

# Privacy by Design in der Praxis



**Beispiele aus Anwendungsentwicklung und Unternehmensalltag**

Internet Security Days, Brühl, 20.09.2018

# whoami

## Jutta Horstmann

Dipl. Pol. → Dipl. Inf. → Sysadmin → DB-Admin  
→ Entwicklerin → Geschäftsführerin → Consultant  
→ **Head of Filters bei der eyeo GmbH**

## eyeo GmbH

ANGESTELLTE STANDORTE MALMÖ

TE **130+**



Beliebtester  
WERBEBLOCKER  
seit  
**2006**

Mitarbeiter in über  
**20** LÄNDERN



# Agenda

---

1. Privacy by Design - Das Konzept
2. Relevanz
3. Fallbeispiel: Privacy by Design bei eyeo / Adblock Plus



# Privacy by Design - Das Konzept

---

# 1. Proaktiv, nicht reaktiv

## **2. Datenschutz als Default-Einstellung**

# **3. Datenschutz als Kernfeature jedes Konzepts**

# 4. Voller Funktionsumfang



# **5. Datenschutz über den gesamten Lifecycle**

# **6. Verständlichkeit, Offenheit, Transparenz**

# **7. Souveräne Nutzer im Zentrum des Datenschutzes**

# Relevanz



Charles J. Sykes, The End of Privacy, 1999

**„Privatsphäre ist wie  
Sauerstoff – man schätzt  
sie erst, wenn sie fehlt.“**

# Full text of EU GDPR (General Data Protection Regulation)

## GDPR Table of Contents

[Useful GDPR links](#)

Search in articles...



Chapter 1 (Art. 1 – 4)  
**GENERAL PROVISIONS**



Chapter 2 (Art. 5 – 11)  
**PRINCIPLES**



Chapter 3 (Art. 12 – 23)  
**RIGHTS OF THE DATA SUBJECT**



Chapter 4 (Art. 24 – 43)  
**CONTROLLER AND PROCESSOR**



Section 1 (Art. 24 – 31)  
**GENERAL OBLIGATIONS**



Article 24 – Responsibility of the controller

Article 25 – Data protection by design and by default

EU GDPR > Chapter 4 > Section 1 > Article 25

## Article 25 – Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to [Article 42](#) may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

« Article 24 – Responsibility of the controll...

Article 26 – Joint controllers »



# Fallbeispiel: Privacy by Design bei eyeo

---

# Datenschutz tief in der DNA verwurzelt

---



Adblock **Plus**

[Über](#)

[Beitragen](#)

[Hilfe](#)

[Deutsch \(DE\) ▾](#)

## Unsere Werte

Wir erheben so wenig Daten wie möglich. Sofern eine anonyme oder pseudonyme Nutzung möglich ist, anonymisieren oder pseudonymisieren wir deine Daten.





# Anwendungsentwicklung

---

- Produkte
- Kommunikation
  - Website(s)
  - Blog(s) / Kommentarfunktion
  - Forum
  - User Support
- Online-Tools
  - Issue Tracker
  - Code Repositories
  - Code Review



# eyeo - Produkte

—



# Proaktiv, nicht reaktiv



The screenshot shows a GitLab issue page for the project 'adblockplusui'. The issue title is 'Support machine learning through issue reporter'. The issue description states: 'Earlier prototypes of issue reporter had an option to allow us to use submitted data for machine learning. However currently we are not planning to have this checkbox at all. I think we should at least explore what we can do with the submitted data using machine learning, so I would like to include that checkbox back.'

The 'Related issues' section shows one related issue: 'Run user testing on "Machine Learning Opt-in" #46'.








The comment history includes:

- Thomas Greiner (Developer) asked @jeenlow if they knew anything about the reason for including the checkbox in the prototype, noting technical considerations and privacy policy requirements.
- @ollie-eyeo responded that existing information was documented in the spec and that a version collecting screenshots was ready for release.
- Thomas Greiner marked the issue as related to #46.
- Winsley (Maintainer) mentioned an IIRC from a meeting that screenshots were of questionable use for ML due to privacy concerns, but they were happy to add a checkbox if valuable.
- Judith Nink (Developer) noted that a privacy policy amendment was necessary and that the decision on whether to include a consent checkbox depended on the data to be forwarded.

