

# ***DO! NOT! TRACK!***

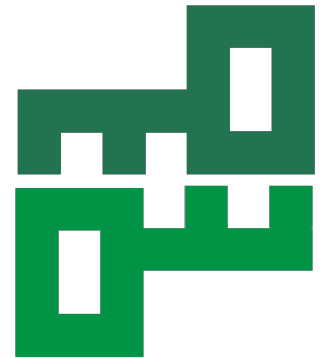
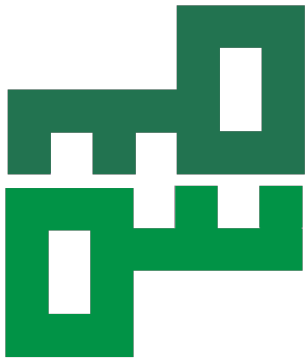
*Workshop for Firefox*

Anton, **Cryptoparty Graz**

CC BY-NC-SA 4.0 (w/o product logos)

2015-04-25

**Linuxtage Graz, FH Joanneum**



**Anton**

[PGP-key and Fingerprint](#)

2048R, 2014-02-27

A727 CC1E 08AD F9F3 9C43

E650 BFE1 E2F8 8AF5 A989

# New Firefox profile for playing around

→ *If you crash something ... :-)*

## Windows

{Windows-key + R}, “firefox.exe -p”

path:

C:\Users\USER\AppData\Roaming\Mozilla\Firefox\Profiles

## Linux

Open terminal,

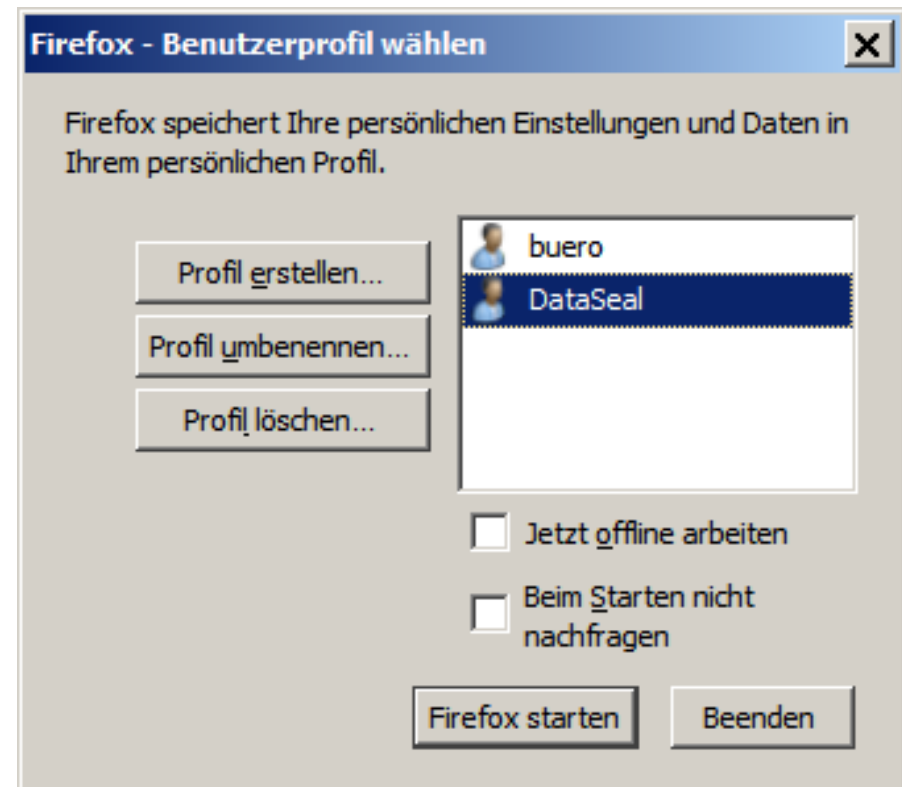
run “firefox -p”

path: /home/USER/.mozilla/firefox

## OS X

open terminal

/Applications/Firefox.app/Contents/MacOS/firefox-bin --profilemanager



# Countermeasures against webtracking for Firefox *(setting named "DNT1", see the study)*

If possible: Use Firefox ESR (higher frequency!)

Only search engines:

Ixquick, DuckDuckGo, Qwant, Startpage

The logo for ixquick, with 'ix' in red and 'quick' in blue.

die diskreteste Suchmaschine der Welt

Zu Firefox hinzufügen | Als Startseite einrichten



=> promise of data protection (one needs to believe that ...)

The logo for start page, with 'start' in red and 'page' in blue.

die diskreteste Suchmaschine der Welt

enhanced by  
Google  
[Infos dazu](#)

Zu Firefox hinzufügen | Als Startseite einrichten



★ Ixquick HTTPS - Deuts

- Google
- Yahoo
- Amazon.com
- Amazon.de
- Bing
- DuckDuckGo
- eBay
- LEO Eng-Deu
- Twitter
- Wikipedia (de)
- Wikipedia (en)
- ★ Ixquick HTTPS - Deutsch
- Startpage HTTPS - Deutsch

"Qwant" hinzufügen

Suchmaschinen verwalten...

★ Ixquick HTTPS - Deuts

- Google
- Yahoo
- Amazon.com
- Amazon.de
- Bing
- DuckDuckGo
- eBay
- LEO Eng-Deu
- Twitter
- Wikipedia (de)
- Wikipedia (en)
- ★ Ixquick HTTPS - Deutsch
- Startpage HTTPS - Deutsch

Suchmaschinen verwalten...

### Liste der Suchmaschinen verwalten

Momentan sind folgende Suchmaschinen installiert:

Name	Schlüsselwort
Google	
DuckDuckGo	
★ Ixquick HTTPS ...	
Startpage HTT...	
Qwant.com	

Schlüsselwort bearbeiten...

Nach oben

Nach unten

Entfernen

Suchvorschläge anzeigen

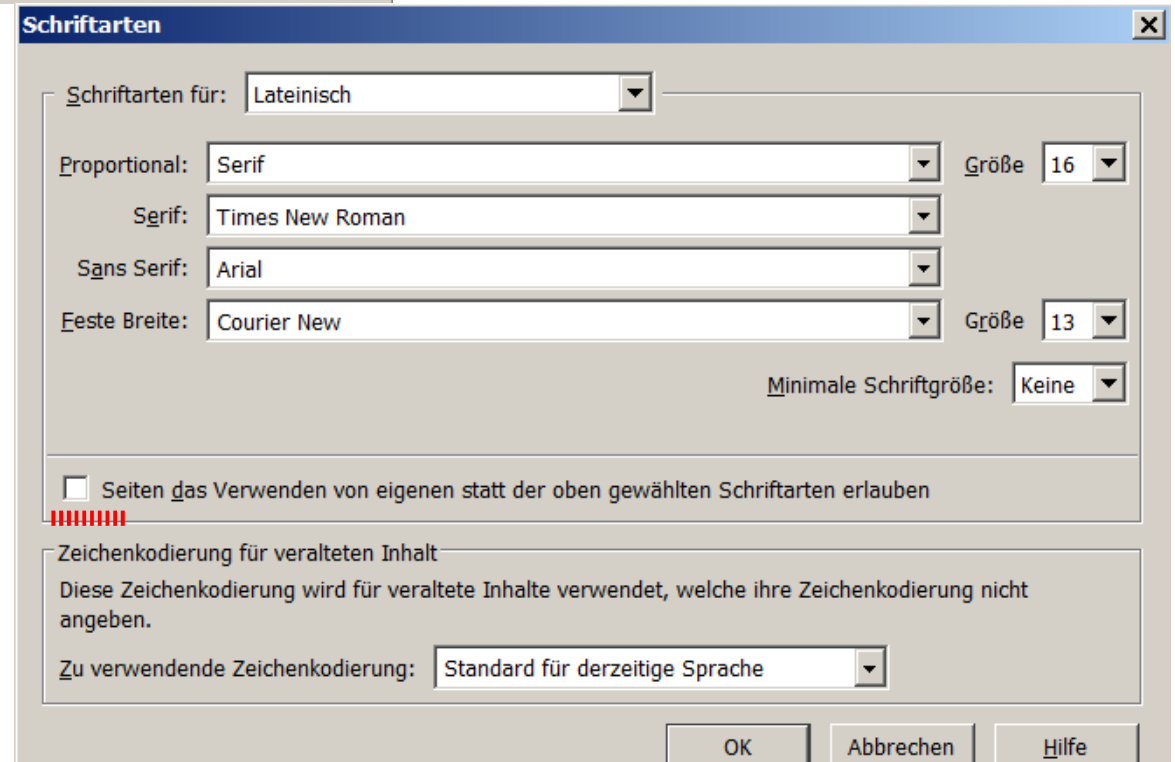
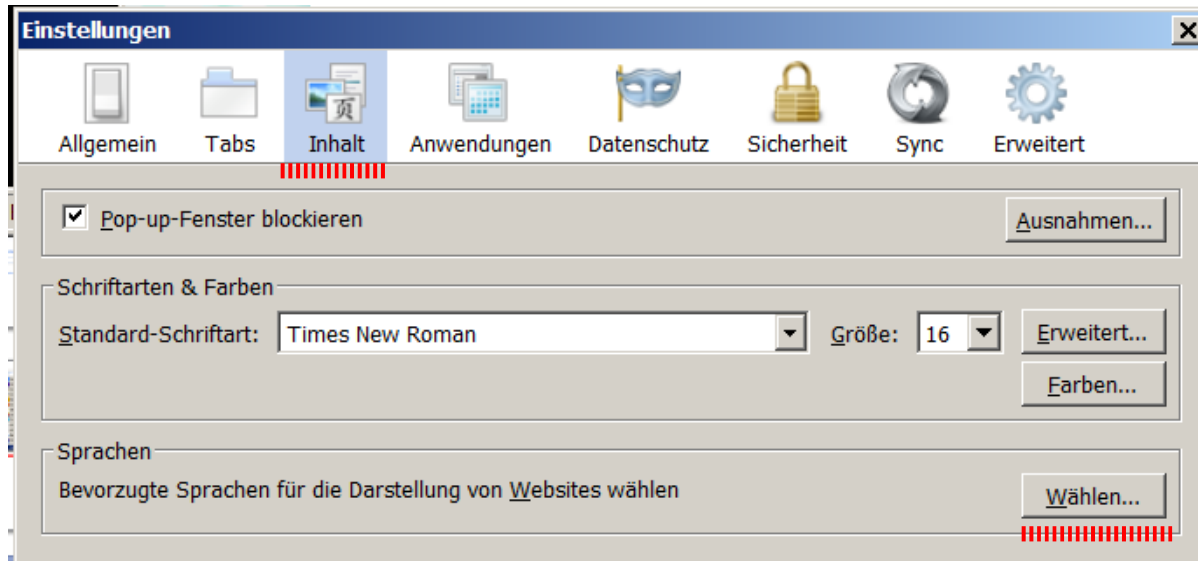
Weitere Suchmaschinen hinzufügen...

