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
- Benachrichtigungsanzeigen für garrioCOM aktivieren/ deaktivieren (Browserbezogen)
- Passwort vergessen

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

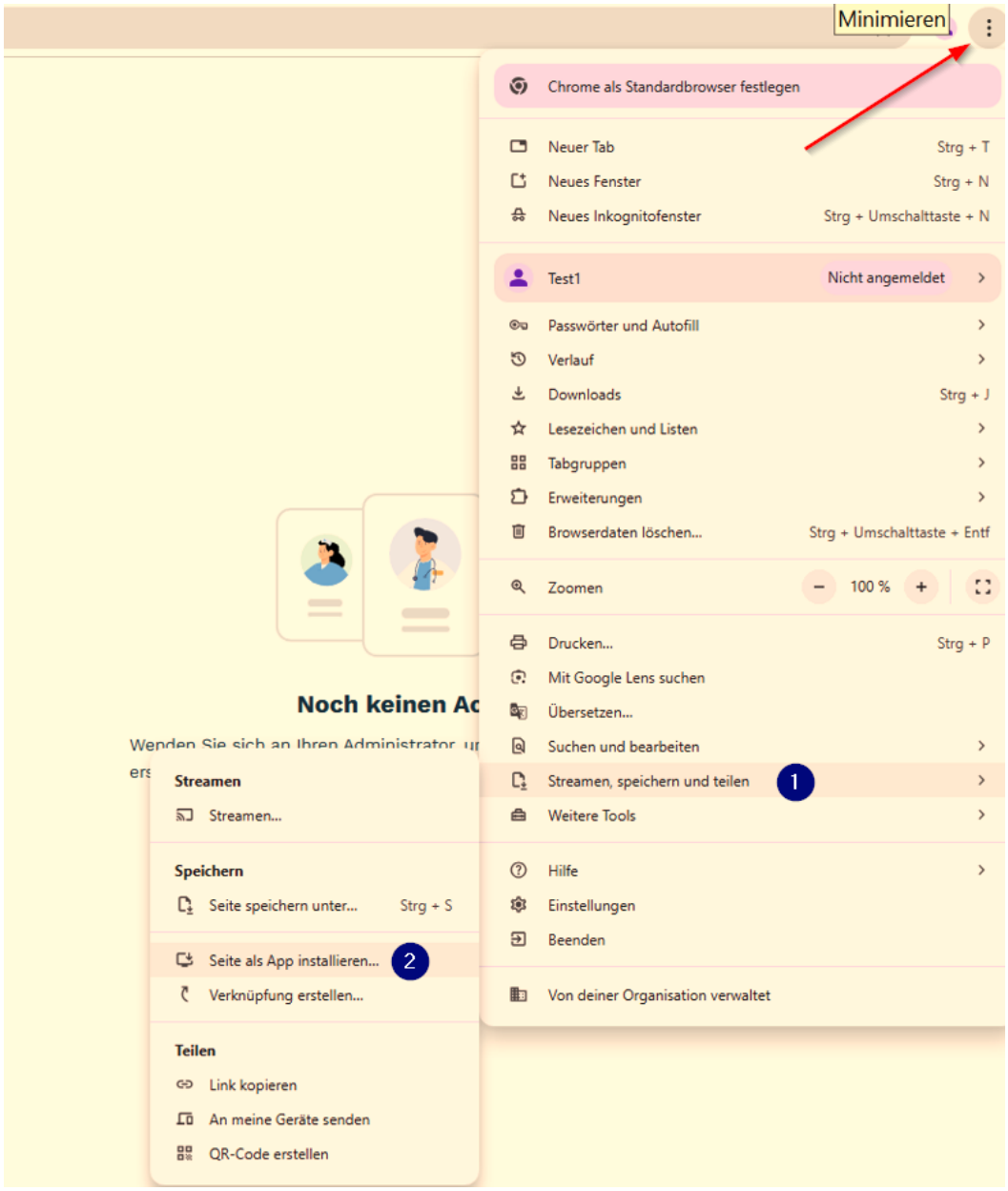
Da es im Inkognito-/Privat-Modus keine Möglichkeit gibt die Daten zur Verifizierung der Arbeitsplätze zu erhalten (in diesem Modus wird nach Sitzungsende immer gelöscht), ist dieser Modus für die sinnvolle Nutzung von garrioCOM nicht geeignet und nicht empfohlen.

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"**.

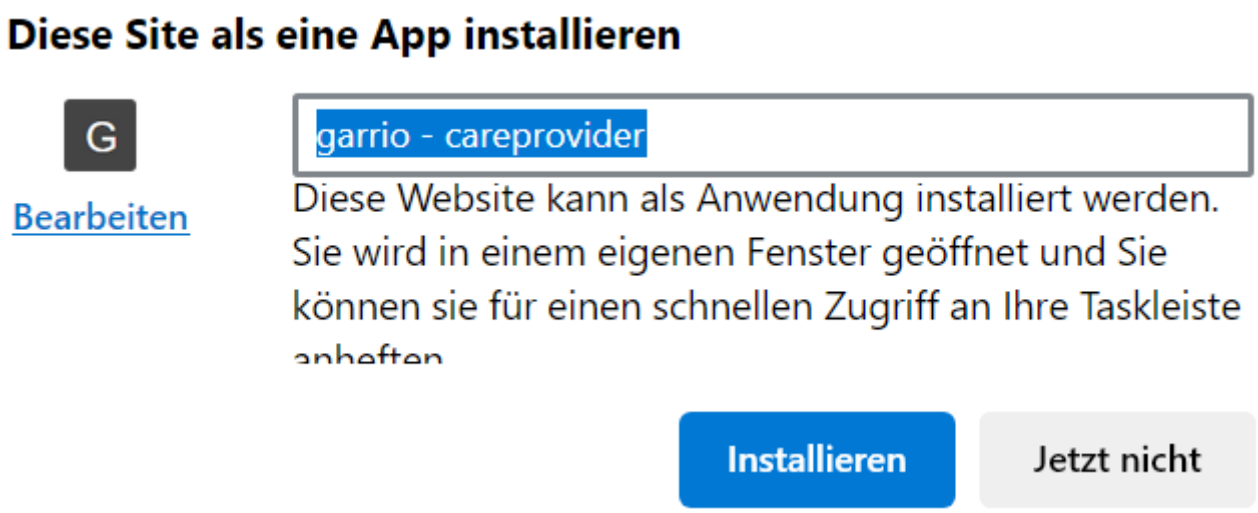
Edge Browser

Wenn Sie den **garrioCOM Messenger** zur Taskleiste hinzufügen möchten, gehen Sie bitte wie folgt vor:

- **Öffnen Sie den Microsoft Edge Browser**.
  Geben Sie in die Adressleiste **garrioCOM Careprovider** ein und rufen Sie die entsprechende Seite auf.

Klicken Sie auf die drei Punkte (. . .) oben rechts im Browserfenster.
(Hinweis: Diese befinden sich im rechten, oberen Bereich des Fensters.)

- Wählen Sie im Dropdown-Menü den Punkt
  (1) „Apps“ und anschließend
  (2) „Diese Seite als eine App installieren“ aus.
- Es erscheint ein Bestätigungsfenster.
  Klicken Sie auf **„Installieren“**, um die Seite als App zu installieren.
- Nach der Installation können Sie den Messenger an die Taskleiste anheften, indem Sie mit der rechten Maustaste auf das Symbol klicken und **„An Taskleiste anheften“** auswählen.



Meine Benutzerkonten werden nicht mehr angezeigt

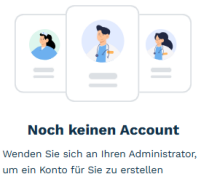
Beschreibung des Problems

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

Dies kann zwei verschiedene Ursachen haben:

1. Passiert dies immer nach dem Schließen des Browsers, so werden die für garrioCOM notwendigen Cookies automatisch gelöscht → Lösung "Ausnahme garrioCOM bei Cookie-Löschung"
2. Sollte der Browser so eingestellt sein, dass Cookies allgemein beibehalten werden oder bereits eine Ausnahme für garrioCOM besteht, so handelt es sich um ein anderes Problem → Lösung "Cookies löschen und erneut Browser aktivieren"





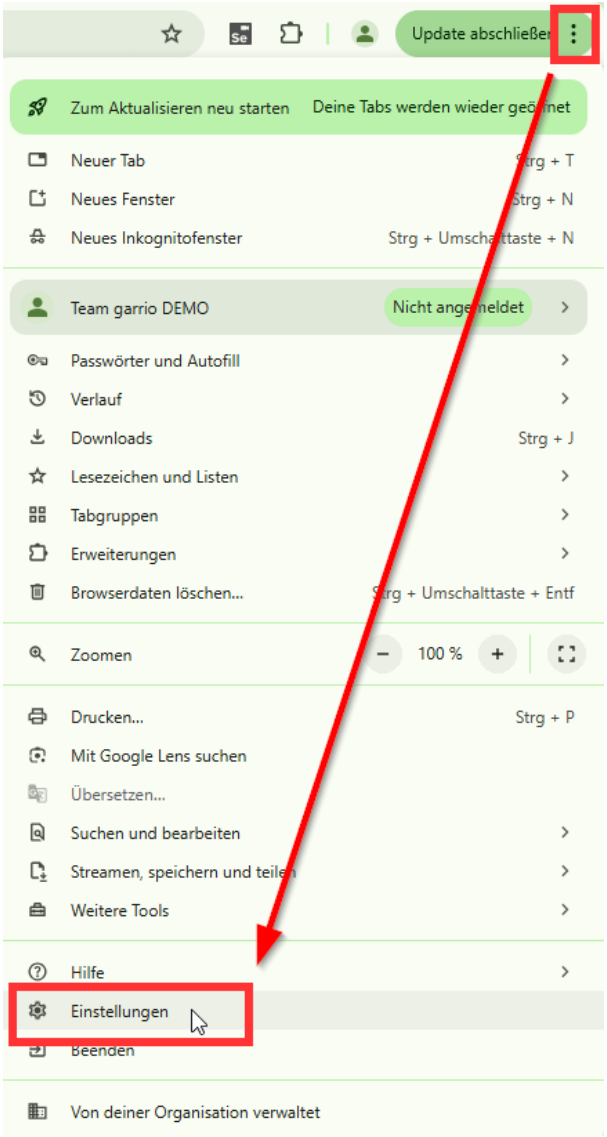
Lösung "Ausnahme garrioCOM bei Cookie-Löschung"