# Datenschutz als Default-Einstellung

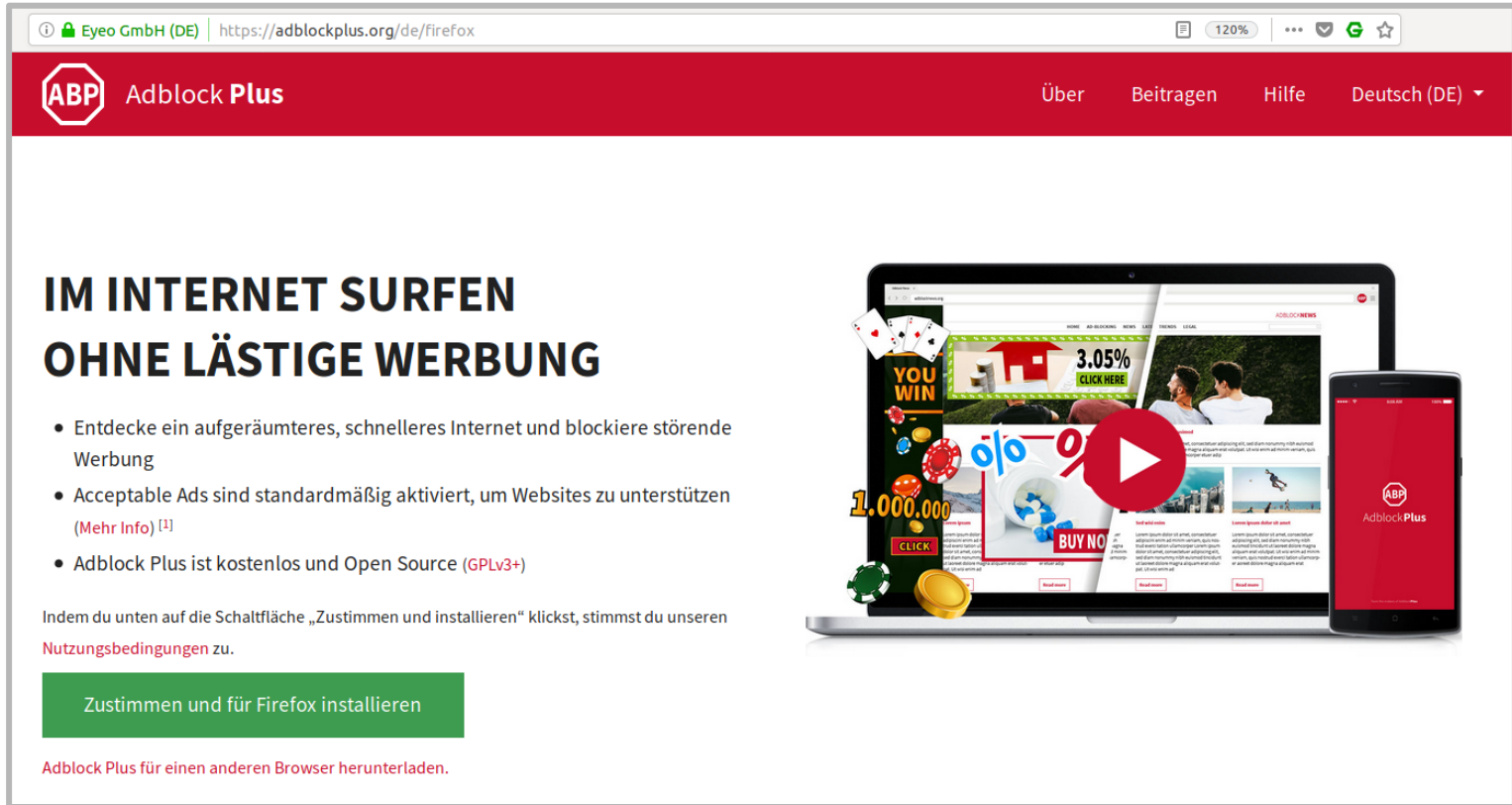


## NoTrack: No Tracking by Website and Third Parties

	<b>Check if 3rd party embeds are being used</b> The site does not use any third parties.	reliable	▼
	<b>Check if embedded 3rd parties are known trackers</b> The site does not use any known tracking- or advertising companies.	reliable	▼
	<b>Determine how many cookies the website sets</b> The website itself is not setting any cookies.	reliable	▼
	<b>Determine how many cookies are set by third parties</b> No one else is setting any cookies.	reliable	▼
	<b>Check if Google Analytics is being used</b> The site does not use Google Analytics.	reliable	▼
	<b>Check if Google Analytics has the privacy extension enabled</b> Not checking if Google Analytics data is being anonymized, as the site does not use Google Analytics.	reliable	▼
	<b>Check whether web server is located in a country which implements the GDPR</b> All web servers are located in Germany.	unreliable	▼