Vorgaben wiederherstellen

OK

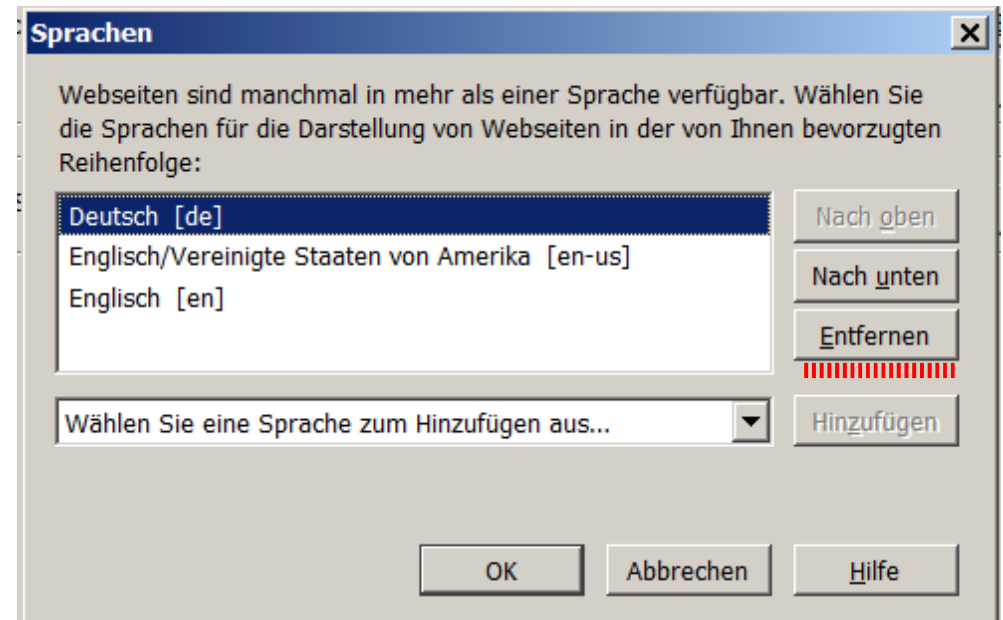
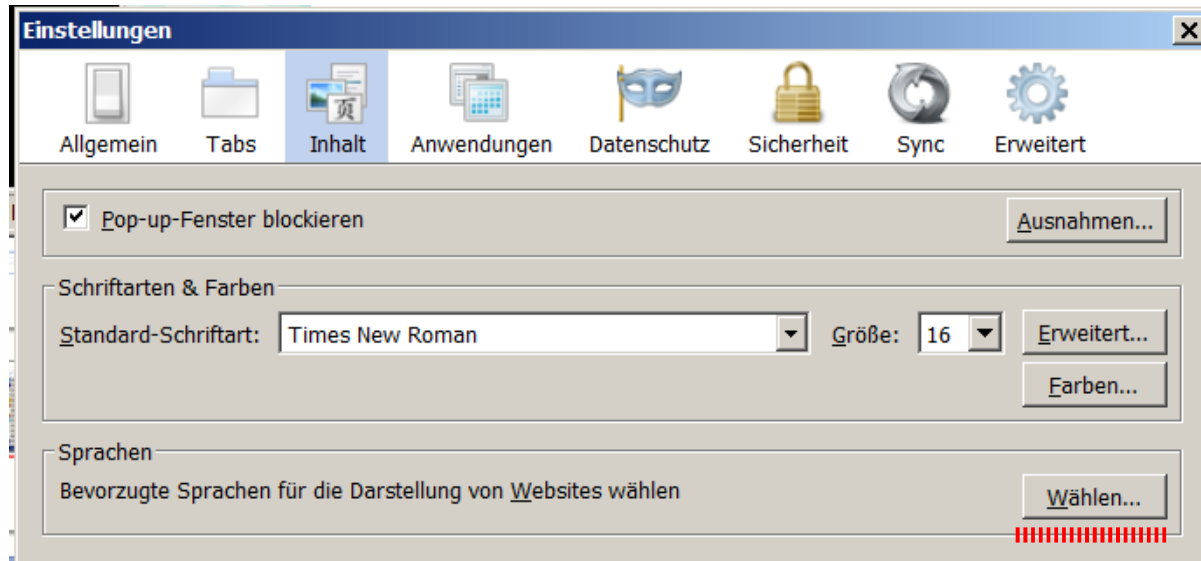
Abbrechen