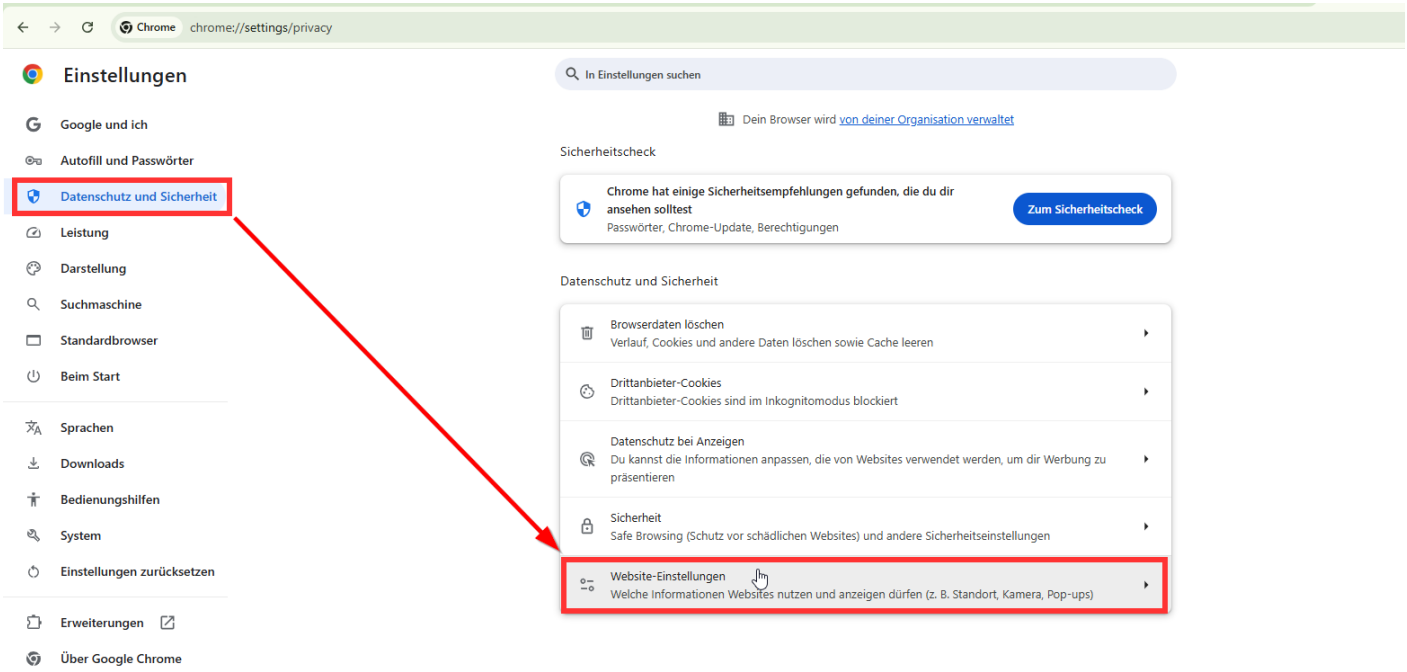
Stellen Sie Ihren Browser so ein, dass beim Schließen des Browsers keine Cookies gelöscht werden oder zumindest eine Ausnahme für garrioCOM gilt.

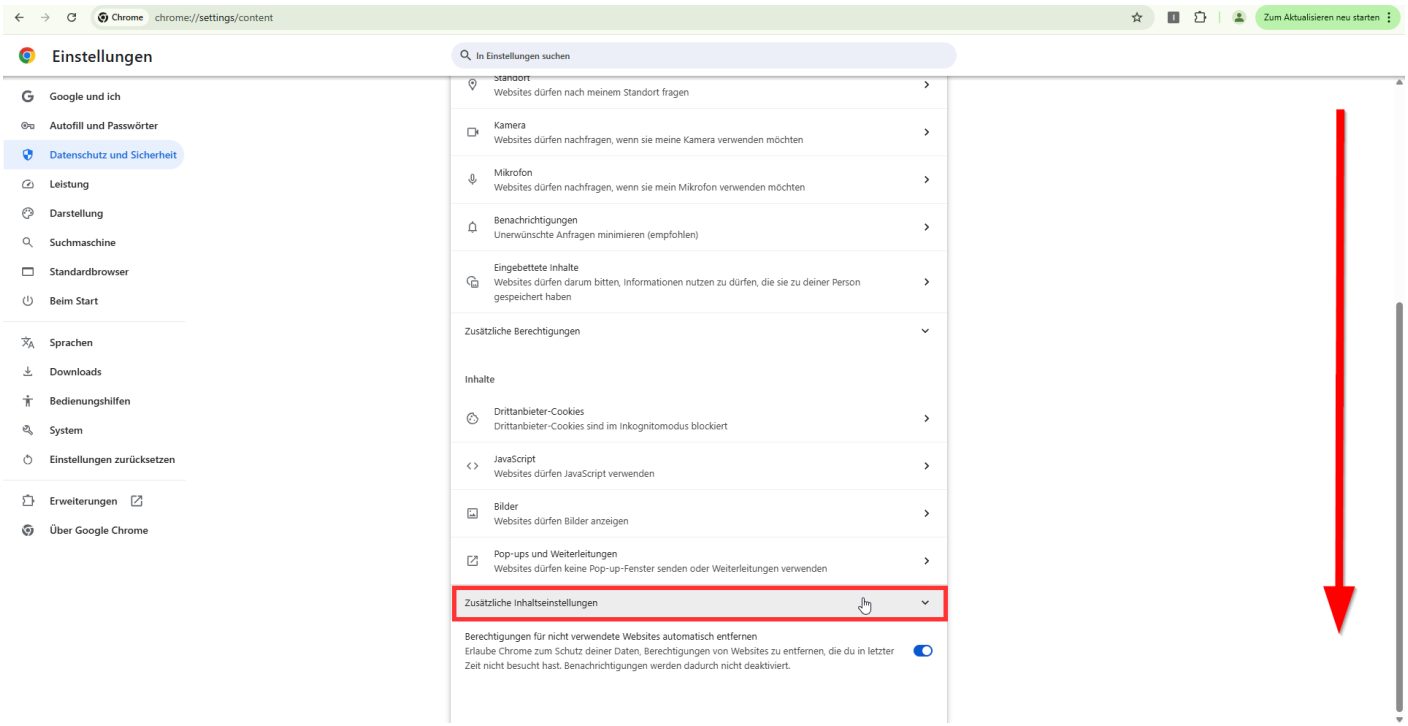
Einstellungen für Cookies mit Google Chrome

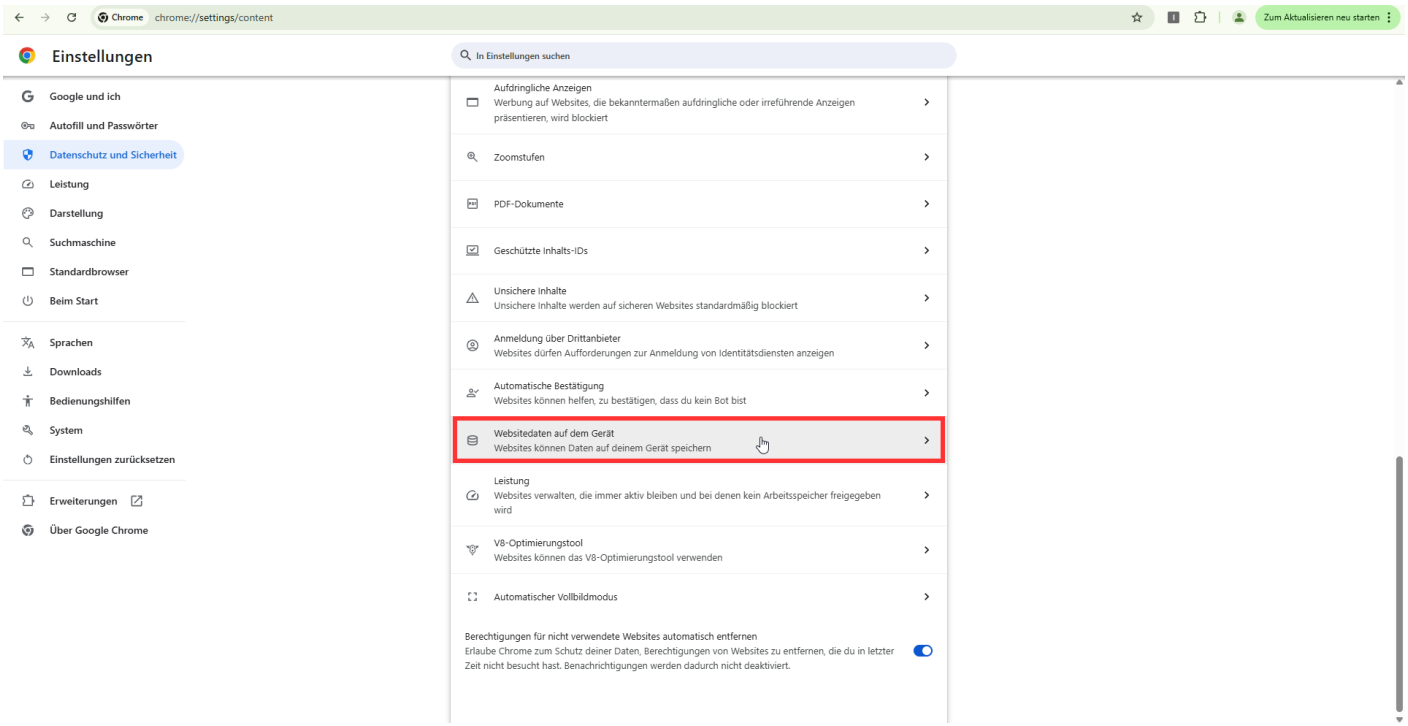
Öffnen Sie die Einstellungen des Browsers und gehen Sie wie abgebildet zu den Einstellungen für das Verhalten beim Schließen.

Alternativ können Sie auch direkt folgenden Link in Ihrem Chrome Browser eingeben, Sie gelangen dann direkt zu diesen Einstellungen: chrome://settings/content/siteData




Chrome
chrome://settings/privacy
Einstellungen
In Einstellungen suchen
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
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)