# Beispiel: Website



Eyeo GmbH (DE) | <https://adblockplus.org/de/firefox>

**ABP** Adblock Plus

Über Beitragen Hilfe Deutsch (DE) ▾

## IM INTERNET SURFEN OHNE LÄSTIGE WERBUNG

- Entdecke ein aufgeräumteres, schnelleres Internet und blockiere störende Werbung
- Acceptable Ads sind standardmäßig aktiviert, um Websites zu unterstützen [\(Mehr Info\)](#) <sup>[1]</sup>
- Adblock Plus ist kostenlos und Open Source [\(GPLv3+\)](#)

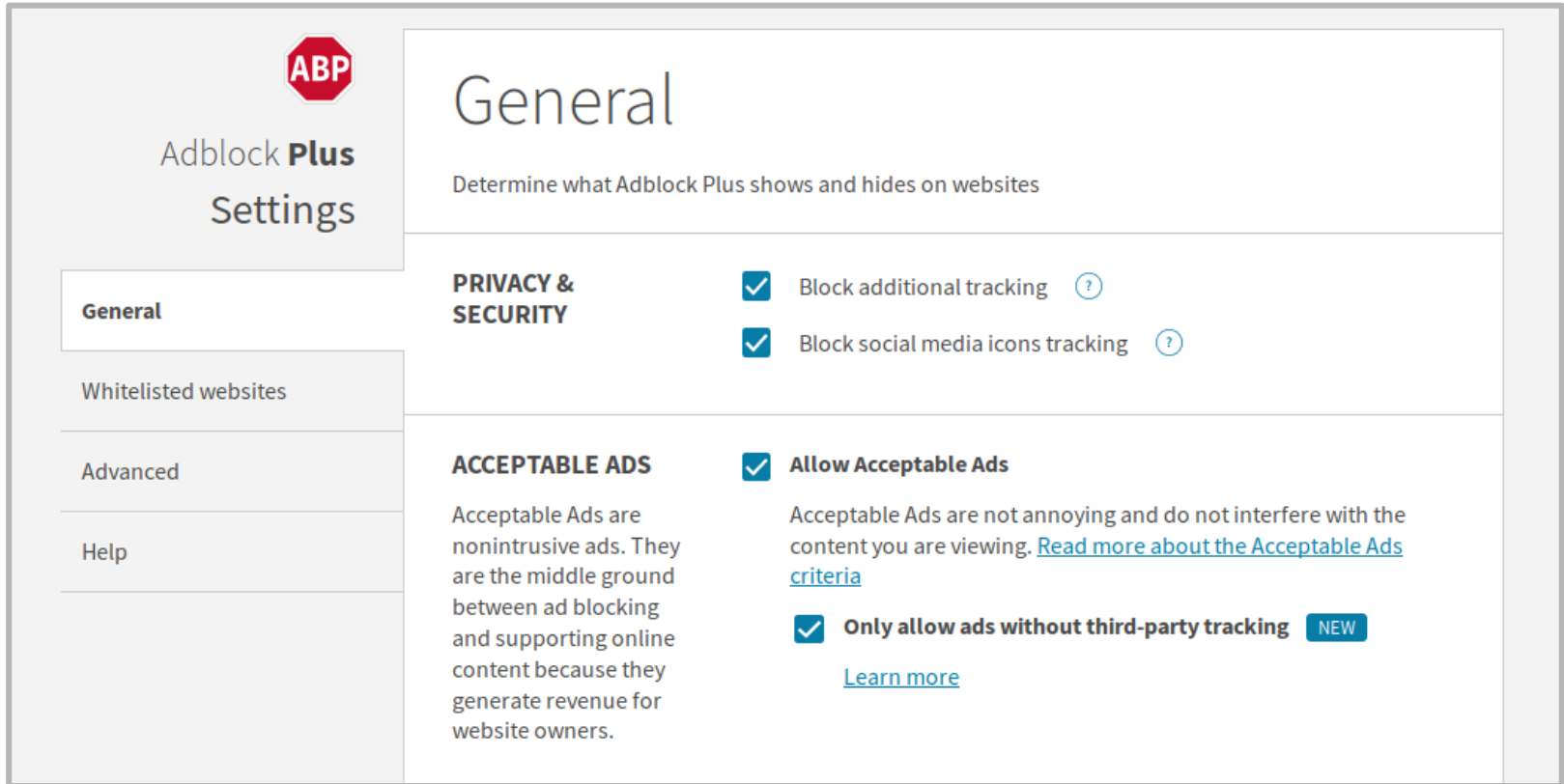
Indem du unten auf die Schaltfläche „Zustimmen und installieren“ klickst, stimmst du unseren [Nutzungsbedingungen](#) zu.