# Only 3 local standard fonts (less data broadcasted, smaller fingerprint)

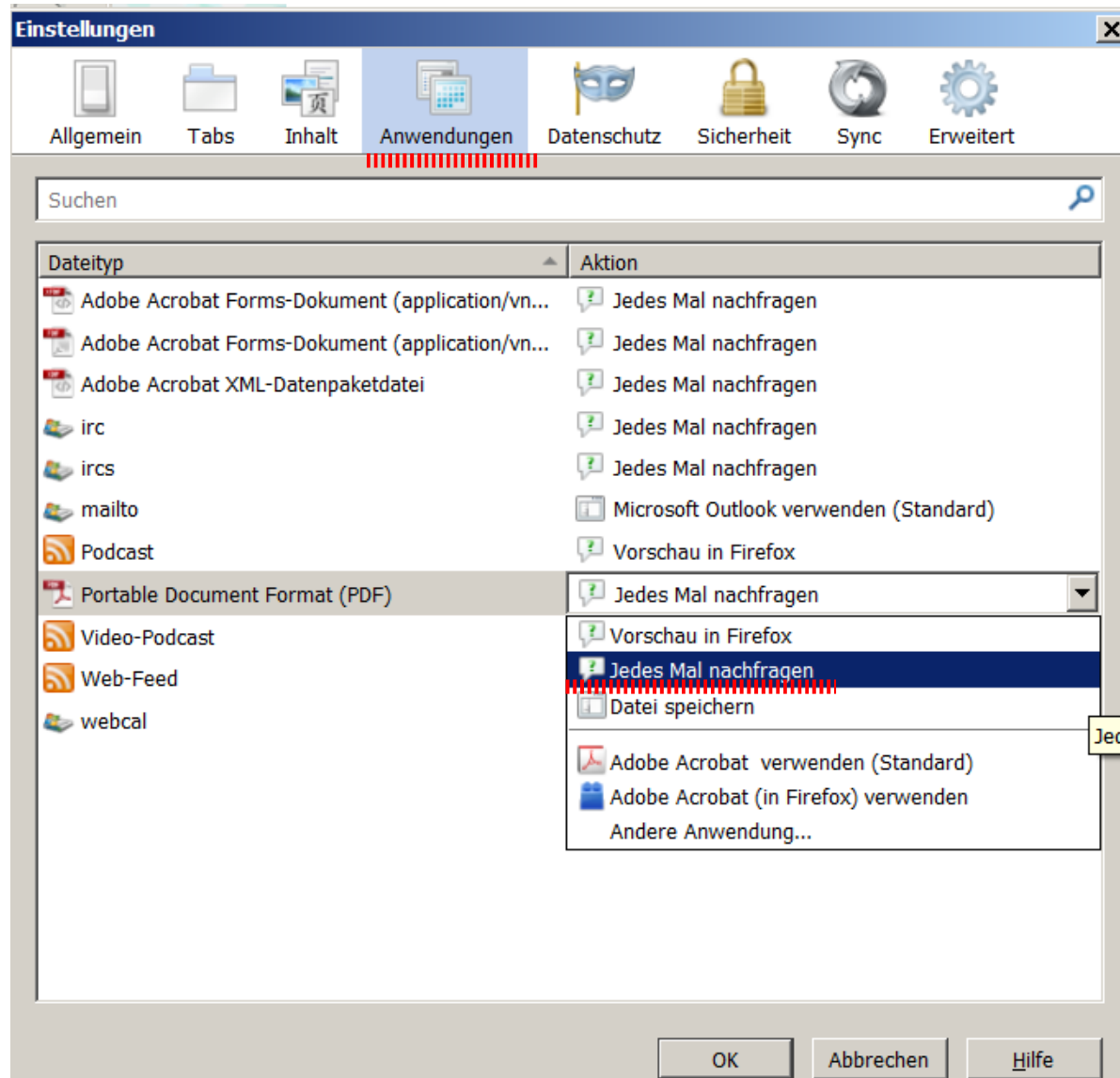


*Here with Windows fonts,  
other for Mac, Linux, BSD*

# Set language to en-us,en (most widespread, smaller fingerprint)

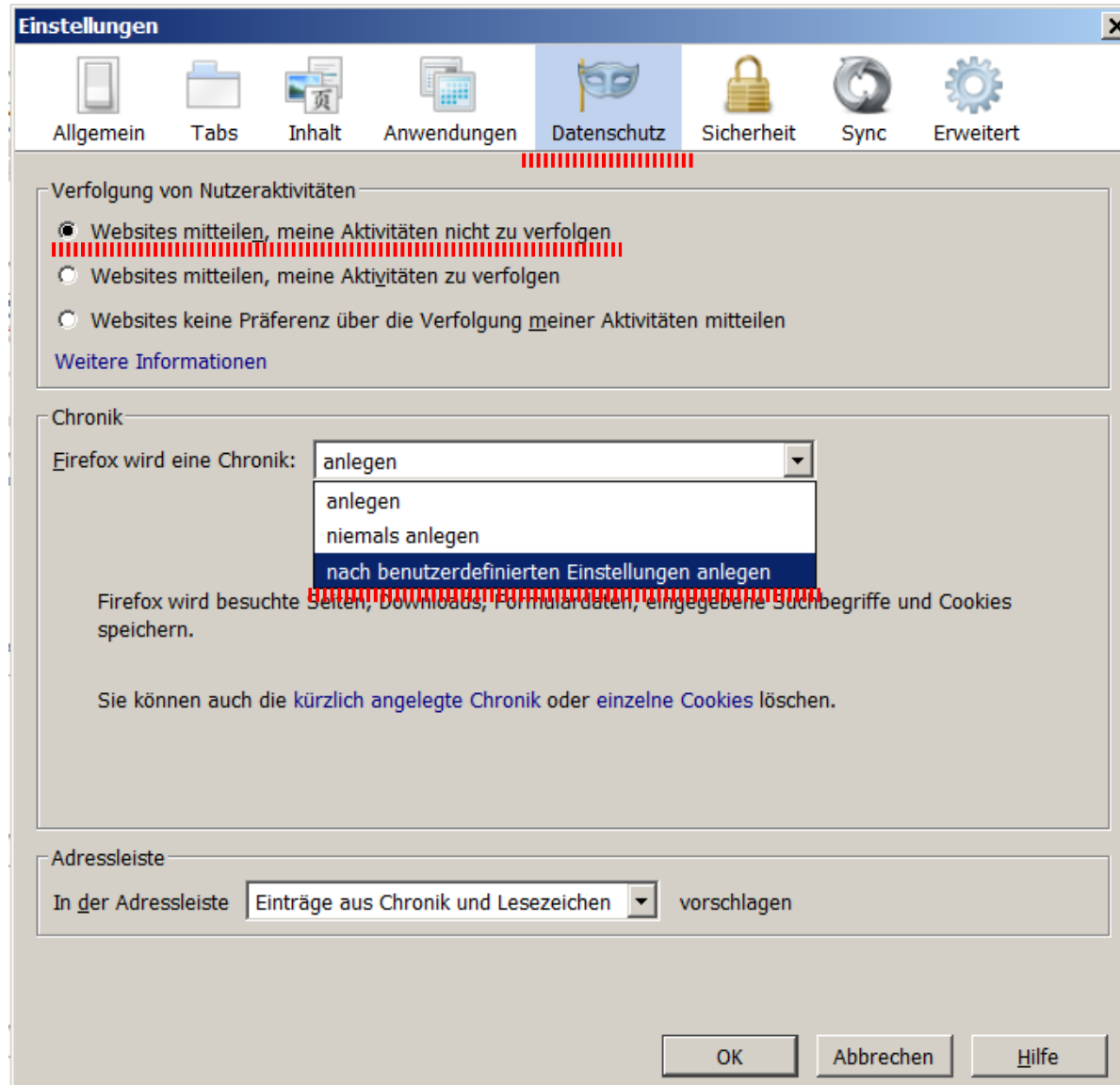


# External applications: Always ask (less data broadcasted, smaller fingerprint, better security)



# Send Do-not-track header

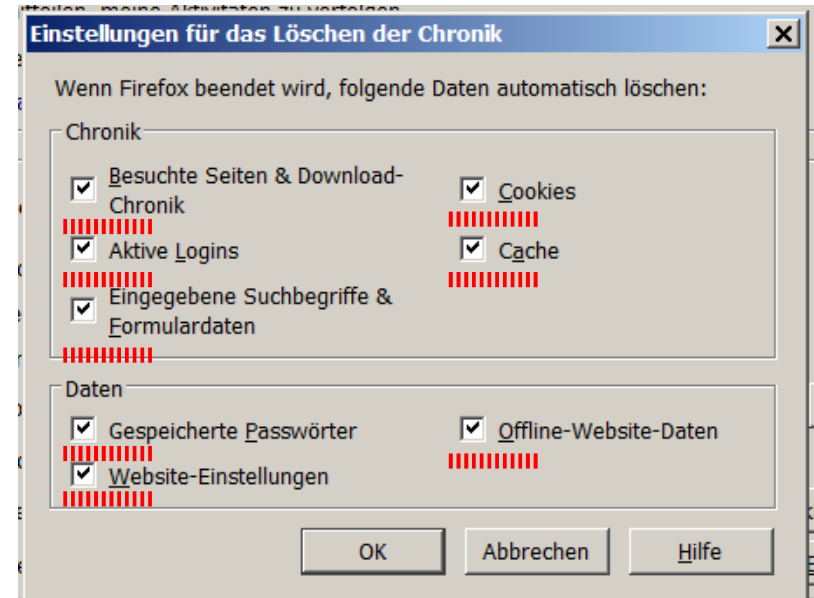
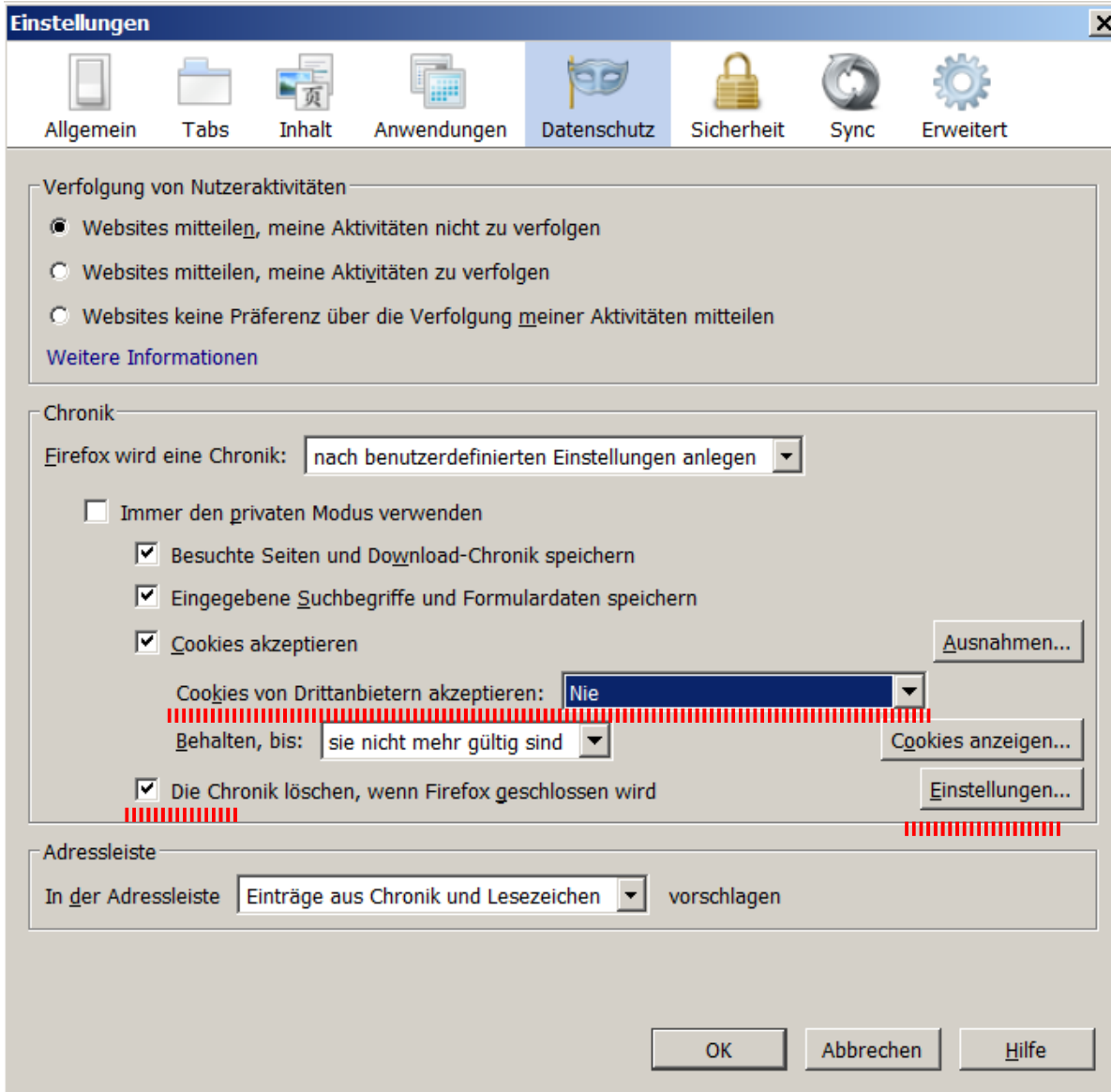
## Change settings for local storage