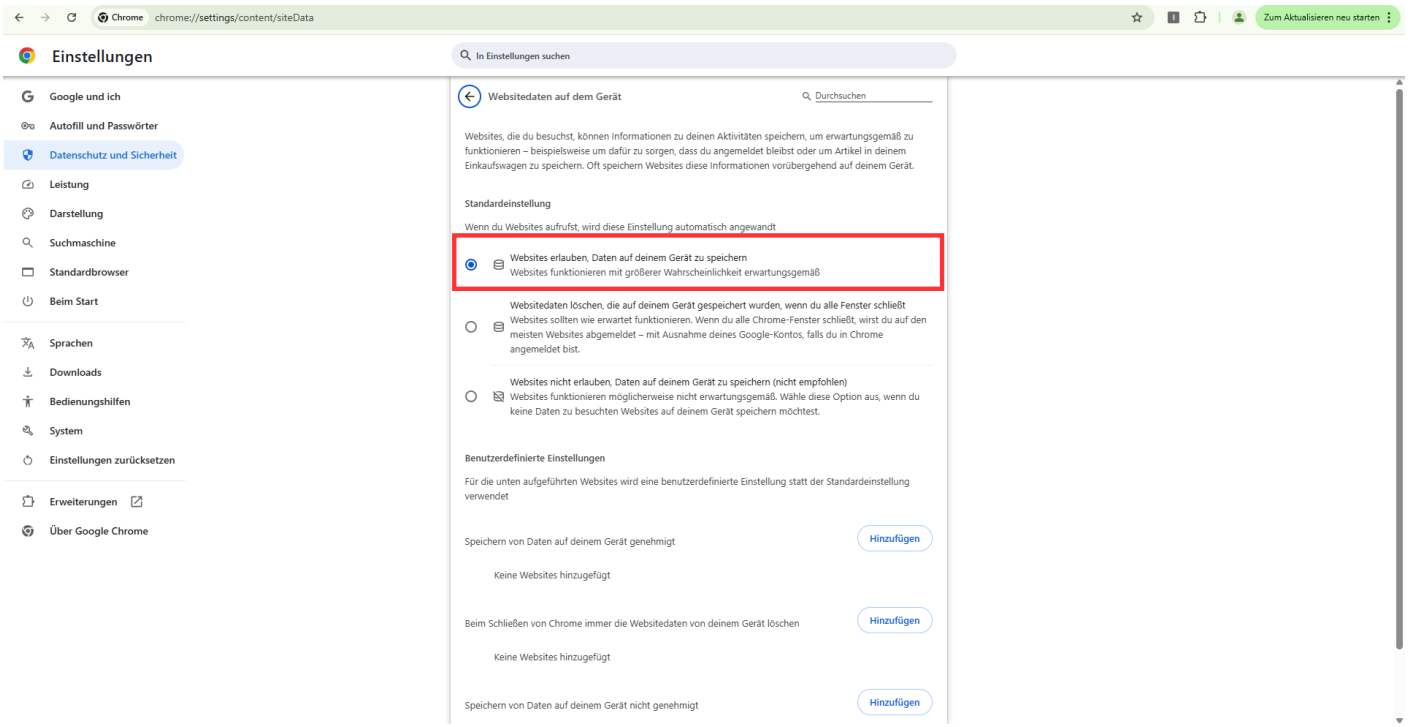

Chrome
chrome://settings/content
Zum Aktualisieren neu starten
Einstellungen
In Einstellungen suchen
Google und ich
Autofill und Passwörter
Datenschutz und Sicherheit
Leistung
Darstellung
Suchmaschine
Standardbrowser
Beim Start
Sprachen
Downloads
Bedienungshilfen
System
Einstellungen zurücksetzen
Erweiterungen
Über Google Chrome
Standort
Websites dürfen nach meinem Standort fragen
Kamera
Websites dürfen nachfragen, wenn sie meine Kamera verwenden möchten
Mikrofon
Websites dürfen nachfragen, wenn sie mein Mikrofon verwenden möchten
Benachrichtigungen
Unerwünschte Anfragen minimieren (empfohlen)
Eingebettete Inhalte
Websites dürfen darum bitten, Informationen nutzen zu dürfen, die sie zu deiner Person gespeichert haben
Zusätzliche Berechtigungen
Inhalte
Drittanbieter-Cookies
Drittanbieter-Cookies sind im Inkognitomodus blockiert
JavaScript
Websites dürfen JavaScript verwenden
Bilder
Websites dürfen Bilder anzeigen
Pop-ups und Weiterleitungen
Websites dürfen keine Pop-up-Fenster senden oder Weiterleitungen verwenden
Zusätzliche Inhaltseinstellungen
Berechtigungen für nicht verwendete Websites automatisch entfernen
Erlaube Chrome zum Schutz deiner Daten, Berechtigungen von Websites zu entfernen, die du in letzter Zeit nicht besucht hast. Benachrichtigungen werden dadurch nicht deaktiviert.



Cookies dauerhaft beibehalten

Mit dieser Einstellung werden alle Cookies dauerhaft vom Browser auf Ihrem Gerät gespeichert.

Wenn Sie folgenden Link in Ihrem Chrome Browser eingeben, gelangen Sie direkt zu diesen Einstellungen: chrome://settings/content/siteData.



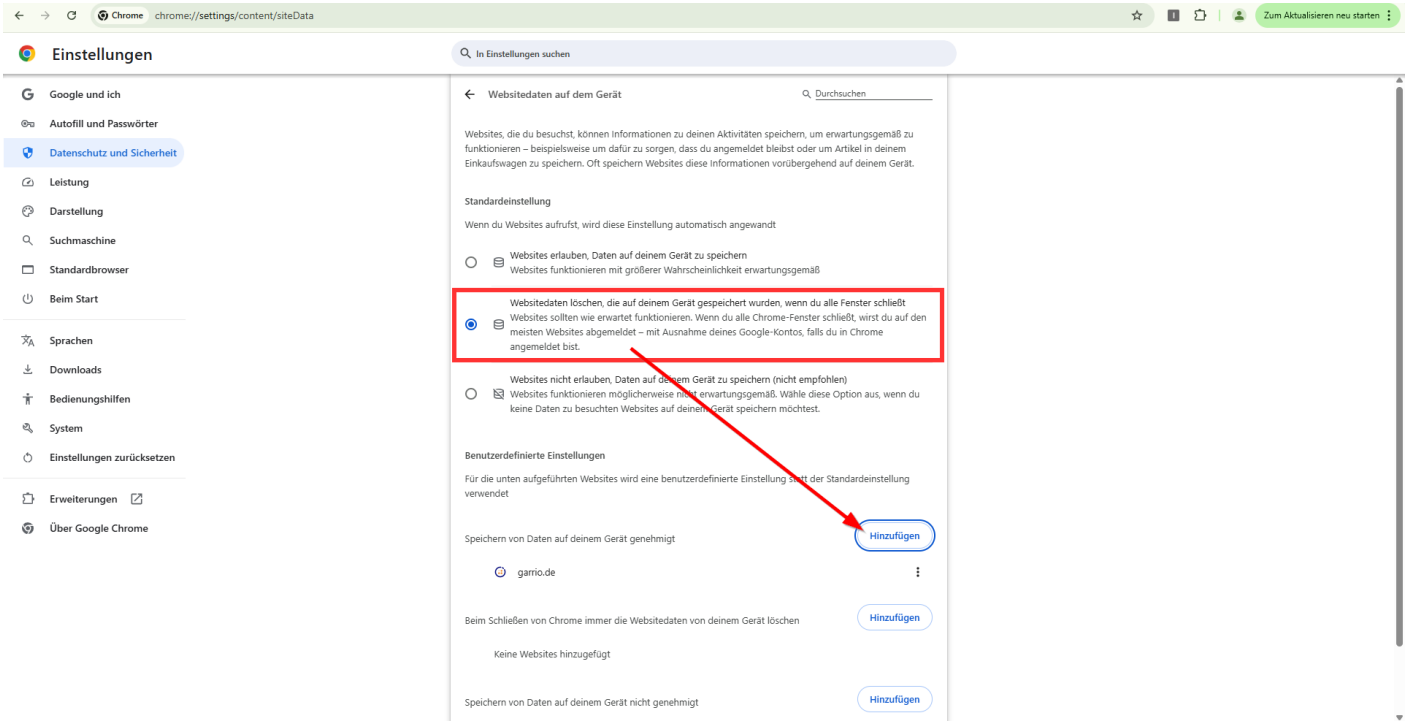
Ausnahme für garrioCOM einrichten

Mit dieser Einstellung werden Cookies beim Schließen des Chrome Browsers gelöscht, mit Ausnahme der eingestellten (hier: garrioCOM).

Dazu müssen Sie mittels des "Hinzufügen"-Buttons "**garrio.de**" (ohne Anführungszeichen) hinzufügen.

Die Einstellungen sind sofort gespeichert und wirksam.

Wenn Sie folgenden Link in Ihrem Chrome Browser eingeben, gelangen Sie direkt zu diesen Einstellungen: chrome://settings/content/siteData.

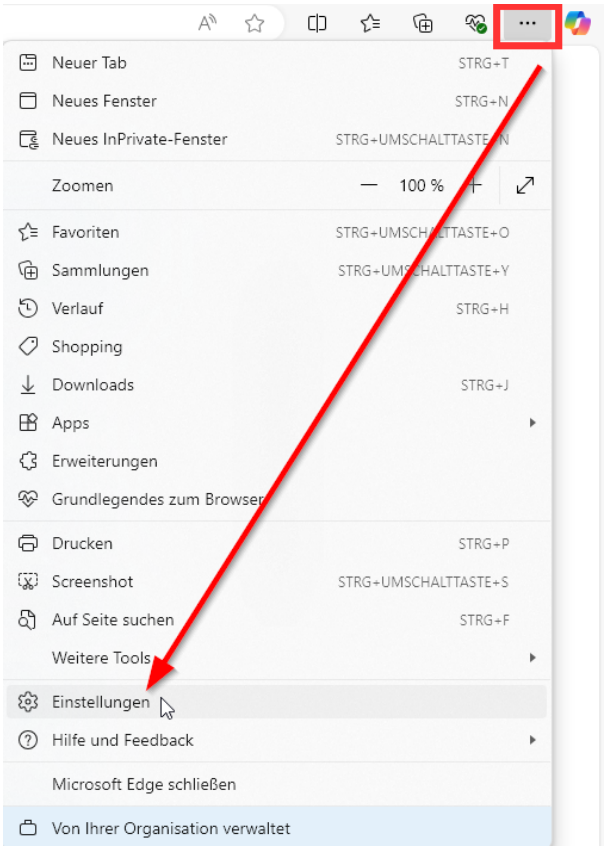


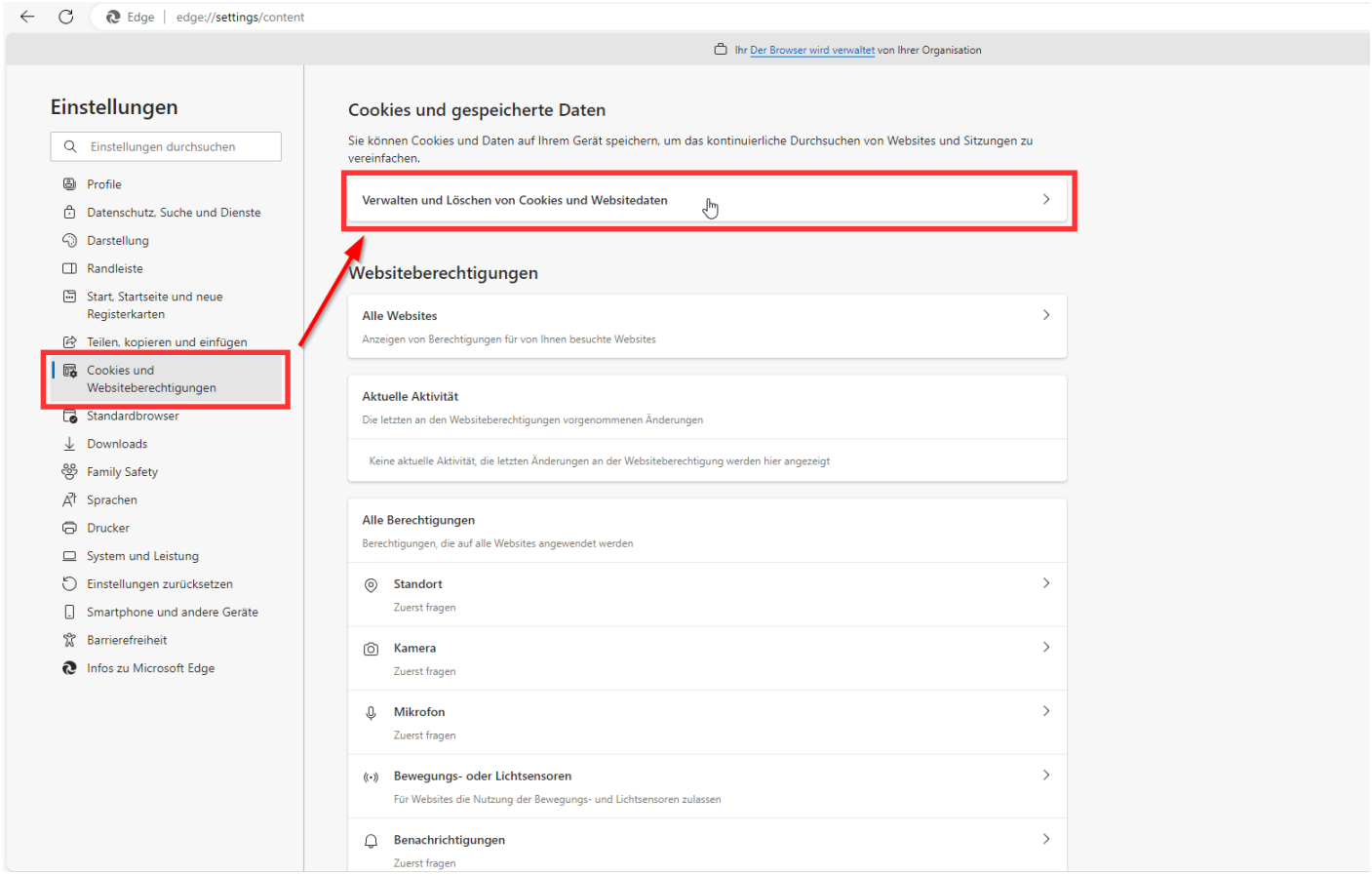
Lösung "Cookies löschen und Browser erneut aktivieren"