Zustimmen und für Firefox installieren

[Adblock Plus für einen anderen Browser herunterladen.](#)



# Datenschutz als Kernfeature jedes Konzepts



The image shows a screenshot of the Adblock Plus settings interface. On the left is a sidebar with the Adblock Plus logo and the text 'Adblock Plus Settings'. Below the logo are four menu items: 'General' (which is highlighted), 'Whitelisted websites', 'Advanced', and 'Help'. The main content area is titled 'General' and has a subtitle 'Determine what Adblock Plus shows and hides on websites'. It is divided into two sections: 'PRIVACY & SECURITY' and 'ACCEPTABLE ADS'. The 'PRIVACY & SECURITY' section contains two checked options: 'Block additional tracking' and 'Block social media icons tracking', each with a help icon. The 'ACCEPTABLE ADS' section contains one checked option: 'Allow Acceptable Ads', with a descriptive paragraph and a link to 'Read more about the Acceptable Ads criteria'. Below this is another checked option: 'Only allow ads without third-party tracking', which has a 'NEW' badge and a link to 'Learn more'.

**Adblock Plus Settings**

**General**

Determine what Adblock Plus shows and hides on websites

**PRIVACY & SECURITY**

- Block additional tracking [?](#)
- Block social media icons tracking [?](#)

**ACCEPTABLE ADS**

**Allow Acceptable Ads**

Acceptable Ads are nonintrusive ads. They are the middle ground between ad blocking and supporting online content because they generate revenue for website owners.

[Read more about the Acceptable Ads criteria](#)

**Only allow ads without third-party tracking** **NEW**

[Learn more](#)