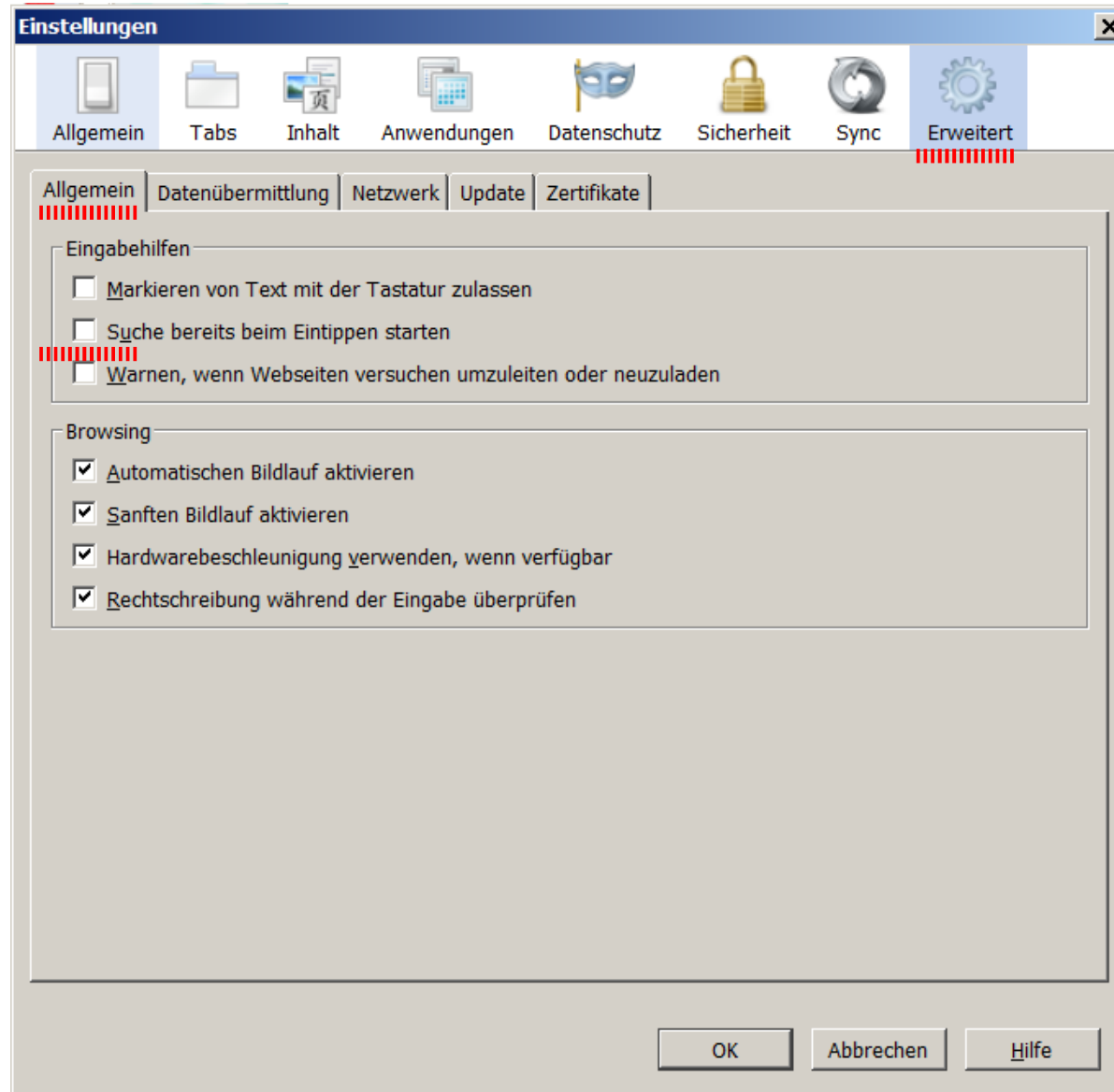


# Block 3rd party cookies

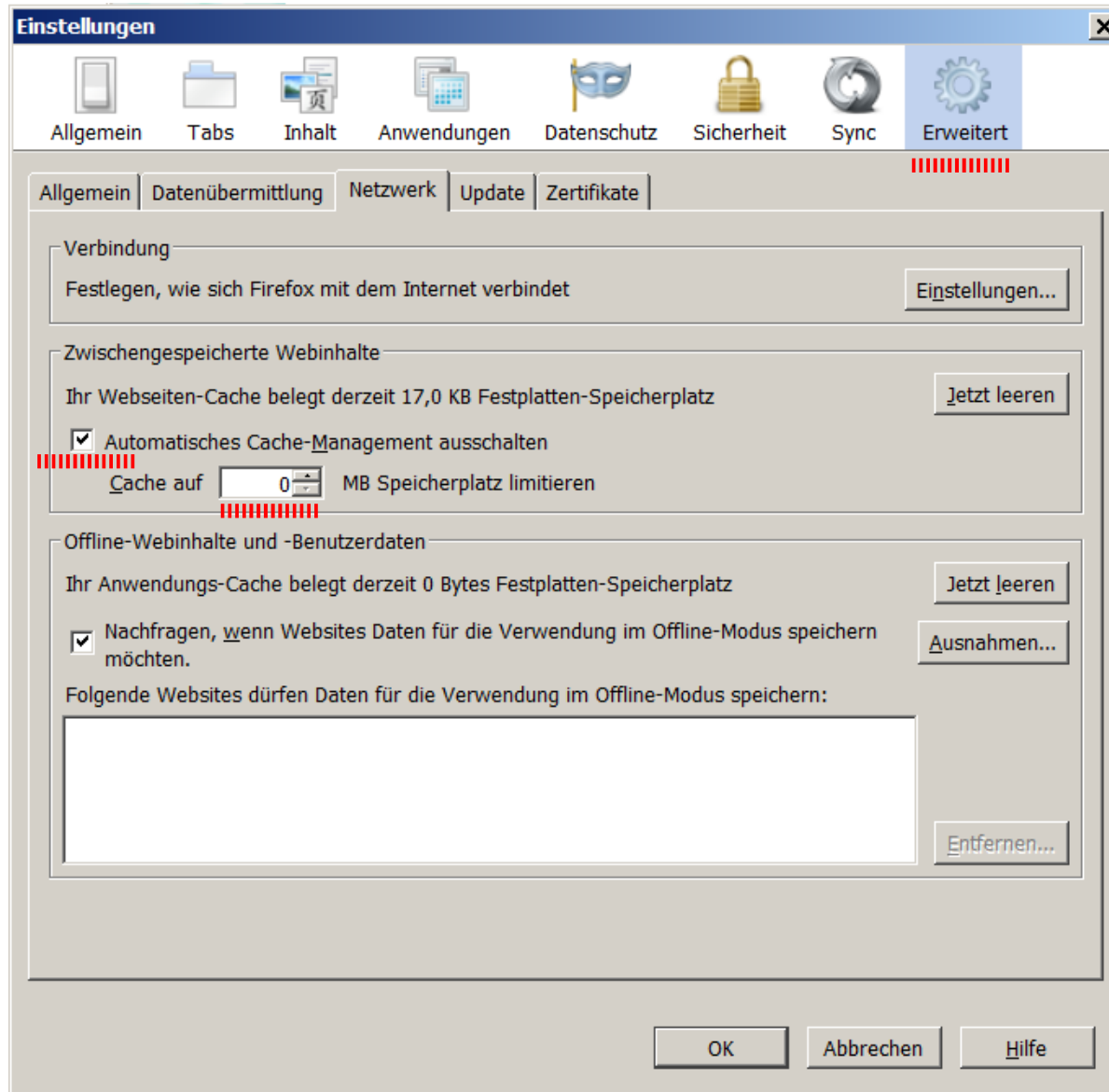
## Automatic deletion of locally stored markers



