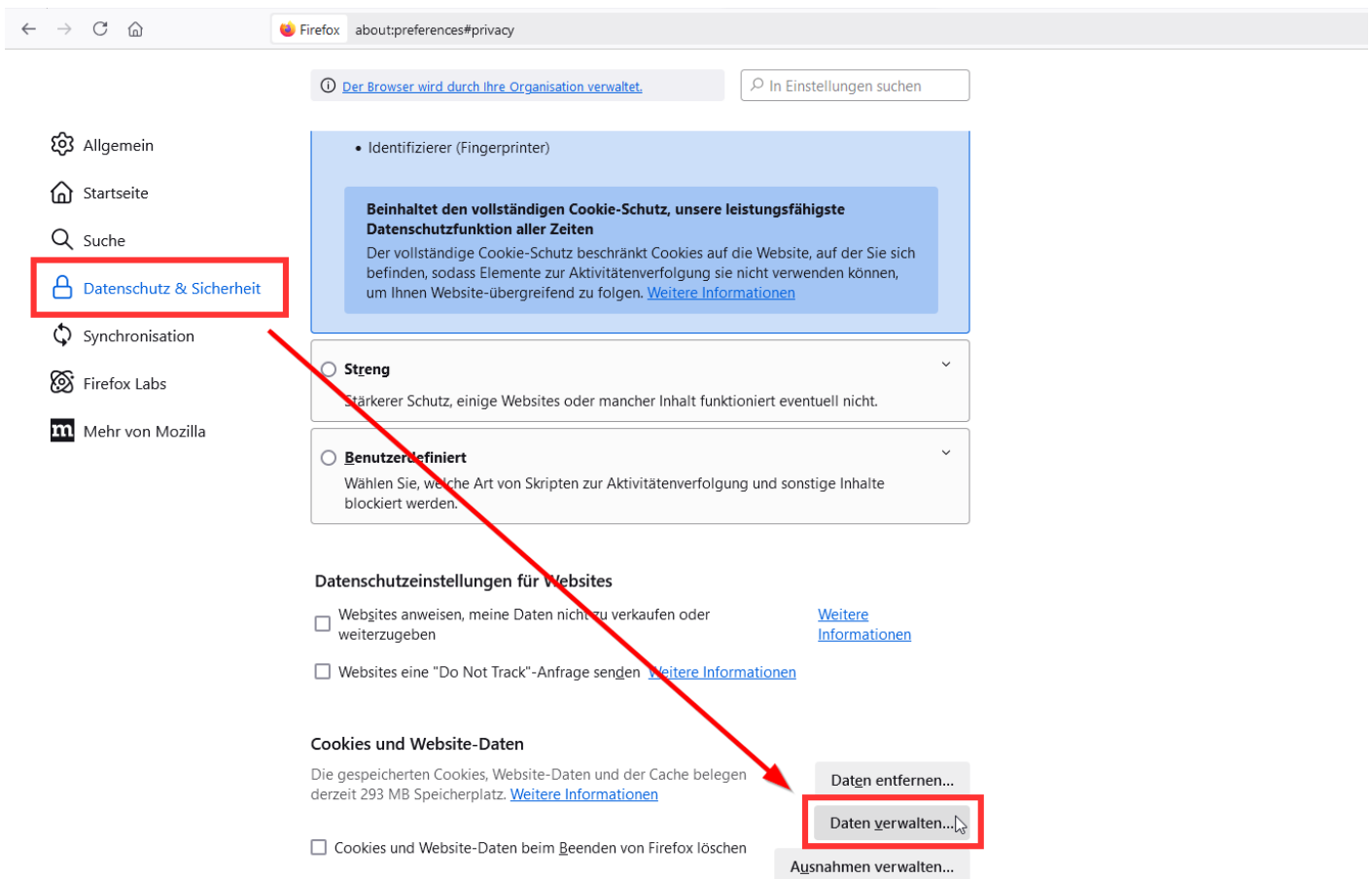
Alternativ können Sie auch direkt folgenden Link in Ihrem Chrome Browser eingeben, sie gelangen dann direkt zu diesen Einstellungen:

<chrome://settings/content/all?searchSubpage=garrio.de>

Hier löschen Sie alle zu den Seiten garrio.de, login.garrio.de, praxis.garrio.de und ggf. admin.garrio.de angezeigten Cookies.