# ABP als Privacy-Tool: Anti-Tracking

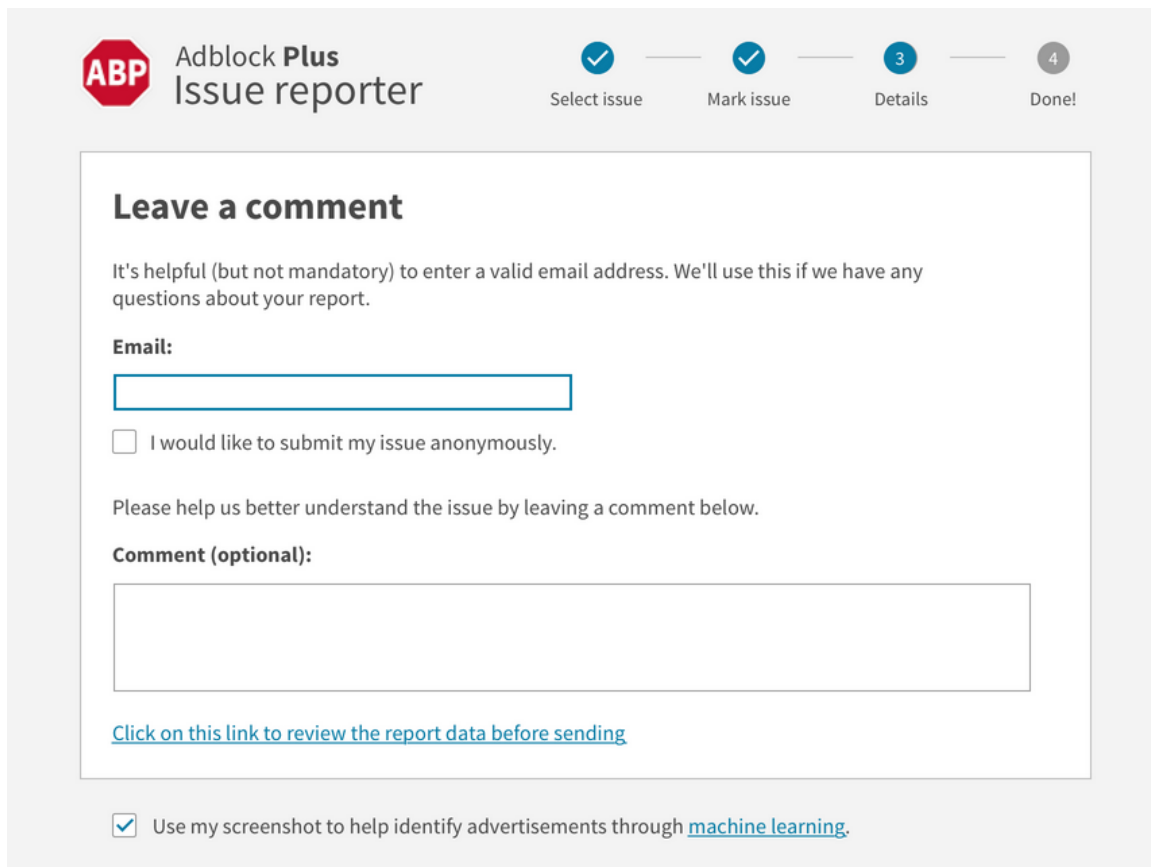


*"On the Internet, nobody knows you're a dog."*

- Tracking cookies
- Behavioral Analysis
- Re-Targeting
- Social Tracking
- Fingerprinting
- Session-Replay Scripts
- Site Analytics tracking
- Customer interaction tracking
- 3rd party fonts



# Voller Funktionsumfang



The screenshot shows the Adblock Plus Issue reporter interface. At the top, there is a progress bar with four steps: 'Select issue' (checked), 'Mark issue' (checked), 'Details' (3), and 'Done!' (4). The main content area is titled 'Leave a comment' and contains the following text: 'It's helpful (but not mandatory) to enter a valid email address. We'll use this if we have any questions about your report.' Below this is an 'Email:' label and an empty text input field. A checkbox labeled 'I would like to submit my issue anonymously.' is present. The text 'Please help us better understand the issue by leaving a comment below.' is followed by a 'Comment (optional):' label and a large empty text area. A blue link 'Click on this link to review the report data before sending' is located below the comment area. At the bottom, a checked checkbox is followed by the text 'Use my screenshot to help identify advertisements through [machine learning](#)'.

**ABP** Adblock Plus  
Issue reporter

Select issue ✓ — Mark issue ✓ — Details 3 — Done! 4

## Leave a comment

It's helpful (but not mandatory) to enter a valid email address. We'll use this if we have any questions about your report.

**Email:**

I would like to submit my issue anonymously.

Please help us better understand the issue by leaving a comment below.

**Comment (optional):**

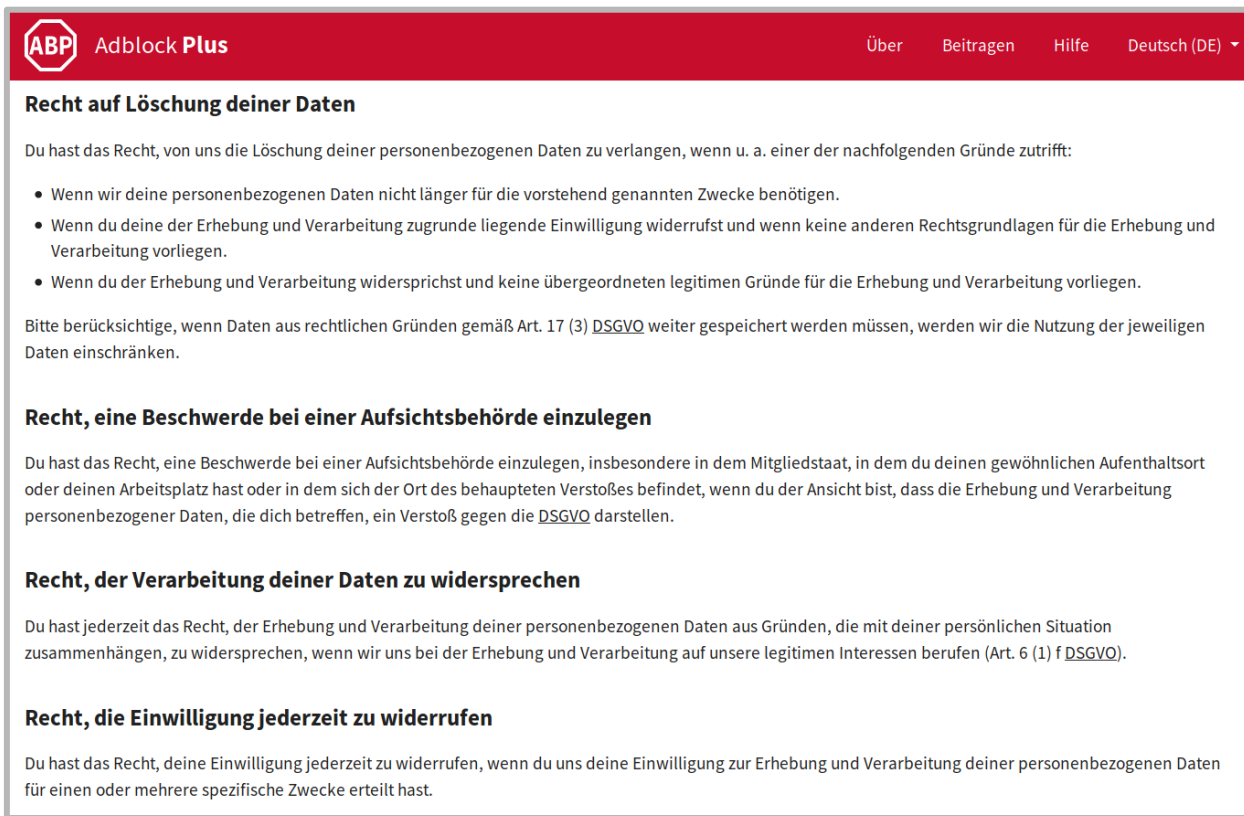
[Click on this link to review the report data before sending](#)