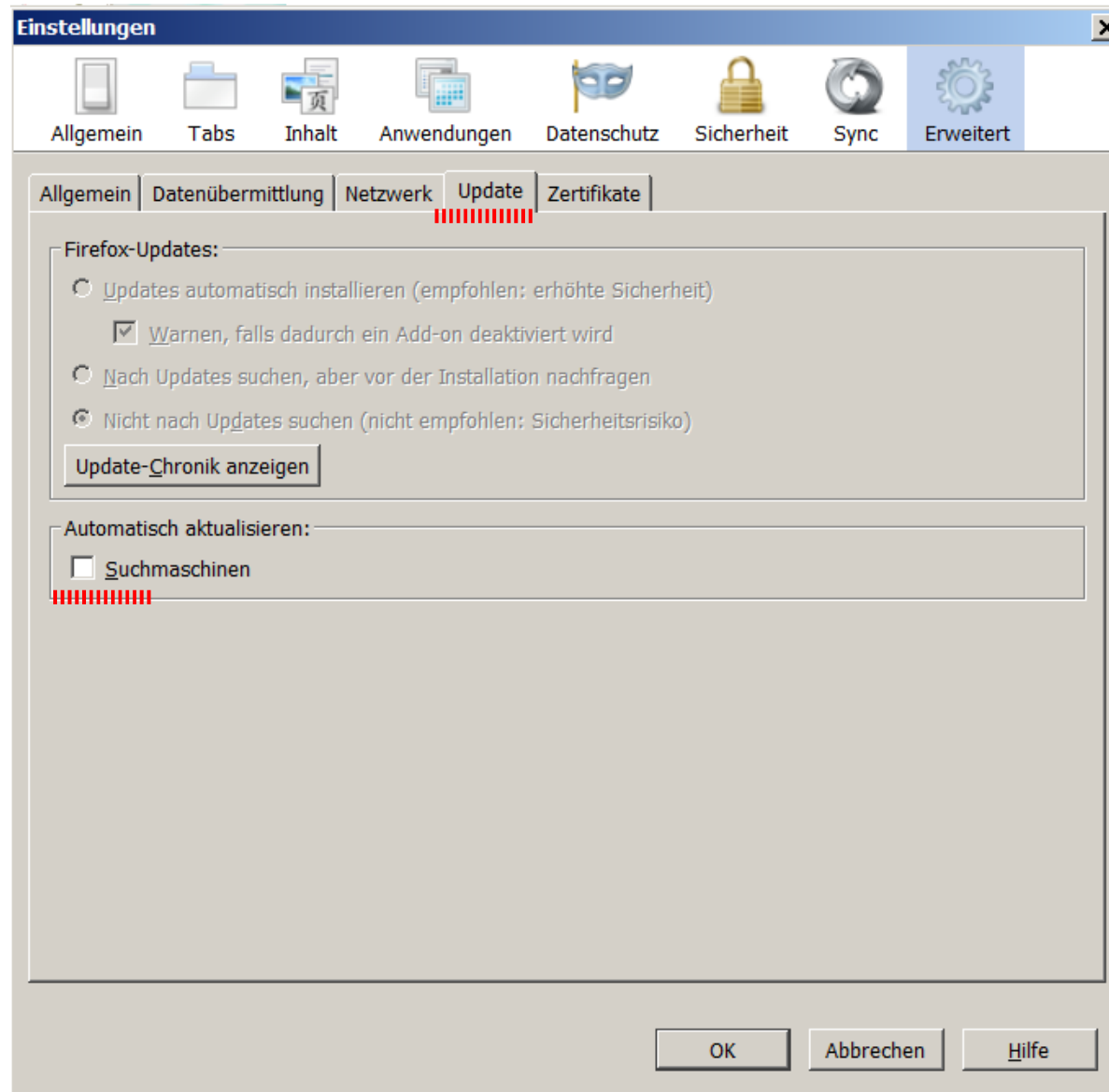
# Stop sending you entries in the address bar to search engines



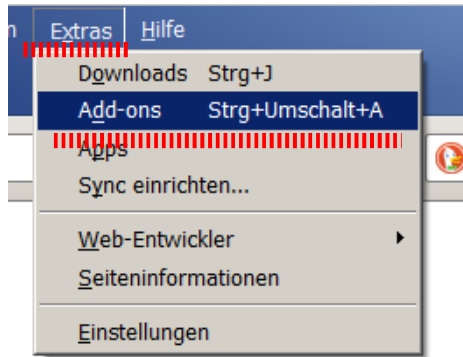
# Set cache disk to 0 MB (less tracking pixels)



# Disable automatic update of search engines (Google won't come back ...)



Set necessary plugins to always ask (e. g. Flash Player, PDF reader), disable the rest. Drastically reduces the amount of broadcasted data and the fingerprint. Improves the security, deactivates exploitable plugins.

A screenshot of the Firefox Add-ons Manager interface. The 'Plugins' section is selected, showing a list of installed plugins. The 'Plugins' section is highlighted in blue. The list includes:

- OpenH264-Videocodec zu... 1.3 (deaktiviert)
- Adobe Acrobat 10.1.13.16
- Google Update 1.3.26.9 (deaktiviert)
- Intel® Identity Prote... 4.0.5.0 (deaktiviert)
- Intel® Identity Prote... 4.0.5.0 (deaktiviert)
- Java Deployment Toolkit 7.0.750.13 ist bekannt dafür, Sicherheitsprobleme zu haben. Verwenden Sie das Plugin mit Vorsicht. (deaktiviert)
- Java Deployment ... 10.75.2.13 (deaktiviert)
- Java(TM) Platfor... 10.75.2.13 (deaktiviert)
- Microsoft Off... 14.0.4761.1000 (deaktiviert)

Each plugin entry has a status indicator (deaktiviert) and a dropdown menu to set its behavior (e.g., 'Nie aktivieren', 'Nachfragen, ob aktiviert werden soll').

# Measures in about:config



The screenshot shows the Firefox browser's 'about:config' page. The browser's address bar displays 'about:config' and the search engine is set to 'DuckDuckGo'. A prominent warning message is displayed in the main content area, featuring a yellow warning icon and the heading 'Hier endet möglicherweise die Gewährleistung!'. The warning text states that changes to default values of these settings can be dangerous for stability, security, and performance. Below the text is a checkbox labeled 'Diese Meldung beim nächsten Mal anzeigen', which is currently unchecked. A button with the text 'Ich werde vorsichtig sein, versprochen!' is located at the bottom of the warning area.

about:config

Firefox about:config

DuckDuckGo

 **Hier endet möglicherweise die Gewährleistung!**

Änderungen der Standardwerte dieser erweiterten Einstellungen können gefährlich für Stabilität, Sicherheit und Geschwindigkeit dieser Anwendung sein. Sie sollten nur fortfahren, wenn Sie genau wissen, was Sie tun.