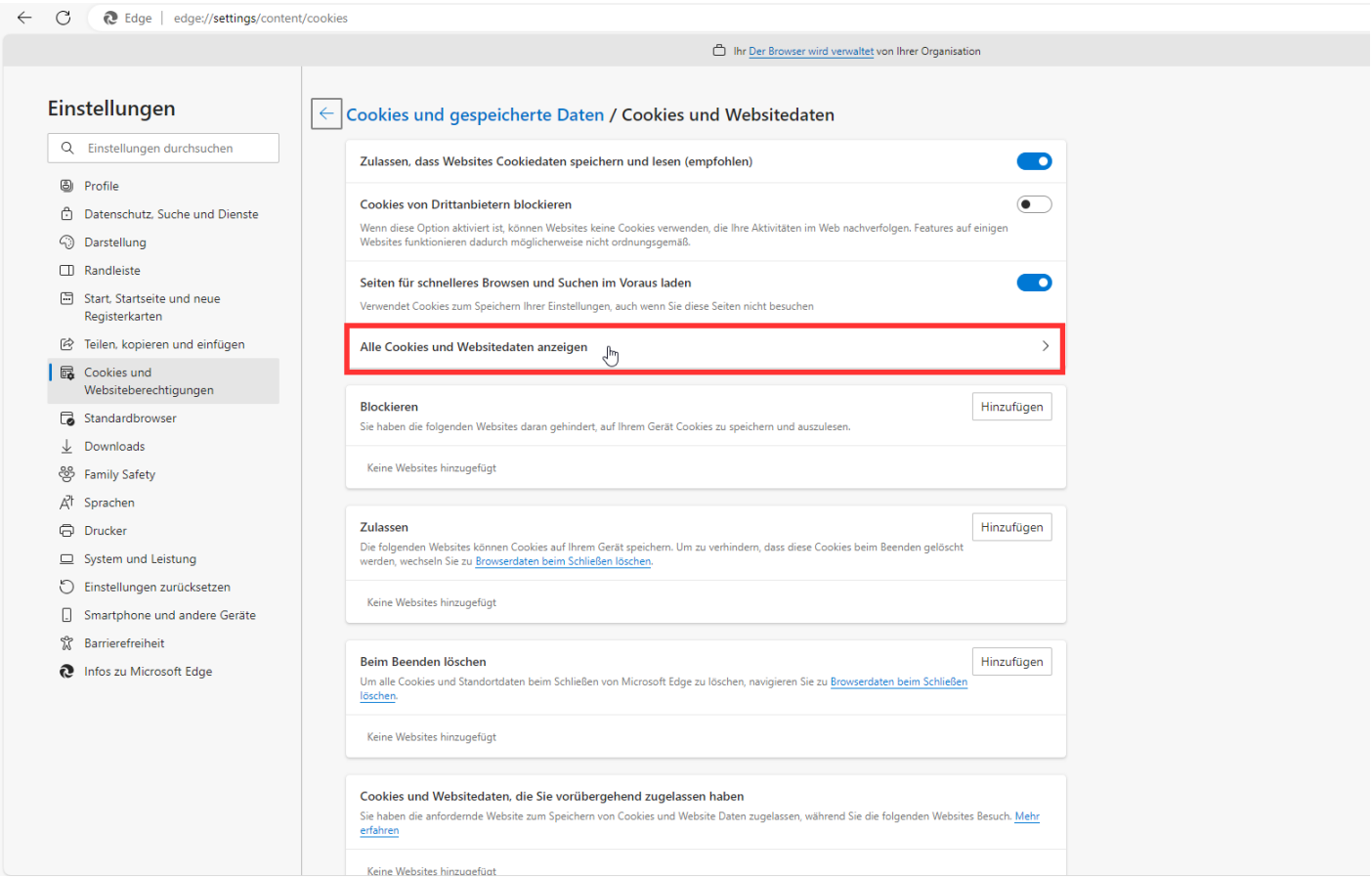
Löschen Sie zunächst die Cookies in Ihrem Browser und aktivieren Sie den Browser dann wieder mittels Magischem Link.

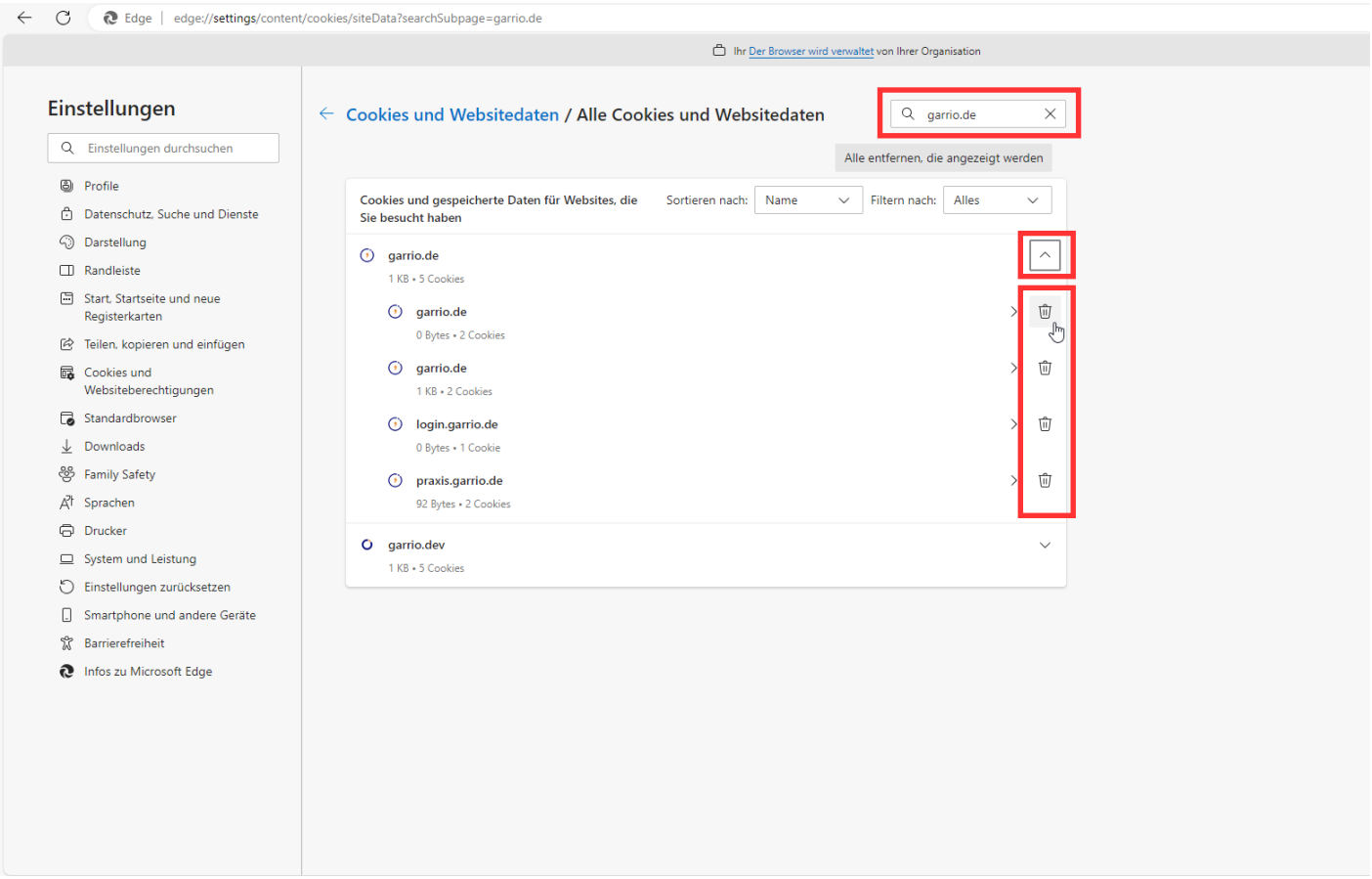
Cookies löschen mit Microsoft Edge

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


Neuer Tab STRG+T
Neues Fenster STRG+N
Neues InPrivate-Fenster STRG+UMSCHALTTASTE+N
Zoomen 100 %
Favoriten STRG+UMSCHALTTASTE+O
Sammlungen STRG+UMSCHALTTASTE+Y
Verlauf STRG+H
Shopping
Downloads STRG+J
Apps
Erweiterungen
Grundlegendes zum Browser
Drucken STRG+P
Screenshot STRG+UMSCHALTTASTE+S
Auf Seite suchen STRG+F
Weitere Tools
Einstellungen
Hilfe und Feedback
Microsoft Edge schließen
Von Ihrer Organisation verwaltet


Edge | edge://settings/content
Ihr Der Browser wird verwaltet von Ihrer Organisation
Einstellungen
Einstellungen durchsuchen
Profile
Datenschutz, Suche und Dienste
Darstellung
Randleiste
Start, Startseite und neue Registerkarten
Teilen, kopieren und einfügen
Cookies und Websiteberechtigungen
Standardbrowser
Downloads
Family Safety
Sprachen
Drucker
System und Leistung
Einstellungen zurücksetzen
Smartphone und andere Geräte
Barrierefreiheit
Infos zu Microsoft Edge
Cookies und gespeicherte Daten
Sie können Cookies und Daten auf Ihrem Gerät speichern, um das kontinuierliche Durchsuchen von Websites und Sitzungen zu vereinfachen.
Verwalten und Löschen von Cookies und Websitedaten
Websiteberechtigungen
Alle Websites
Anzeigen von Berechtigungen für von Ihnen besuchte Websites
Aktuelle Aktivität
Die letzten an den Websiteberechtigungen vorgenommenen Änderungen
Keine aktuelle Aktivität, die letzten Änderungen an der Websiteberechtigung werden hier angezeigt
Alle Berechtigungen
Berechtigungen, die auf alle Websites angewendet werden
Standort
Zuerst fragen
Kamera
Zuerst fragen
Mikrofon
Zuerst fragen
Bewegungs- oder Lichtsensoren
Für Websites die Nutzung der Bewegungs- und Lichtsensoren zulassen
Benachrichtigungen
Zuerst fragen