Use my screenshot to help identify advertisements through [machine learning](#).





# Datenschutz über den gesamten Lifecycle



The image shows a screenshot of the Adblock Plus website. The top navigation bar is red with the Adblock Plus logo and the text 'Adblock Plus'. To the right, there are links for 'Über', 'Beitragen', 'Hilfe', and 'Deutsch (DE)'. The main content area is white and contains several sections of text, each with a bold heading. The sections are: 'Recht auf Löschung deiner Daten', 'Recht, eine Beschwerde bei einer Aufsichtsbehörde einzulegen', 'Recht, der Verarbeitung deiner Daten zu widersprechen', and 'Recht, die Einwilligung jederzeit zu widerrufen'. Each section contains a paragraph of text and, in the first section, a bulleted list of three items.

**ABP** Adblock Plus Über Beitragen Hilfe Deutsch (DE) ▾

## Recht auf Löschung deiner Daten

Du hast das Recht, von uns die Löschung deiner personenbezogenen Daten zu verlangen, wenn u. a. einer der nachfolgenden Gründe zutrifft:

- Wenn wir deine personenbezogenen Daten nicht länger für die vorstehend genannten Zwecke benötigen.
- Wenn du deine der Erhebung und Verarbeitung zugrunde liegende Einwilligung widerrufenst und wenn keine anderen Rechtsgrundlagen für die Erhebung und Verarbeitung vorliegen.
- Wenn du der Erhebung und Verarbeitung widersprichst und keine übergeordneten legitimen Gründe für die Erhebung und Verarbeitung vorliegen.

Bitte berücksichtige, wenn Daten aus rechtlichen Gründen gemäß Art. 17 (3) [DSGVO](#) weiter gespeichert werden müssen, werden wir die Nutzung der jeweiligen Daten einschränken.

## Recht, eine Beschwerde bei einer Aufsichtsbehörde einzulegen

Du hast das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzulegen, insbesondere in dem Mitgliedstaat, in dem du deinen gewöhnlichen Aufenthaltsort oder deinen Arbeitsplatz hast oder in dem sich der Ort des behaupteten Verstoßes befindet, wenn du der Ansicht bist, dass die Erhebung und Verarbeitung personenbezogener Daten, die dich betreffen, ein Verstoß gegen die [DSGVO](#) darstellen.

## Recht, der Verarbeitung deiner Daten zu widersprechen

Du hast jederzeit das Recht, der Erhebung und Verarbeitung deiner personenbezogenen Daten aus Gründen, die mit deiner persönlichen Situation zusammenhängen, zu widersprechen, wenn wir uns bei der Erhebung und Verarbeitung auf unsere legitimen Interessen berufen (Art. 6 (1) f [DSGVO](#)).

## Recht, die Einwilligung jederzeit zu widerrufen

Du hast das Recht, deine Einwilligung jederzeit zu widerrufen, wenn du uns deine Einwilligung zur Erhebung und Verarbeitung deiner personenbezogenen Daten für einen oder mehrere spezifische Zwecke erteilt hast.