Diese Meldung beim nächsten Mal anzeigen

In case of Firefox/Iceweasel on Debian:

Set user agent to standard version of *actual release*

Mozilla/5.0 (X11; Linux i686; rv:37.0) Gecko/20100101 Firefox/37.0 or for x64 to

Mozilla/5.0 (X11; Linux x86\_64; rv:37.0) Gecko/20100101 Firefox/37.0

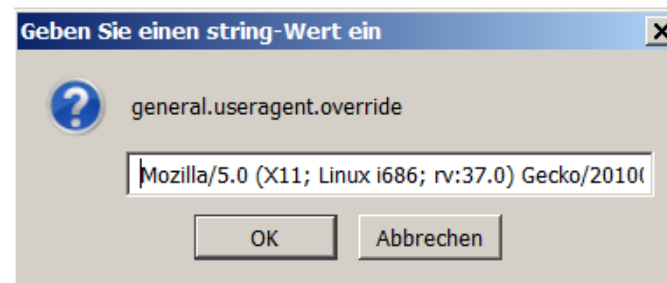
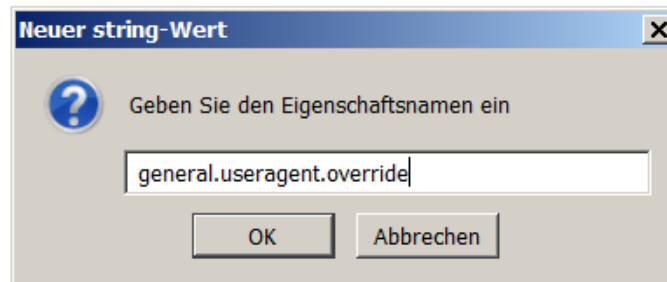
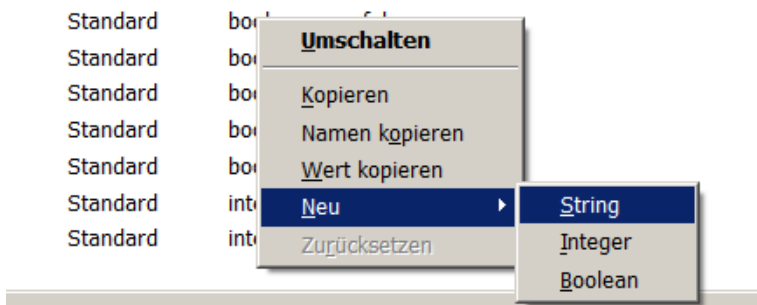
Much more widespread than

Mozilla/5.0 (X11; Linux i686; rv:37.0) Gecko/20100101 Firefox/37.0 **Iceweasel/37.0.1**

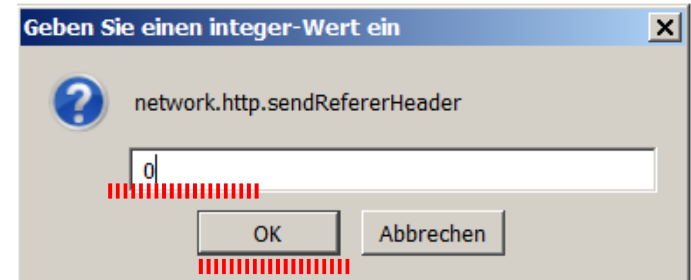
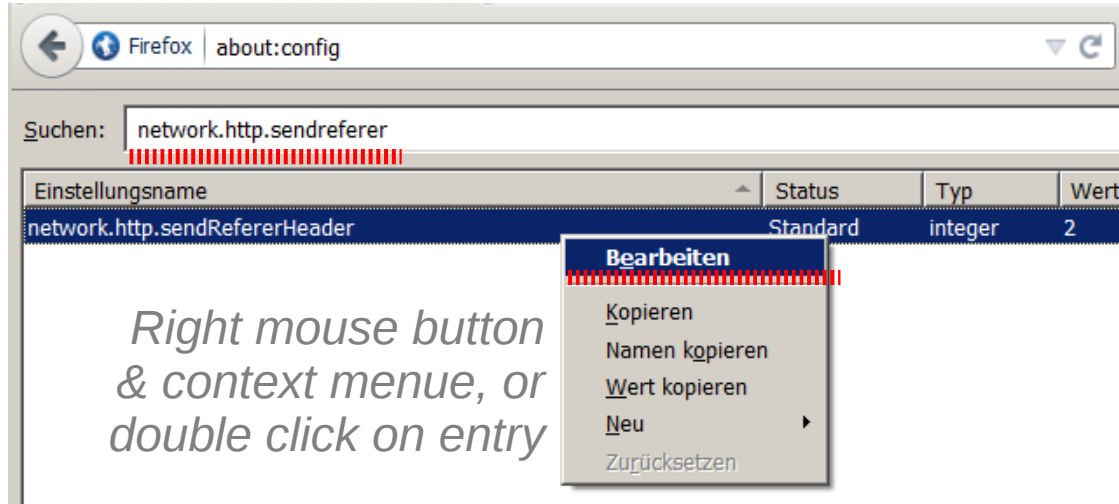
--> Leave small user group, enter bigger user group.

Right mouse click in about:config, new string

*general.useragent.override*



# Stop telling, from which site you come



# Stop telling public IP beside proxy via JS and WebRTC

`media.peerconnection.enabled = false`

# Stop telling your location

`geo.enabled = false`

# Stop pre-loading of linked sites (via http)

`network.dns.disablePrefetch = true`

`network.prefetch-next = false`



# AddOns

- Prefer encrypted version of sites

*Surveillants at net hubs only see, **that** you connect to `https://site1.eu`, not **what** you do there*

**HTTPS everywhere**

- Block 3rd party JS *e. g. JS from tracker.com on site1.eu*

=> mainly fingerprinters

**NoScript** (setup next slide)

- Apply preconfigured filter lists for 3rd party tracking domains (blacklisting)

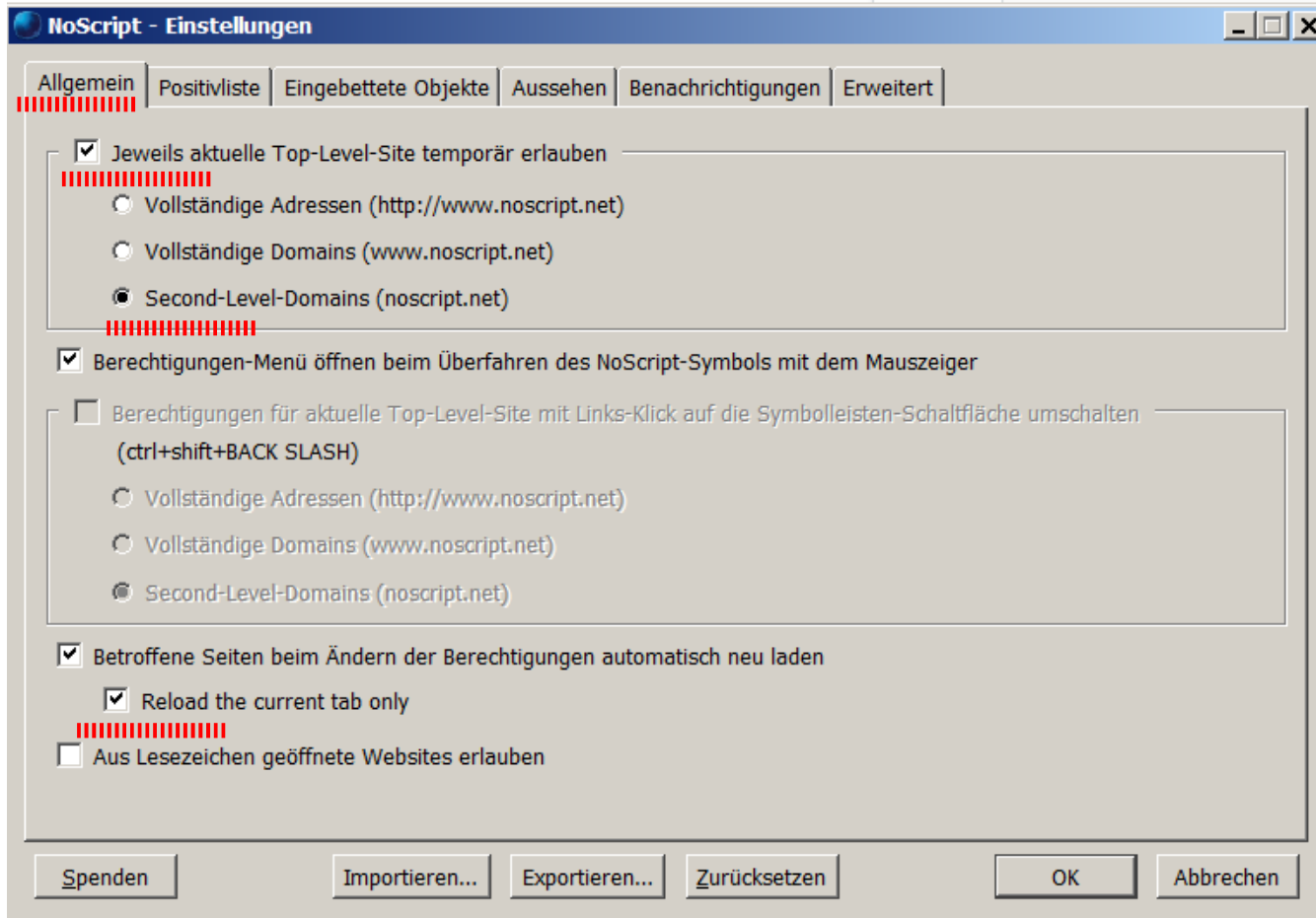
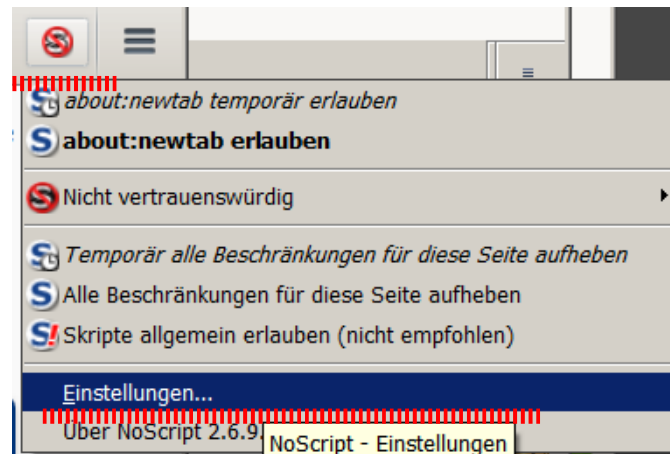
*block at site1.eu connection to google.com, facebook.com, tracker1.de, tracker2.at, ...*