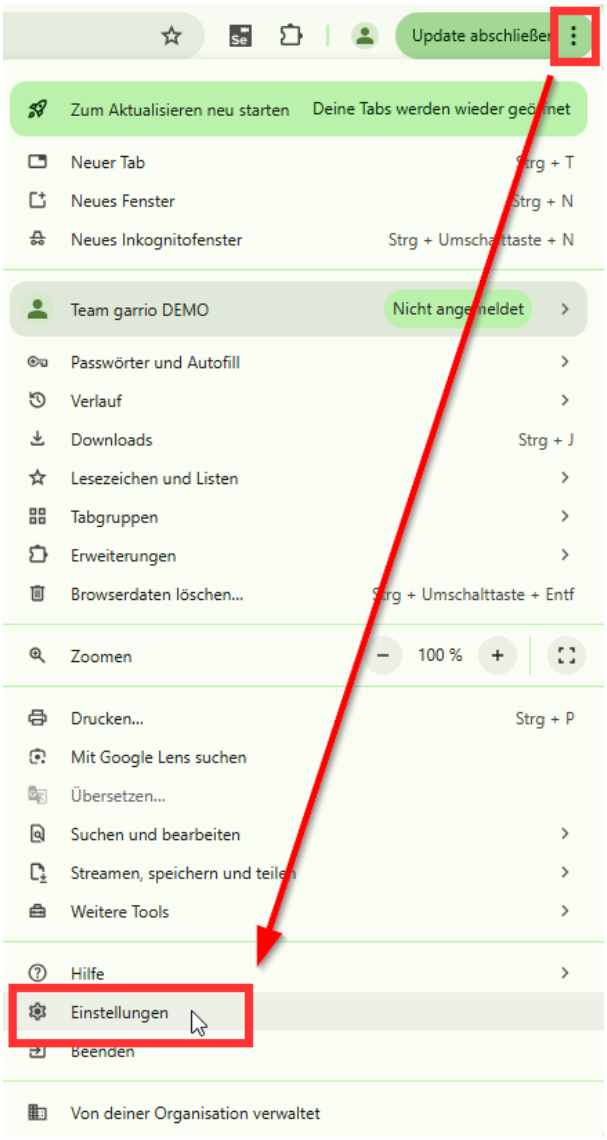


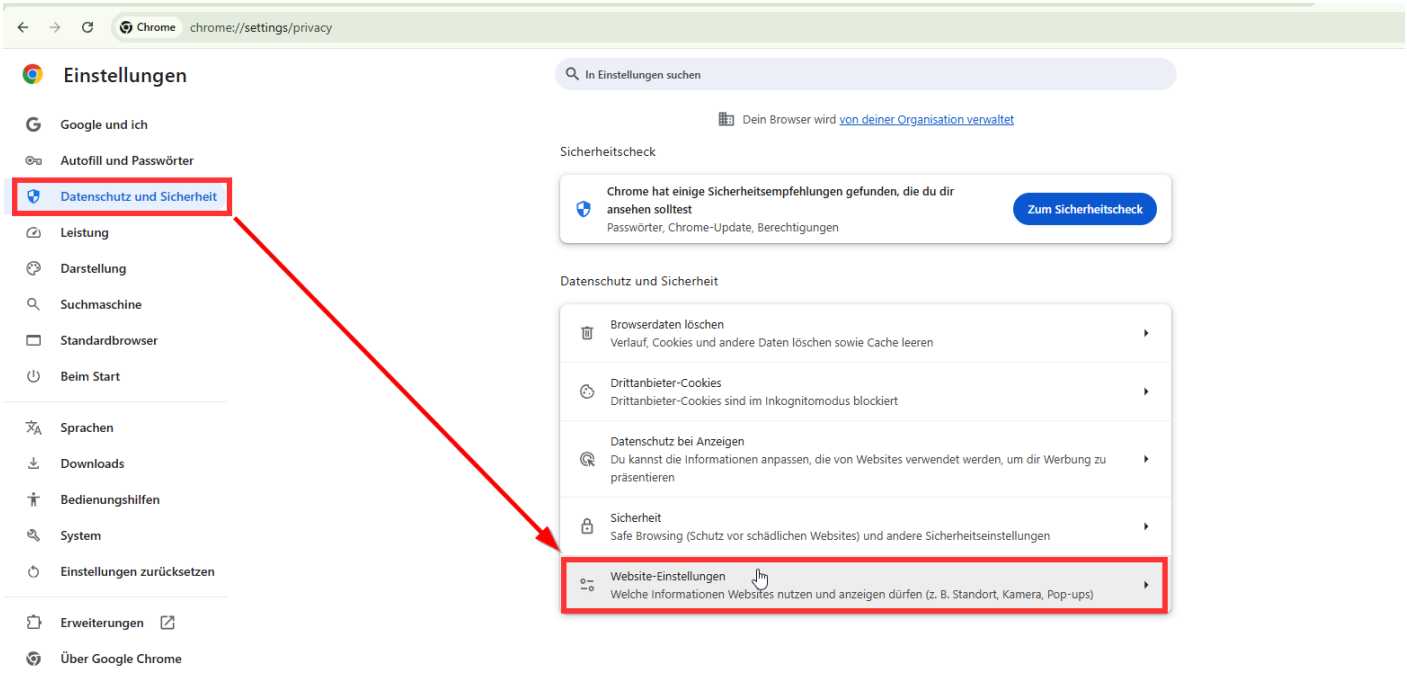
Alternativ können Sie auch direkt folgenden Link in Ihrem Edge Browser eingeben, Sie gelangen dann direkt zu diesen Einstellungen:

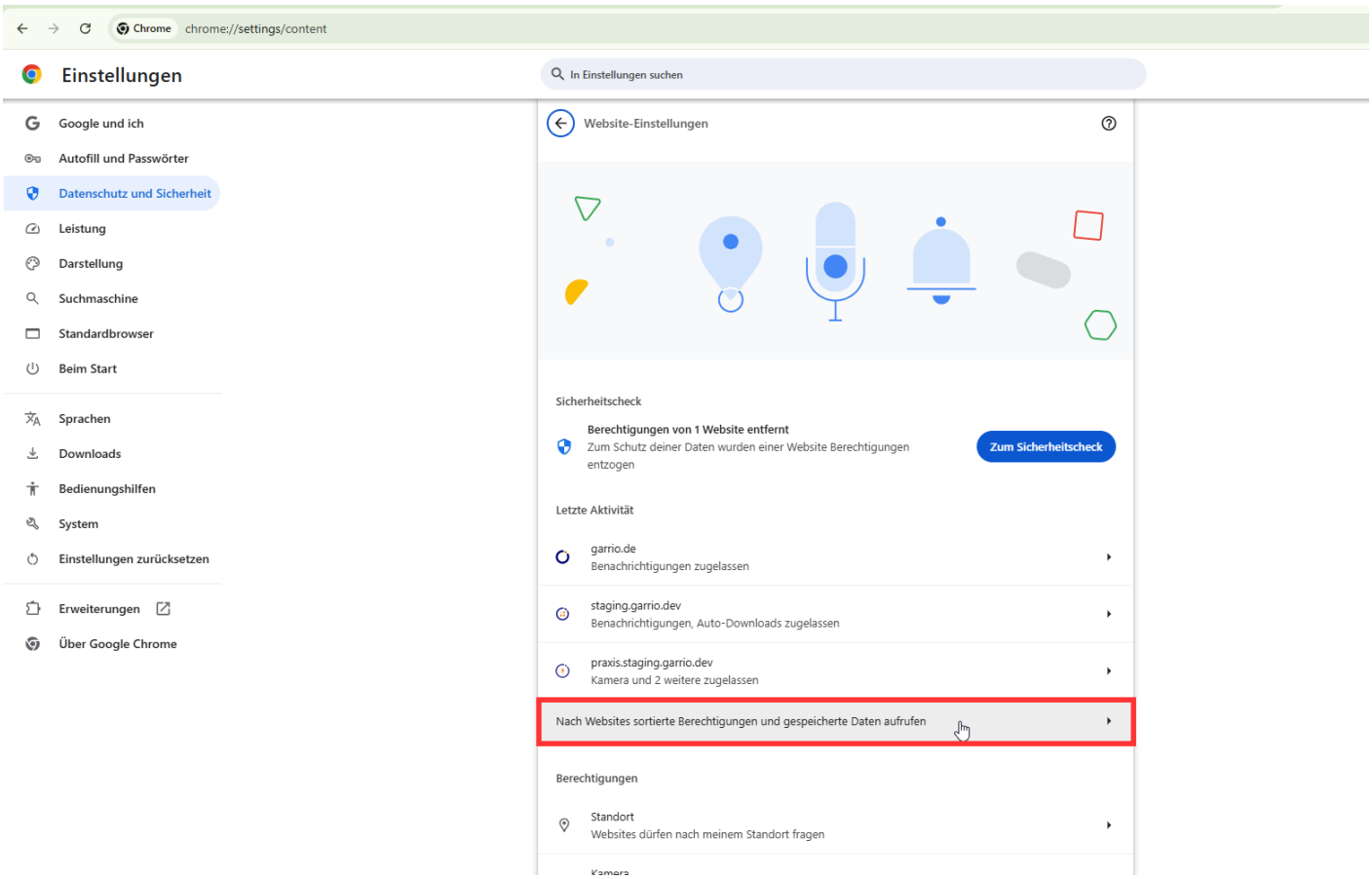
edge://settings/content/cookies/siteData?searchSubpage=garrio.de

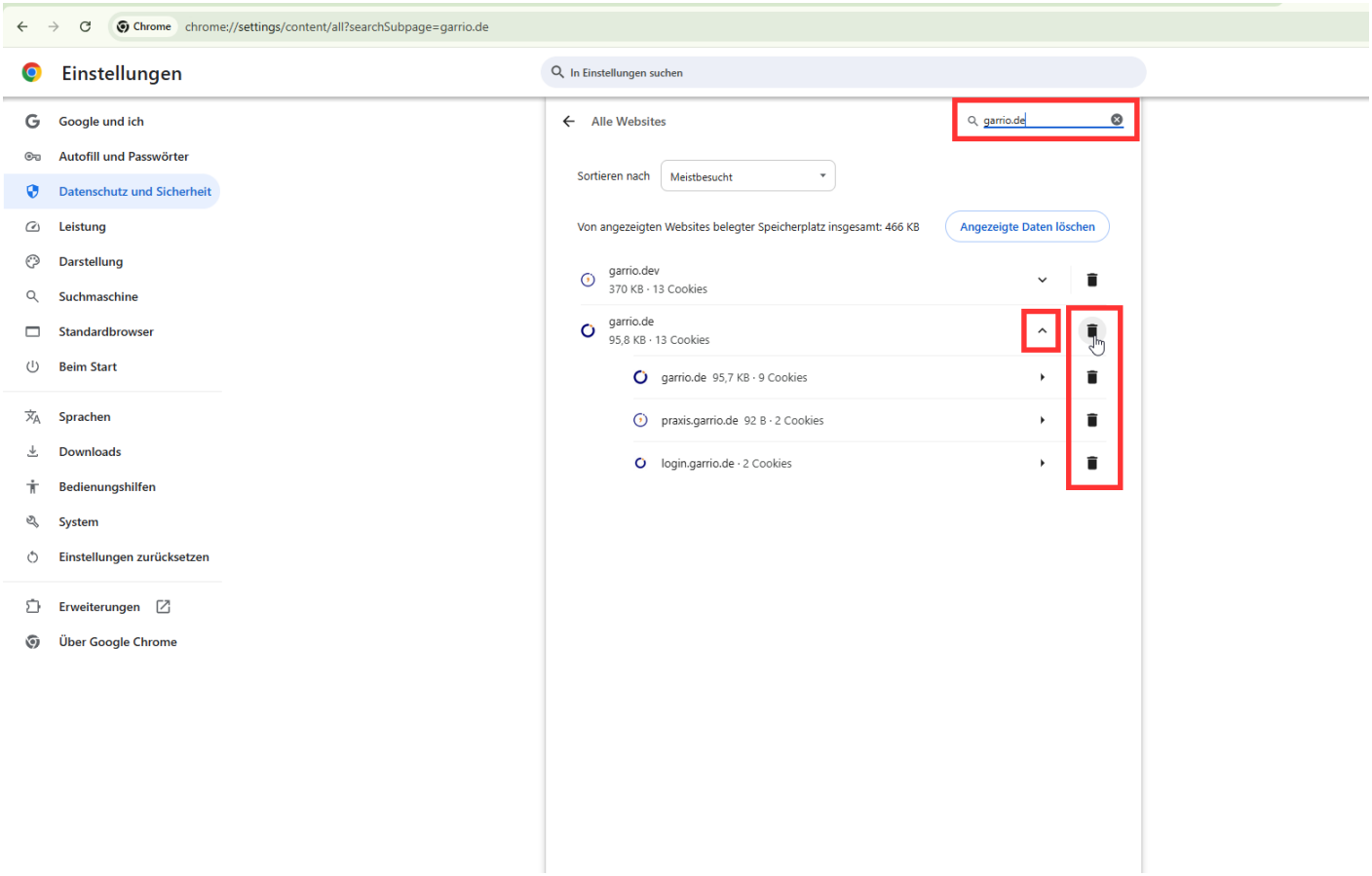
Hier löschen Sie alle zu den Seiten garrio.de, login.garrio.de, praxis.garrio.de und ggf. admin.garrio.de angezeigten Cookies.