# Datenaufbewahrung

---



Adblock **Plus**

[Über](#)

[Beitragen](#)

[Hilfe](#)

[Deutsch \(DE\) ▾](#)

## Datenaufbewahrung

Daten im Zusammenhang mit Abonnement-Downloads, Prüfungen von Erweiterungsupdates, Notfallbenachrichtigungen sowie die vollständigen Berichte (und die damit verbundenen Daten) werden automatisch nach 30 Tagen gelöscht. Nur ein Teil der Daten wird länger aufbewahrt. Dies beinhaltet den Ländercode von Nutzern, die ein Problem gemeldet haben (wird aus der IP-Adresse extrahiert), zu Analyse Zwecken. Dieser wird getrennt von den vollständigen Berichten gespeichert, so dass er nach der Löschung der vollständigen Berichte nicht mit einer einzelnen Person verknüpft werden kann.



# Verständlichkeit, Offenheit, Transparenz

Mozilla  
#adblockplus  
Archives

adblockpluschrome[edge,next] Tristan Lucas 44766c66877b Issue 6717 - Part 2: run qunit in headless firefox  
https://hg.adblockplus.org/adblockpluschrome/rev/44766c66877b

tlucas  
snoack, \_hub\_ ^

GitLab Projects Groups Snippets Help Search or jump to... Sign in / Register

Filter by name... Last created

- adblockplus 3 14 23
- data 0 11 9
- websites 0 9 14
- specs 0 1 15
- external-dependencies 0 9 3  
Mirrored repos from external sources where we've some dependencies to.
- devops 0 7 5  
Development and Operations resources

ABP

View Issues Timeline Search

Custom Query

Group results by [dropdown] [dropdown] Show under each result: [checkbox] [checkbox] Review URL(s) Max items per page 100 Update

Results (1 - 100 of 1173)

Issue	Summary	Module	Status	Assignee	Type	Milestone
#6880	Make DevTools panel translatable	User-Interface	reviewing	greiner	change	P3
#6878	Implement IOFilterSearch	User-Interface	new		change	Unknown
#6877	python-abp can parse filter list lines as headers even when it's not the first line of the file	Scripts	new		defect	P3
#6875	Implement IOFilterList with infinite scroll	User-Interface	new		change	Unknown
#6874	Cannot configure SSH URL for building from repos	Automation	new		defect	Unknown
#6873	Scsp filter can make CSP options more insecure on Firefox 55 (5)	Platform	new		defect	Unknown
#6872	Sgenereblock filter applies to domain specific scsp filter	Unknown	new		defect	Unknown
#6871	Extension incorrectly accepts \$csp filters with blank value	Core	reviewing	jsonesen	defect	P2
#6870	Remove support for legacy ~abp-properties() syntax	Core	new		change	P2
#6869	Add richer DevTools panel reporting for snippets	User-Interface	new		change	Unknown
#6868	Rewrite filter with wildcard doesn't match end of URL	Core	reviewing	mjethani	defect	P3

#/revised Code Review Tool

Issue 29861585: Issue 6871 - Reject filters with blank CSPs

Description: Issue 6871 - Remove support for accepting empty CSP filters with blank values

Patch Set 1: Patch Set 3: Improves logic

Patch Set 3: Address P51 comments

Total comments: 2

Patch Set 4: Address P53 Comment

Created 3 minutes ago

Unified diffs	Side-by-side diffs	Deltas from patch set	State (+7 lines, -1 fix)	Patch
M lib/FilterClasses.js	View	1	1 chunk +5 lines, -1 line	0 comments Download
All test/FilterClasses.js	View	1 2 3	1 chunk +2 lines, -0 lines	0 comments Download

Messages

Total messages: 8

Messages: All Messages Collapse All Messages

Jon Sorenson 2 days ago (2018-09-22 19:40:50 UTC) #1

Jon Sorenson Added both of you to review since Marish is out till Monday and I want...

2 days ago (2018-09-22 19:30:11 UTC) #2

Manish Jethani We should add a test for this. You can search for "filter\_invalid\_csp" in test/FilterClasses.js

1 day, 5 hours ago (2018-09-23 14:31:31 UTC) #3

Manish Jethani You could rewrite the comment message as "Issue 6871 - Reject filters with blank..."

1 day, 5 hours ago (2018-09-23 14:31:31 UTC) #4

Jon Sorenson Will do, also I prefer your comment message so will update that as well.

1 day, 3 hours ago (2018-09-23 18:43:51 UTC) #5

Jon Sorenson Will do, also I prefer your comment message so will update that as well.