**uBlock** (default filter lists, more available)

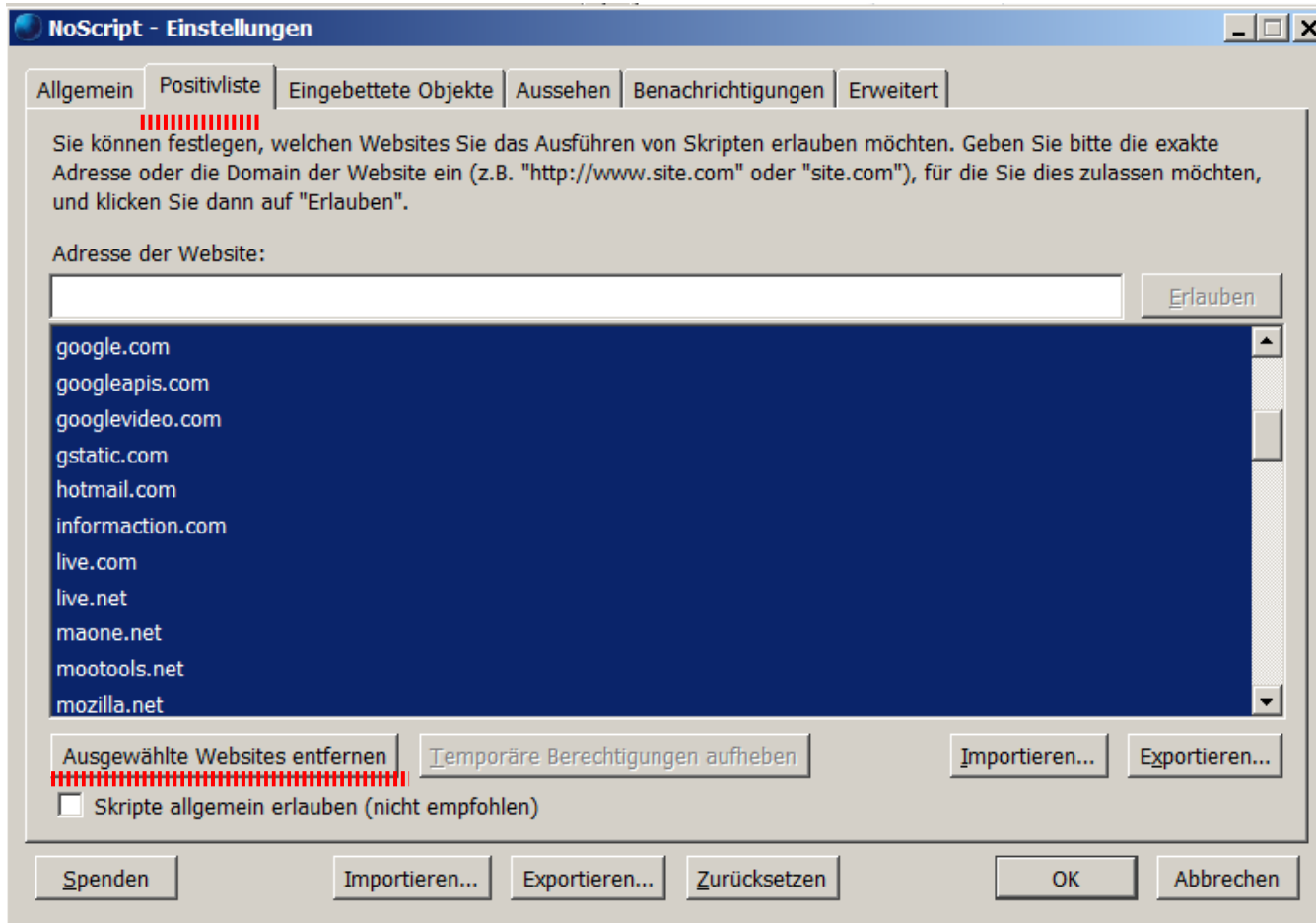
# Setup NoScript

Allow JS from 1st  
and 2nd party

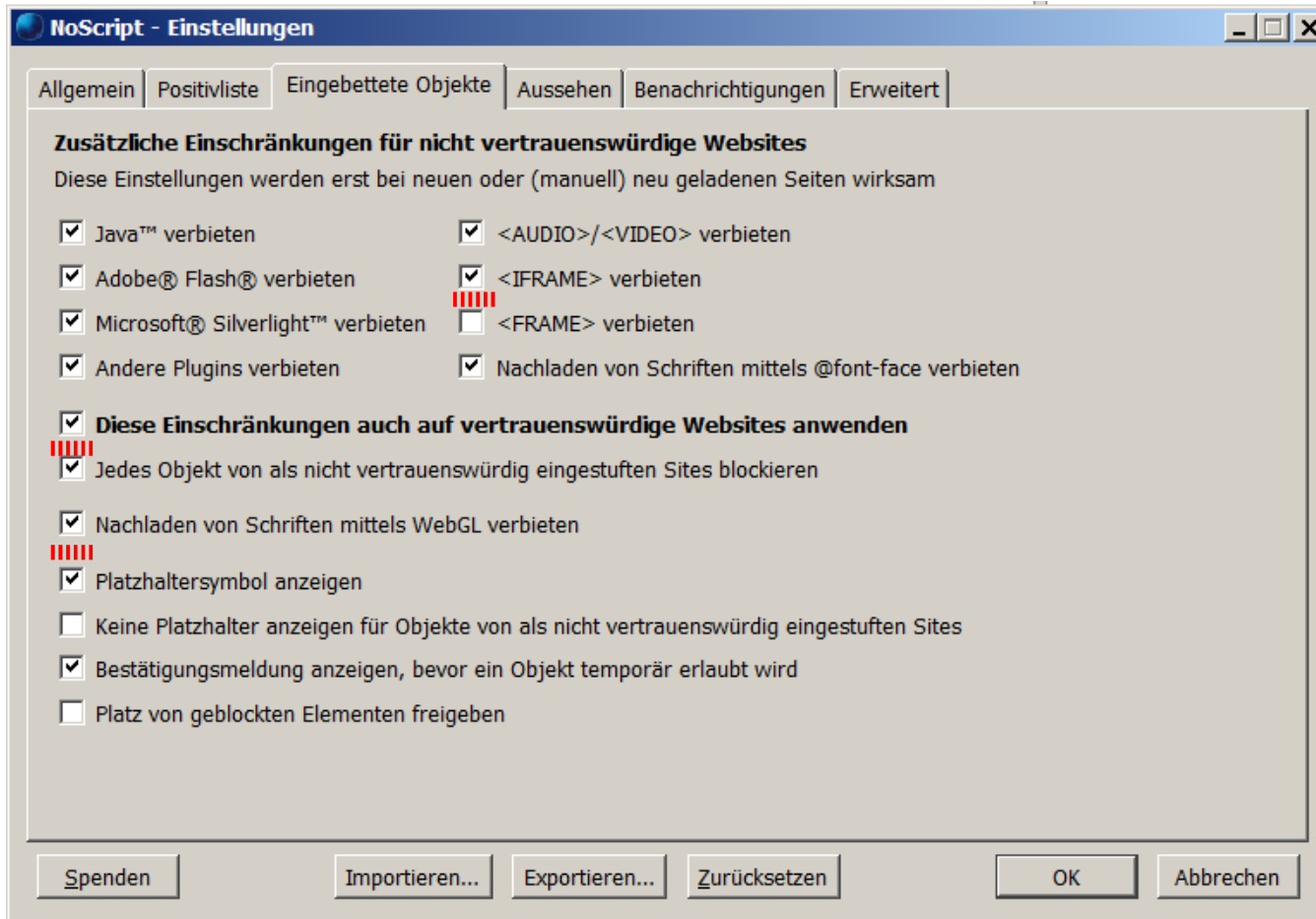
(site1.eu, prefix/site1.eu, site1.eu/subsite1, ...)