Cookies löschen mit Google Chrome




Chrome
chrome://settings/privacy
Einstellungen
In Einstellungen suchen
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
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
In Einstellungen suchen
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
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

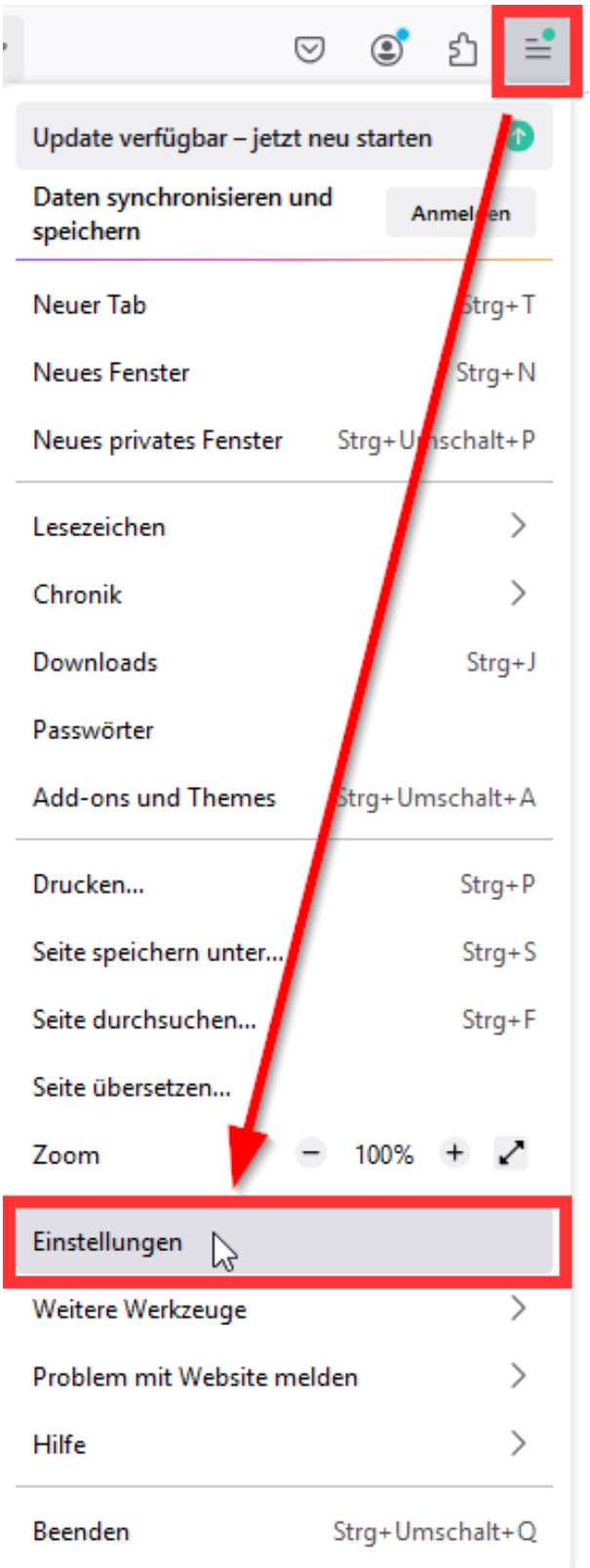


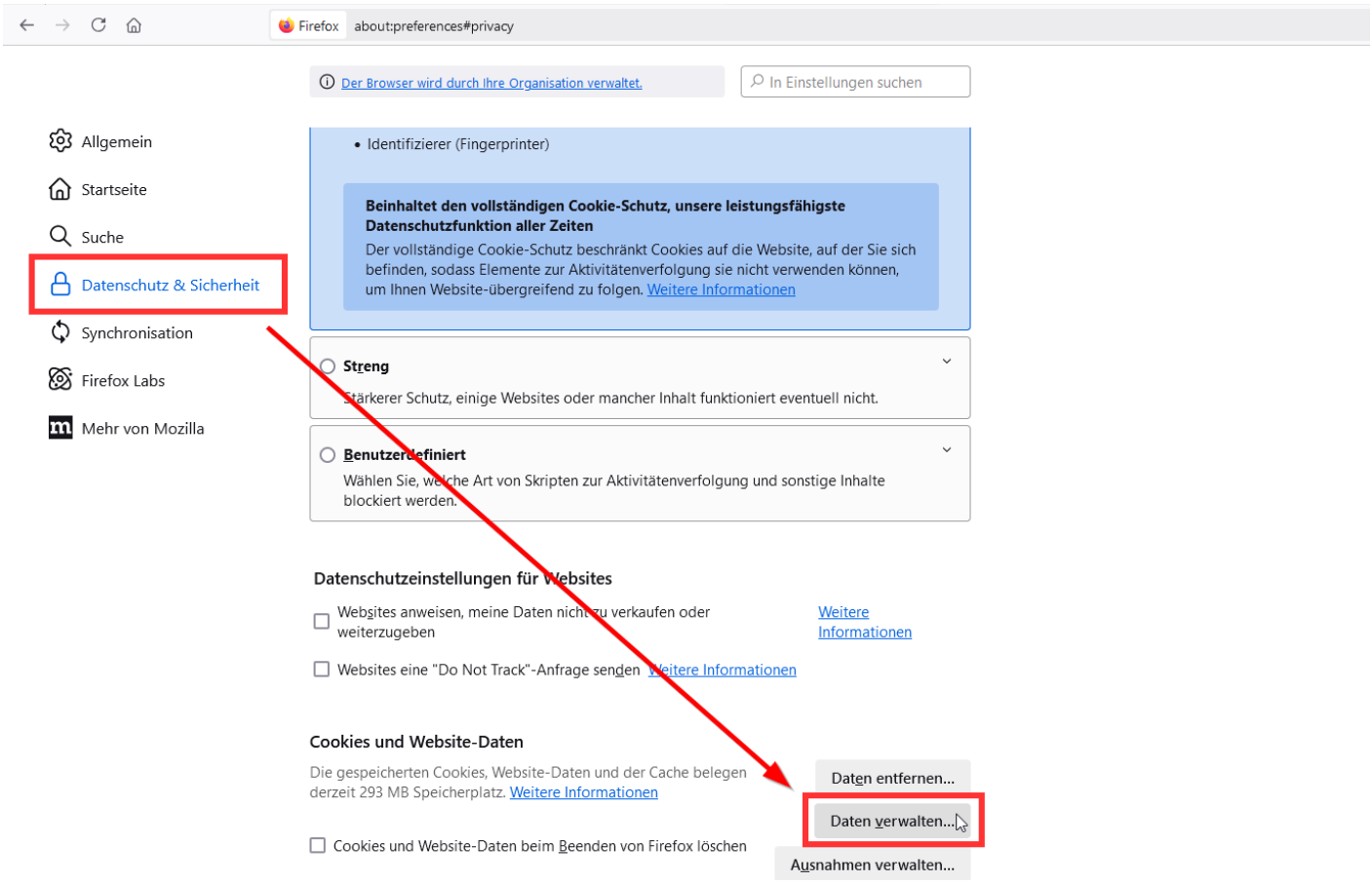
Alternativ können Sie auch direkt folgenden Link in Ihrem Chrome Browser eingeben, Sie gelangen dann direkt zu diesen Einstellungen:

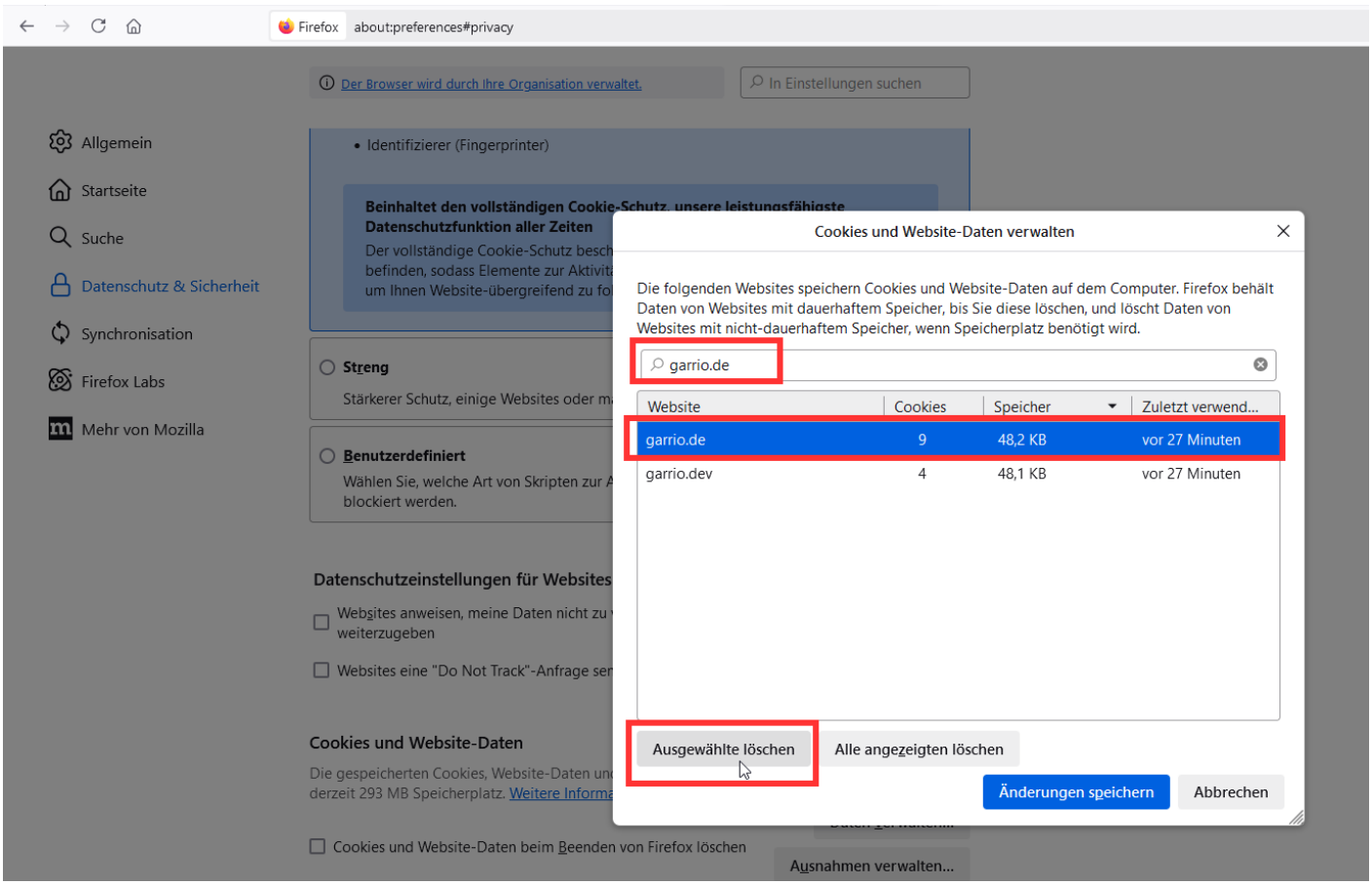
chrome://settings/content/all?searchSubpage=garrio.de