Cookies löschen mit Mozilla Firefox





Browser erneut aktivieren

Anschließend können Sie Ihren Browser mit einem neuen Magischen Link erneut aktivieren.

Die Nachrichten der Patienten werden nicht angezeigt

Beschreibung des Problems

In der Anfragepinnwand werden die Nachrichten von Patienten nicht dargestellt, da sie nicht entschlüsselt werden können. Die Nachrichten werden lediglich ausgegraut angezeigt, wie der beigefügte Screenshot veranschaulicht.

The screenshot displays a medical software interface. On the left is a dark blue sidebar with various icons. The main area is divided into two panels. The top panel shows patient information: 'Unterschrift' (Signature) with an edit icon, 'PATIENT' details (name, date of birth 01.01.1980), 'ZUGEWIESEN AN' (Assigned to) with a dropdown menu showing 'Nicht zugeordnet' and an 'Übernehmen' (Take over) button, 'ERSTELLT VON' (Created by) with a name and date 'Am 27.01.2025 07:46', and 'STATUS' with a blue 'Offen' (Open) button and a 'Schnellaktion' (Quick action) link. Below this is a tabbed interface with 'Extern', 'Intern', 'Dateien', and 'Verlauf' tabs. The 'Verlauf' tab is active, showing a chat history with messages from 'garrio' and an automated response. The bottom panel shows a chat input area with a lock icon, a plus icon, and a text field labeled 'Antworten...'. On the right side, there is a separate panel titled 'Anfragen von Patienten' (Patient requests) with a search bar and a list of 'OFFEN (1)' (Open (1)) requests. One request is visible, showing a patient's name, the word 'Unterschrift', and a status of '#114'.

Lösung

Das beschriebene Problem ist als eine systemimmanente Sicherheitsfunktion zu betrachten. Der Hauptzweck dieser Sicherheitsfunktionen besteht darin, die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Sie dienen dazu, sicherzustellen, dass ausschließlich die intendierten Empfänger die Nachrichten einsehen können und dass eine Manipulation der Nachrichten während der Übertragung unterbunden wird. Wenngleich es mitunter zu Unannehmlichkeiten kommen kann, wenn Nachrichten nicht entschlüsselt werden können, stellt dies einen wesentlichen Kompromiss für eine sichere Kommunikation dar.

Technische Hintergründe

Es existieren mehrere Gründe, warum Nachrichten versandt werden können, die der Empfänger nicht entschlüsseln und lesen kann. Diese Sicherheitsfunktionen dienen im Wesentlichen dem Schutz der Privatsphäre und der Integrität der Kommunikation. Die folgenden Ausführungen geben Aufschluss über die Hauptgründe und den Zweck dieser Funktionen.

Fehlende oder falsche Schlüssel

- **Wie es passiert:** Die Ende-zu-Ende-Verschlüsselung (E2EE) funktioniert durch den Austausch von kryptografischen Schlüsseln zwischen den Kommunikationspartnern. Jeder Teilnehmer besitzt einen privaten Schlüssel, der geheim gehalten wird, und einen öffentlichen Schlüssel, der mit anderen geteilt wird. Nachrichten werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können nur mit dessen privatem Schlüssel entschlüsselt werden. Wenn der Empfänger keinen passenden privaten Schlüssel hat (z.B. weil er ein neues Gerät verwendet oder seinen Schlüssel zurückgesetzt hat), kann er die Nachricht nicht entschlüsseln.
- **Zweck:** Dies verhindert, dass jemand, der die Nachricht abfängt (z.B. ein Hacker oder der Serverbetreiber), den Inhalt lesen kann. Nur der rechtmäßige Empfänger mit dem passenden privaten Schlüssel kann die Nachricht entschlüsseln.