1 day, 3 hours ago (2018-09-23 18:43:51 UTC) #6

Manish Jethani On the other comment, @snoack's CFM link: https://adblockplus.org/2018-09-20-11-hours-22-minute-ago (2018-09-24 08:55:03 UTC) #7

Jon Sorenson 4 minutes ago (2018-09-24 20:12:49 UTC) #8


https://code-review.adblockplus.org/29861585/diff/29861585/1/test/FilterClasses.js

File test/FilterClasses.js (1 diff)

```
https://code-review.adblockplus.org/29861585/diff/29861585/1/test/FilterClasses.js
diff --git a/test/FilterClasses.js b/test/FilterClasses.js
index 1111111..2222222
--- a/test/FilterClasses.js
+++ b/test/FilterClasses.js
@@ -1,10 +1,10 @@
 test('filterClasses.js: 1:342: compareFilterTest: "blacsp"', {type:'invalid',
  'testInvalidCsp': 'reason:filter_invalid_csp'});
 on 2018/09/24 08:55:02, Manish Jethani wrote:
 => Let's also add a test for "blacsp" (without the "-").
```

# Transparenz

Note: An additional tab will temporarily open so the page you are on won't be affected by the Issue Reporter.

 Adblock Plus  
Issue reporter

## Enter comment

We encourage you to enter a valid email address so that we can contact you if there are questions about your report. It will also allow us to recognize your contributions and to prioritize them higher.

Email:

Anonymous submission

The text field below allows you to enter a comment to help us understand the issue. This step is optional but recommended if the problem isn't obvious. You can also review the report data before it is sent.

Comment (optional):

[Show report data](#)

[Privacy policy](#)

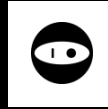
```
<request location="https://maps.googleapis.com/maps-api-v3/api/js/34/6/intl/
thirdParty="true" count="1"/>
<request location="https://maps.googleapis.com/maps/api/js/ViewportInfoServi
amp;2d6.859666569549518&amp;2m2&amp;1d50.80913528303121&amp;2d6.899335459853
amp;11e289&amp;callback=*&amp;client=*&amp;token=*" type="SCRIPT" docDomain=
<request location="https://maps.googleapis.com/maps/api/js/ViewportInfoServi
amp;2d6.859601473274324&amp;2m2&amp;1d50.81250409755823&amp;2d6.899180854295
callback=*&amp;client=*&amp;token=*" type="SCRIPT" docDomain="www.google.com
<filters>
<filter text="||googletagmanager.com/gtag/$third-party" subscriptions="https
<filter text="/piwik.$image,script,domain=-matomo.org|~piwik.org" subscrip
hitCount="1"/>
<filter text=".net/p.gif?" subscriptions="https://easylist-downloads.adblock
<window url="https://www.eco.de/events/internet-security-days-2018/" />
<subscriptions>
<subscription id="https://easylist-downloads.adblockplus.org/easylist.txt" v
119773" softExpiration="85579" hardExpiration="53027" downloadStatus="synchr
<subscription id="https://easylist-downloads.adblockplus.org/easylistgermany
lastDownloadSuccess="-134591" softExpiration="41528" hardExpiration="38209" />
<subscription id="https://easylist-downloads.adblockplus.org/exceptionrules
lastDownloadSuccess="-127391" softExpiration="80024" hardExpiration="45409" />
<subscription id="https://easylist-downloads.adblockplus.org/easyprivacy.txt
lastDownloadSuccess="-127390" softExpiration="60186" hardExpiration="45410" />
<subscription id="https://easylist-downloads.adblockplus.org/fanboy-social.t
lastDownloadSuccess="-3791" softExpiration="75594" hardExpiration="169009" />
<subscription id="https://easylist-downloads.adblockplus.org/abp-filters-ant
lastDownloadSuccess="-3792" softExpiration="173" hardExpiration="3408" downl
<adblock-plus version="3.3.1" locale="en-US" />
<application name="Firefox" version="61.0.1" vendor="" userAgent="Mozilla/5.
<platform name="Gecko" version="61.0" />
<email/></report>
```

# Zusammengefasst

—

**Fragen? Diskussion!**

—



# THANK YOU!

---

Jutta Horstmann  
Head of Filters

[j.horstmann@eyeo.com](mailto:j.horstmann@eyeo.com)

Twitter: @smphr

## HEADQUARTERS

eyeo GmbH  
Lichtstraße 25  
D-50825 Köln

## BERLIN OFFICE

eyeo GmbH  
Zimmerstraße 69  
D-10117 Berlin

## MALMÖ OFFICE

Flattr AB  
Box 4111  
S-23312 Malmö