# Delete 3rd party JS fingerprinters, who bought their place on the NoScript whitelist



# Block iframes and WebGL, apply also to manually whitelisted sites.



## Now we have got:

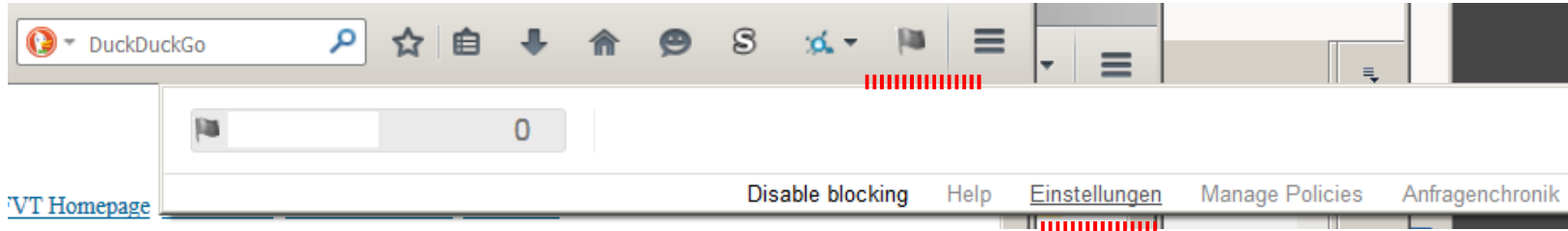
- Only search engines, who promise data protection
  - No activation of plugins w/o confirmation
  - Blocking of all 3rd party cookies
  - Storage of cache markers only in RAM
  - Deletion of locally stored markers at end of session
  - Blocking of 3rd party cache elements (depending on timeliness of filter blacklists)
  - Reduced data output to fingerprinters
  - Blocking of 3rd party fingerprinters
- (+) **Acceptable user comfort!**
- (-) **External password manager needed**  
**Sometimes 3rd party JS is necessary**  
**Very seldom: Necessity of 3rd party cookies**

# **DO! NOT! TRACK! Hardcore** (*setting DNT4*)

## *Masochist setting :-)*

- Like before
- Block all cookies
- Block all Javascript
- Turn all plugins off
- Set user agent to v31, the actual ESR (bigger user group)
- **Request Policy Contd.** instead of uBlock
- Deactivate Request Policie's automatic whitelists
- Block all 3rd party requests by default.
- Stepwise activation of 3rd party requests, cookies and Javascript (manual whitelisting)

# Setup Request policy



## RequestPolicy

Einstellungen

[Manage Policies](#)

Help

About

Your Policy

**Default Policy**

Subscriptions

## Default Policy

When you don't have any "allow" or "block" rules that match a request, this is what RequestPolicy will do. [Learn more.](#)

- Allow requests by default.
- Block requests by default. (For advanced users. Breaks many websites.)
- Allow requests to the same domain (www.example.com -> static.example.com).

Changing your default rule means different subscriptions are available. [Manage subscriptions.](#)

# RequestPolicy

Einstellungen

[Manage Policies](#)

Help

About

Your Policy

Default Policy

[Subscriptions](#)  
■■■■■■■■■■

# Subscription Policies

Subscription policies are sets of rules maintained by us with help from the community. These rules are updated automatically and minimize website breakage while blocking requests that impact your privacy.

## Usability

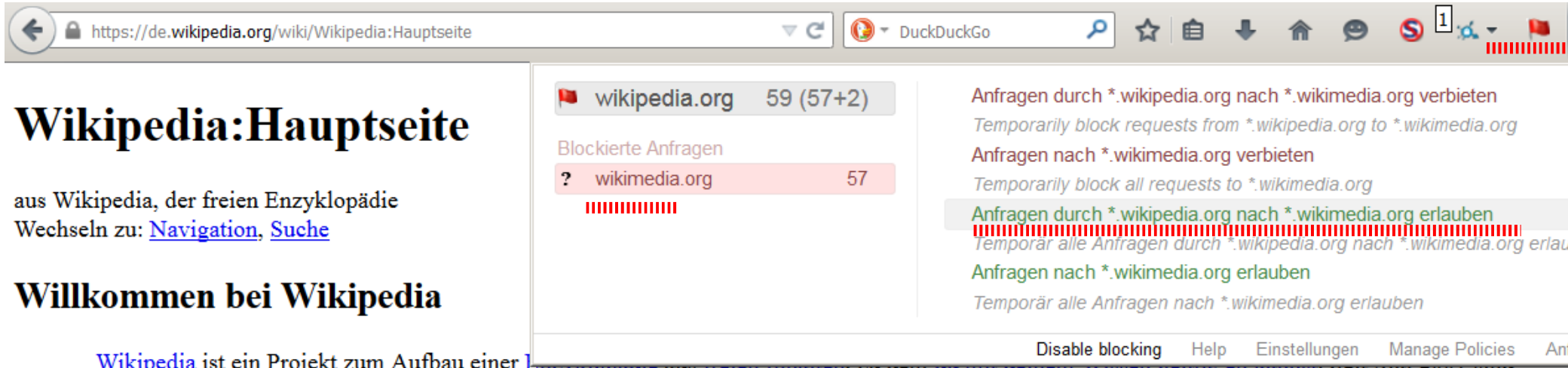
- Allow destinations that belong to the same organization as the origin webpage
- Allow requests that are needed for websites to work properly
- Allow requests for embedded content such as images and videos

## Browser

- Allow requests related to Mozilla and Firefox websites
- Allow requests that are needed for other extensions to work properly



# Manual activation of requests



The screenshot shows the Wikipedia main page with a sidebar on the right containing a list of blocked requests. The browser address bar shows 'https://de.wikipedia.org/wiki/Wikipedia:Hauptseite' and the search engine is 'DuckDuckGo'. The sidebar has a search bar with 'wikipedia.org' and '59 (57+2)' results. Below it, a section titled 'Blockierte Anfragen' shows a search for 'wikimedia.org' with '57' results. A red progress bar is visible below the search results. The main content area shows a list of requests with their status: 'Anfragen durch \*.wikipedia.org nach \*.wikimedia.org verbieten' (Temporarily block requests from \*.wikipedia.org to \*.wikimedia.org), 'Anfragen nach \*.wikimedia.org verbieten' (Temporarily block all requests to \*.wikimedia.org), and 'Anfragen durch \*.wikipedia.org nach \*.wikimedia.org erlauben' (Temporarily allow all requests from \*.wikipedia.org to \*.wikimedia.org). The third request is highlighted in green. At the bottom of the sidebar, there are links for 'Disable blocking', 'Help', 'Einstellungen', 'Manage Policies', and 'Ant'.

## Wikipedia:Hauptseite

aus Wikipedia, der freien Enzyklopädie  
Wechseln zu: [Navigation](#), [Suche](#)

## Willkommen bei Wikipedia


[Wikipedia](#) ist ein Projekt zum Aufbau einer [1.808.316](#) Artikel in deutscher Sprache entstanden.

[Geographie](#) [Geschichte](#) [Gesellschaft](#) [Kunst und Kultur](#) [Religion](#) [Sport](#) [Technik](#) [Wissenschaft](#)

[Artikel nach Themen](#) · [Alphabetischer Index](#) · [Artikel nach Kategorien](#) · [Gesprochene Wikipedia](#)

[Kontakt](#) · [Presse](#) · [Statistik](#) · [Sprachversionen](#) · [Mitmachen](#) · [Mentorenprogramm](#)


## Artikel des Tages



Der [Völkermord an den Armeniern](#) geschah während des Ersten Weltkrieges unter Verantwortung der jung-türkischen, von der Organisation Komitee für Einheit und Fortschritt gebildeten Regierung des Osmanischen Reichs. Einem der ersten systematischen Genozide des 20. Jahrhunderts fielen bei Massakern und Todesmärschen, die im Wesentlichen in den Jahren 1915 und 1916 stattfanden, je nach Schätzung zwischen 300.000 und mehr als 1,5 Millionen Menschen zum Opfer. Die Angaben zu den getöteten Armeniern während der Übergriffe in den beiden vorangegangenen Jahrzehnten variieren zwischen Zehntausenden und Hunderttausenden. Die Ereignisse, die von den Armeniern selbst mit dem Begriff *Ashet* – „Katastrophe“ – bezeichnet werden.

## In den Nachrichten

[Oskar Gröning](#) · [Calbuco](#) · [Libor-Skandal](#)

- Im Zuge der [Operation Eikonol](#) hat der [BND](#) (Logo) bis zu 40.000 Ziele, darunter Politiker und Unternehmen in Deutschland und Westeuropa, ausgespäht und die Erkenntnisse an die [National Security Agency](#) weitergeleitet.
  - Der ehemalige Staatspräsident Ägyptens [Mohammed Mursi](#) wurde durch ein ägyptisches Gericht zu einer Haftstrafe von 20 Jahren verurteilt.
  - Ein [Flüchtlingsboot im Mittelmeer](#) mit mehr als 700 Menschen an Bord kenterte in der Nacht auf den 19. April. Laut dem [UNHCR](#) ist dies
- 

## Now we have got:

- Standard setting like before
- Maximum protection from 3rd party tracking:  
only necessary 3rd party request are allowed
- Maximum protection from 1st party tracking:  
cookies and JS (**evil fingerprinters!**) only active,  
when allowed
- A big anonymity group: Firefox ESR users w/o JS  
and w/o cookies

(+) highest privacy and security, home-grown!

(-) a really, really bad user experience

**=> Play around. Find you own compromise!**