Nicht verifizierte Sitzungen

- **Wie es passiert:** Element (und andere E2EE-Messenger) ermöglichen es, mehrere Geräte gleichzeitig zu verwenden (z.B. Smartphone, Laptop, Tablet). Jedes dieser Geräte wird als "Sitzung" betrachtet. Die Option "Verschlüsselung auf verifizierte Sitzungen beschränken" sorgt dafür, dass Nachrichten nur an Sitzungen gesendet werden, die der Benutzer explizit als vertrauenswürdig verifiziert hat. Wenn diese Option aktiviert ist und der Absender eine Nachricht an ein Gerät sendet, das der Empfänger noch nicht verifiziert hat, kann die Nachricht nicht entschlüsselt werden.
- **Zweck:** Diese Funktion schützt vor sogenannten "Man-in-the-Middle"-Angriffen. Wenn ein Angreifer Zugriff auf ein unautorisiertes Gerät des Empfängers erlangt, könnte er Nachrichten abfangen. Durch die Verifizierung von Sitzungen stellt der Benutzer sicher, dass Nachrichten nur an seine vertrauenswürdigen Geräte gesendet werden.

Nachrichten gesendet, während der Empfänger offline war und keine Schlüssel verfügbar waren

- **Wie es passiert:** In einigen Fällen kann es vorkommen, dass eine Nachricht gesendet wird, während der Empfänger offline ist und sein Gerät keine Verbindung zum Server hat, um die notwendigen Schlüssel auszutauschen. Wenn der Empfänger später online geht, fehlen möglicherweise die notwendigen Informationen, um die Nachricht zu entschlüsseln.
- **Zweck:** Dies ist oft eine Folge der Art und Weise, wie E2EE implementiert ist. Es stellt sicher, dass Nachrichten auch dann nicht entschlüsselt werden können, wenn der Server kompromittiert wird.

Probleme mit der Zeit und Datums-Synchronisierung

- **Wie es passiert:** Kryptographische Prozesse sind oft zeitabhängig. Wenn die Systemzeit auf den Geräten von Sender und Empfänger stark abweicht, kann dies zu Problemen bei der Schlüsselvereinbarung und Entschlüsselung führen.
- **Zweck:** Dies ist eher eine technische Randbedingung, die aber dennoch relevant sein kann.

Remote-Support mit TeamViewer

TeamViewer herunterladen und starten

Mit TeamViewer kann unser Support-Team auf Ihren Computer zugreifen, um Ihnen schnell und einfach zu helfen.

Schritt 1: Webseite aufrufen

Öffnen Sie Ihren Internetbrowser (z.B. Google Chrome, Microsoft Edge oder Firefox) und geben Sie folgende Adresse in die Adresszeile ein oder klicken Sie direkt auf den folgenden Link:

→ support.medi-verbund.de

Drücken Sie anschließend die Eingabetaste auf Ihrer Tastatur.

Schritt 2: TeamViewer herunterladen


Auf der Webseite sehen Sie eine Schaltfläche mit der Aufschrift „**TeamViewer herunterladen**“ oder „**Fernwartung starten**“.

☐ **Klicken Sie auf diese Schaltfläche**, um den Download zu starten.

Je nach Browser erscheint eine Meldung, dass eine Datei heruntergeladen wird. Dies kann einige Sekunden dauern.

Schritt 3: TeamViewer ausführen

Nach dem Download müssen Sie die Datei öffnen:

- Falls Sie Google Chrome oder Microsoft Edge nutzen, klicken Sie unten links oder oben rechts in der Leiste auf die heruntergeladene Datei.
- Falls Sie Firefox verwenden, klicken Sie oben rechts auf das **Pfeil-Symbol**  und dann auf die Datei.

Der Name der Datei ist in der Regel „**TeamViewerQS.exe**“.

Schritt 4: TeamViewer starten

Nachdem Sie auf die Datei geklickt haben:

- ☐ Bestätigen Sie eventuelle Sicherheitsabfragen mit „**Ja**“ oder „**Zulassen**“.
- ☐ Das TeamViewer-Fenster öffnet sich.
- ☐ Teilen Sie unserem Support die **ID** und das **Passwort** mit, die im Fenster angezeigt werden.

☐ **Rufen Sie uns an oder senden Sie die Daten per E-Mail, damit wir Ihnen helfen können!**