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


Update verfügbar – jetzt neu starten
Daten synchronisieren und speichern
Anmelden
Neuer Tab Strg+T
Neues Fenster Strg+N
Neues privates Fenster Strg+Umschalt+P
Lesezeichen
Chronik
Downloads Strg+J
Passwörter
Add-ons und Themes Strg+Umschalt+A
Drucken... Strg+P
Seite speichern unter... Strg+S
Seite durchsuchen... Strg+F
Seite übersetzen...
Zoom 100%
Einstellungen
Weitere Werkzeuge
Problem mit Website melden
Hilfe
Beenden Strg+Umschalt+Q





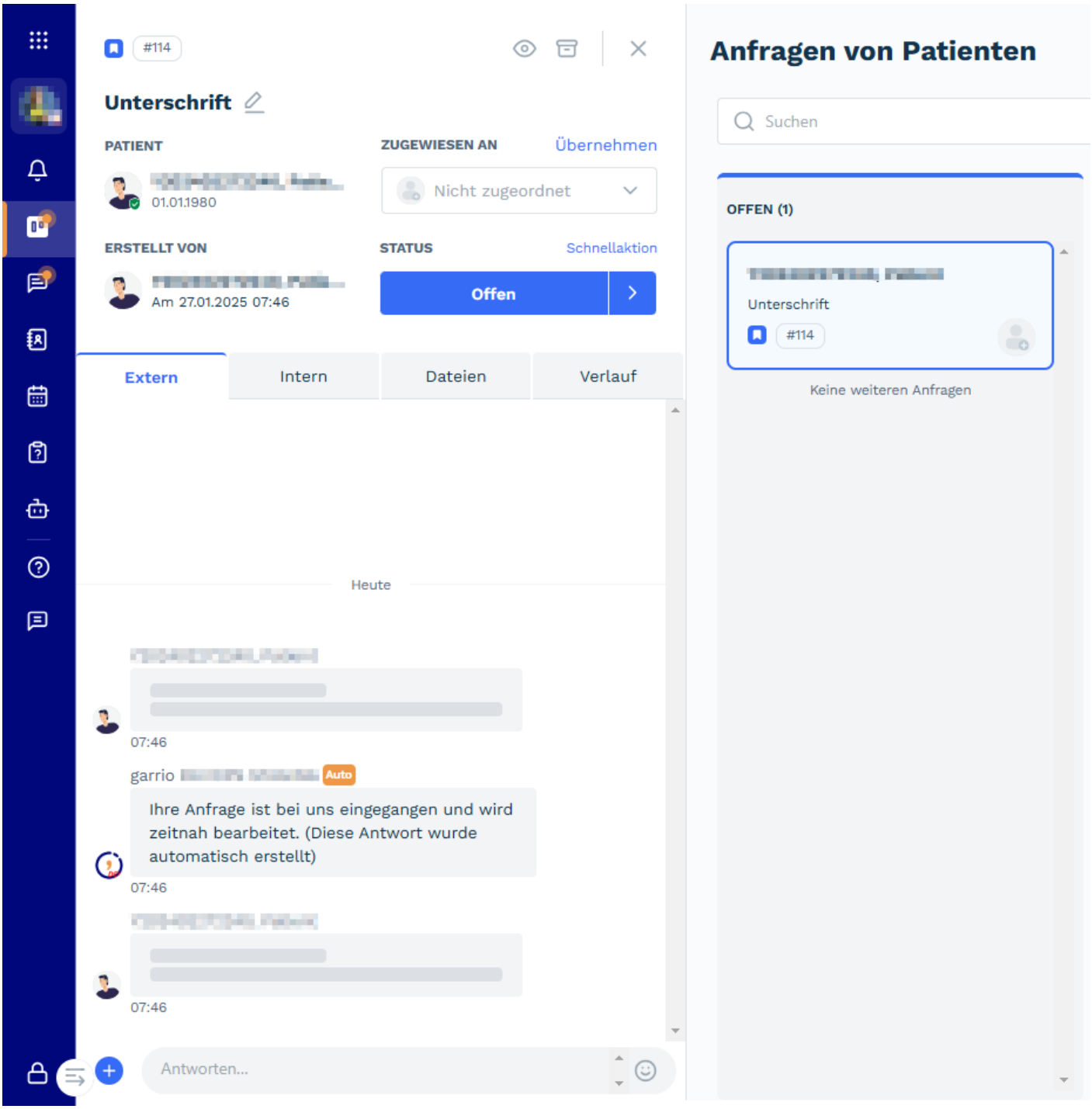
Browser erneut aktivieren

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.



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:

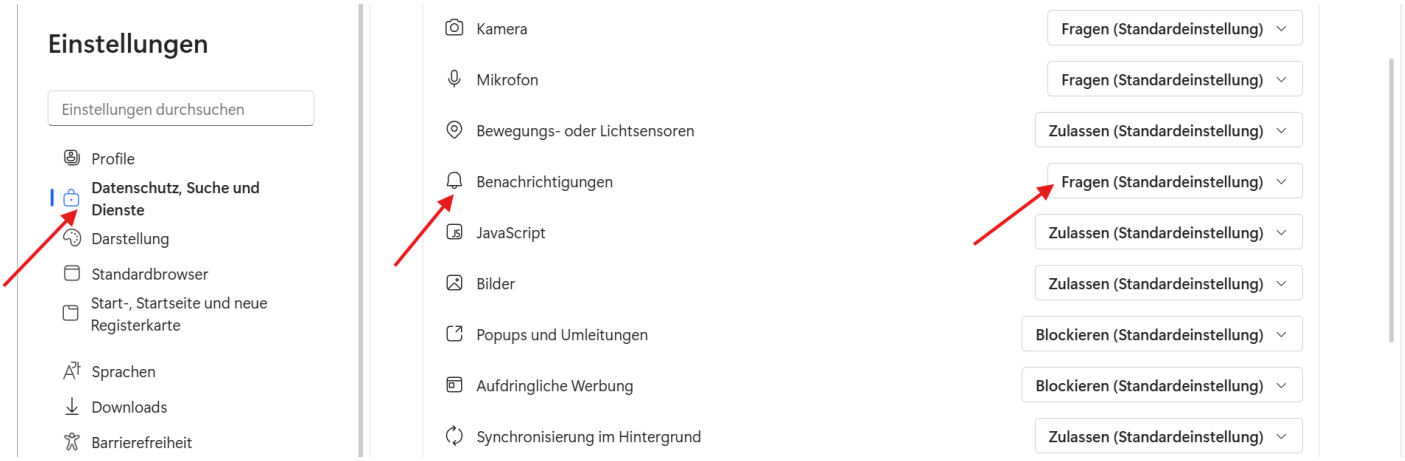
□ Bestätigen Sie eventuelle Sicherheitsabfragen mit **„Ja“** oder **„Zulassen“**.
□ Das TeamViewer-Fenster öffnet sich.
□ Teilen Sie unserem Support die **ID** und das **Passwort** mit, die im Fenster angezeigt werden.

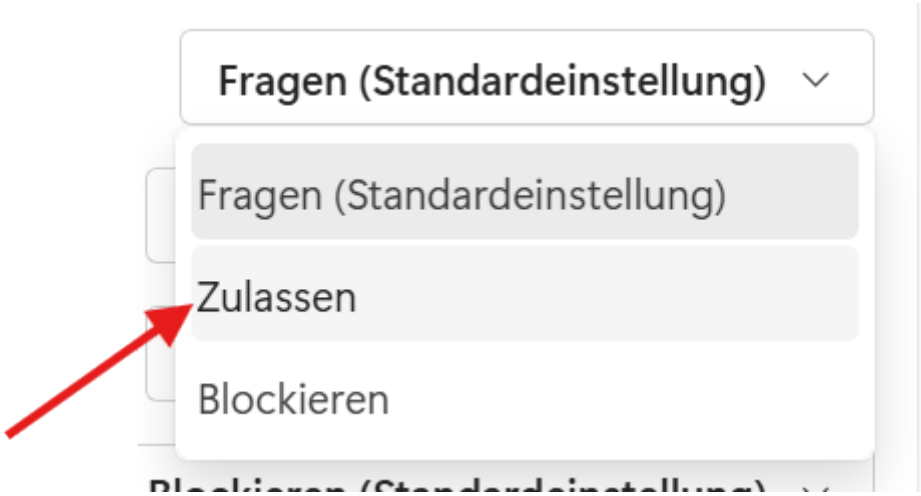
□□ Rufen Sie uns an oder senden Sie die Daten per E-Mail, damit wir Ihnen helfen können!

Benachrichtigungsanzeigen für garrioCOM aktivieren/ deaktivieren (Browserbezogen)

□□ Microsoft Edge

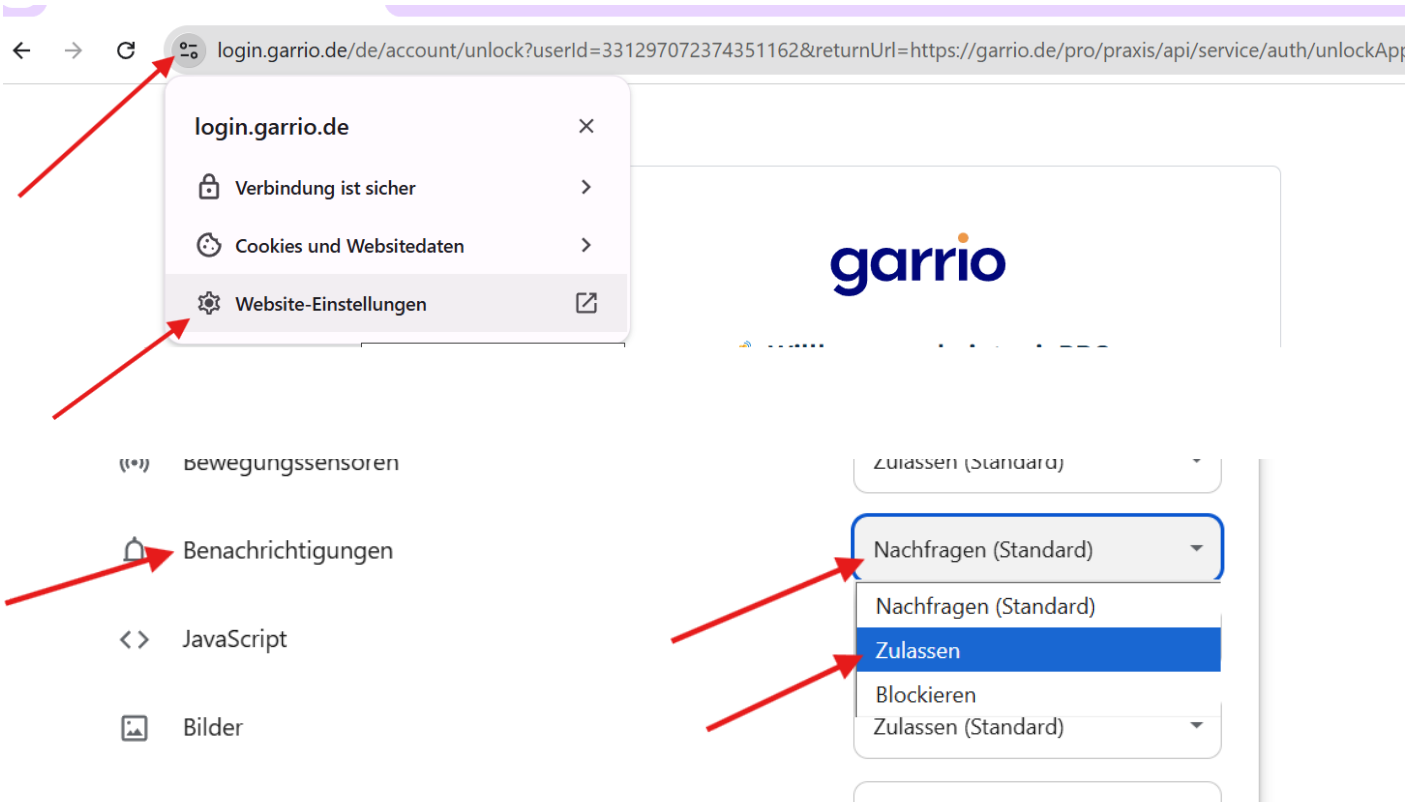
1. Besuchen Sie die gewünschte Website.
2. Klicken Sie links in der Adressleiste auf das **Schloss-Symbol** □□.
3. Wählen Sie **„Websiteberechtigungen“**.
4. Scrollen Sie zu **„Benachrichtigungen“**.
5. Wählen Sie aus: **Zulassen**, **Blockieren** oder **Standard**.





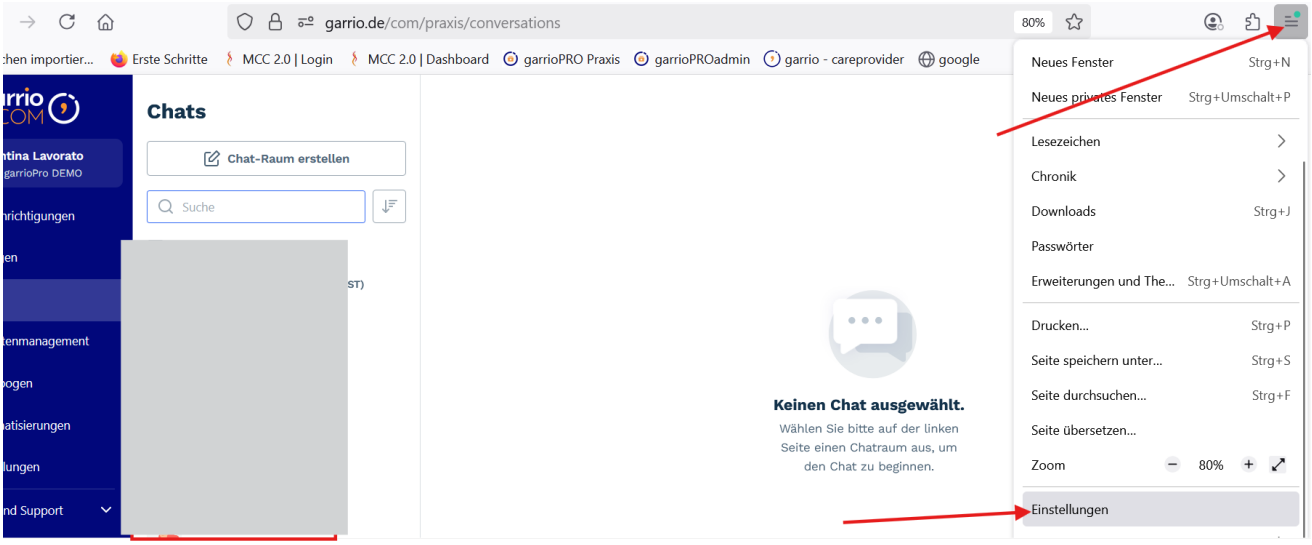
Google Chrome

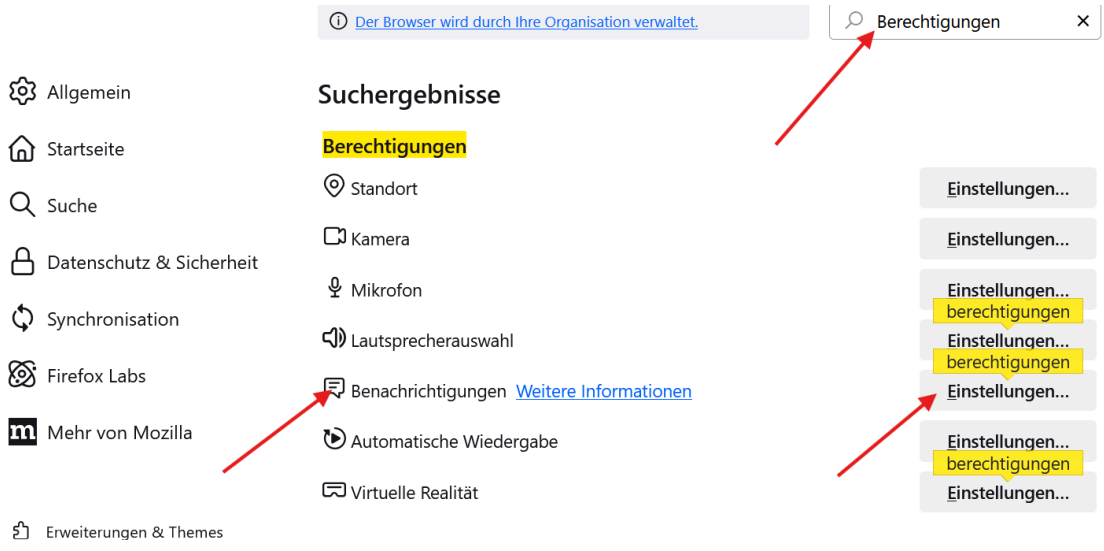
1. Öffnen Sie die gewünschte Website.
2. Klicken Sie links in der Adressleiste auf das **Schloss-Symbol** .
3. Wählen Sie **„Website-Einstellungen“** oder **„Websiteinformationen“**.
4. Sie werden zu einer Übersichtsseite weitergeleitet.
5. Suchen Sie den Eintrag **„Benachrichtigungen“**.
6. Wählen Sie aus: **Zulassen**, **Blockieren** oder **Standard**.

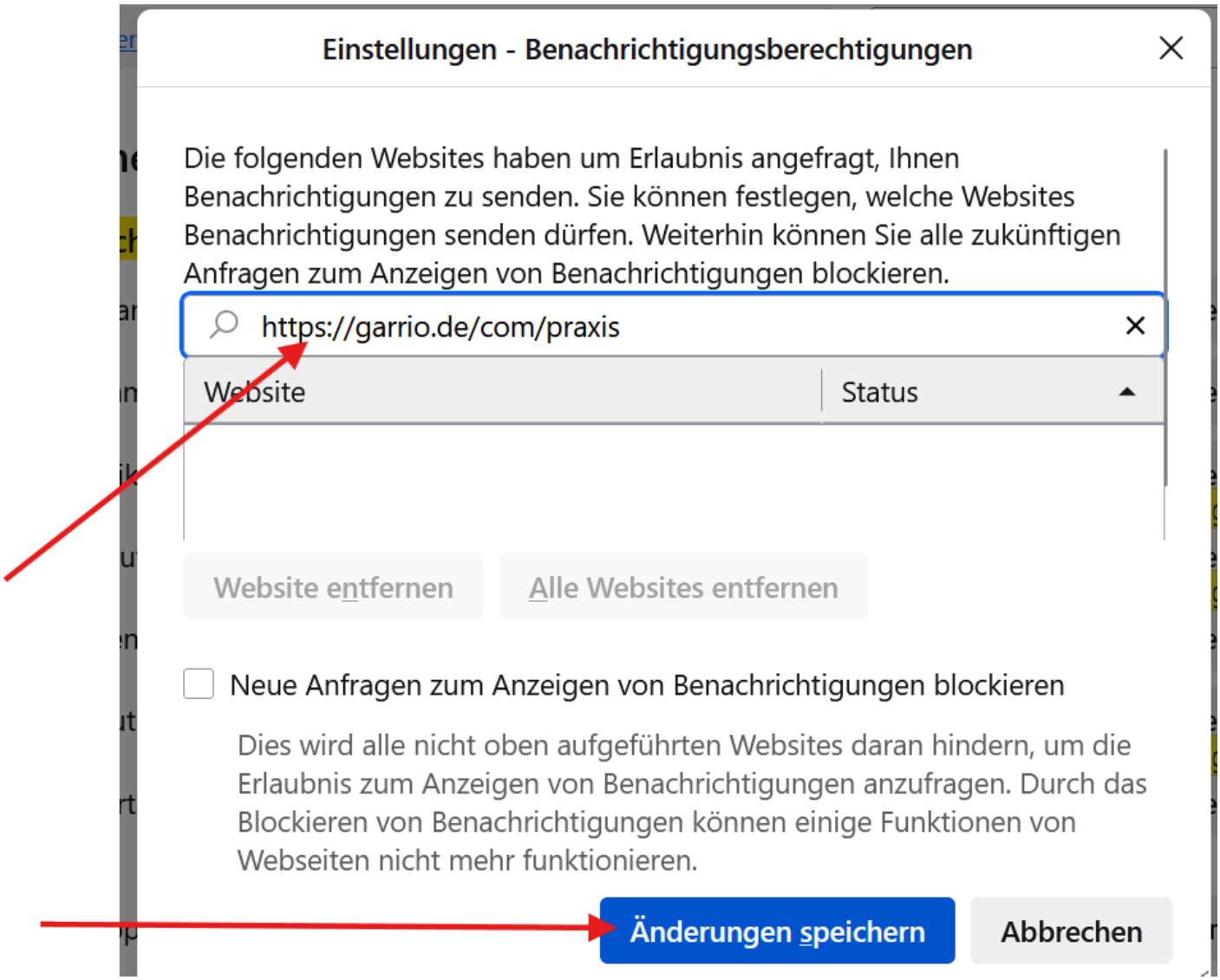


Mozilla Firefox

1. Besuchen Sie die betreffende Website.
2. Klicken Sie rechts auf die **drei Striche** ☰ .
3. Klicken Sie auf **„Berechtigungen“** oder **„Weitere Informationen“**.
4. Fügen Sie in die Leiste den Link der **garrioCOM Website** ein
5. Speichern Sie die Einstellung ab.






Einstellungen - Benachrichtigungsberechtigungen
Die folgenden Websites haben um Erlaubnis angefragt, Ihnen Benachrichtigungen zu senden. Sie können festlegen, welche Websites Benachrichtigungen senden dürfen. Weiterhin können Sie alle zukünftigen Anfragen zum Anzeigen von Benachrichtigungen blockieren.
https://garrio.de/com/praxis
Website
Status
Website entfernen
Alle Websites entfernen
Neue Anfragen zum Anzeigen von Benachrichtigungen blockieren
Dies wird alle nicht oben aufgeführten Websites daran hindern, um die Erlaubnis zum Anzeigen von Benachrichtigungen anzufragen. Durch das Blockieren von Benachrichtigungen können einige Funktionen von Webseiten nicht mehr funktionieren.
Änderungen speichern
Abbrechen

Passwort vergessen

Keine Zurücksetzung des Passworts möglich

Bitte beachten Sie, dass eine Zurücksetzung des Passworts nicht möglich ist. Aus Sicherheitsgründen speichern wir keine Passwörter, sodass wir auch keinen Zugriff darauf haben und diese nicht für Sie zurücksetzen können.
Sollten Sie Ihr Passwort vergessen haben, ist ein Zugriff auf Ihr bestehendes Profil leider nicht mehr möglich. In diesem Fall muss ein neues Profil erstellt werden.