EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

PROTECTION OF PERSONAL DATA PROCESSED THROUGH WEB SERVICES PROVIDED BY EU INSTITUTIONS

Xabier Lareo

44th DPO Meeting

Brussels, 12 December 2018

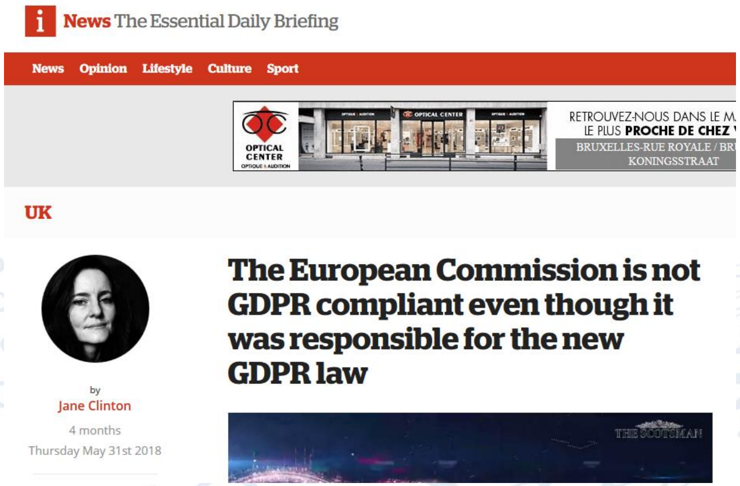
EU INSTITUTIONS OBLIGATIONS

When processing data through their web services, EU Institutions (EUIs) must provide their visitors:

- ✓ Information about the processing of their personal data.
- ✓ Information about the data stored and collected in their devices
- ✓ A meaningful method for accepting and rejecting the storing and collection of data in their devices.
- ✓ Safe transmission channels and servers to ensure personal are securely transferred and processed.

NOT JUST A MATTER OF COMPLIANCE

When dealing with privacy and data protection, compliance issues can quickly become reputational issues.



i News The Essential Daily Briefing

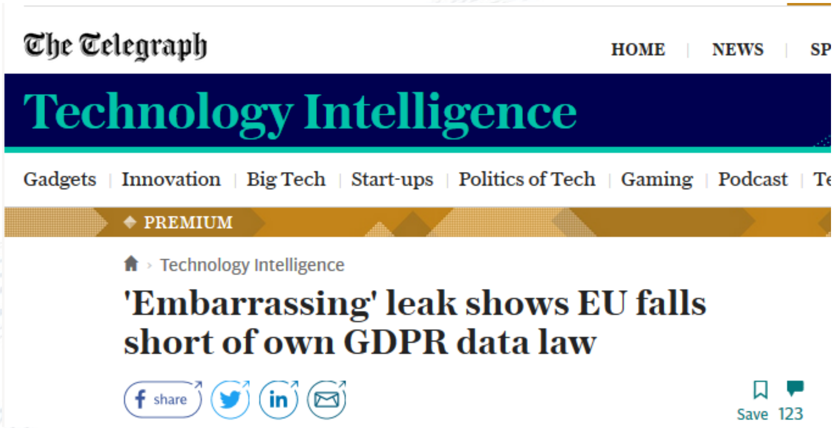
News Opinion Lifestyle Culture Sport

UK

The European Commission is not GDPR compliant even though it was responsible for the new GDPR law

by
Jane Clinton
4 months
Thursday May 31st 2018

THE SCOTSMAN



The Telegraph HOME | NEWS | SP

Technology Intelligence

Gadgets | Innovation | Big Tech | Start-ups | Politics of Tech | Gaming | Podcast | Te

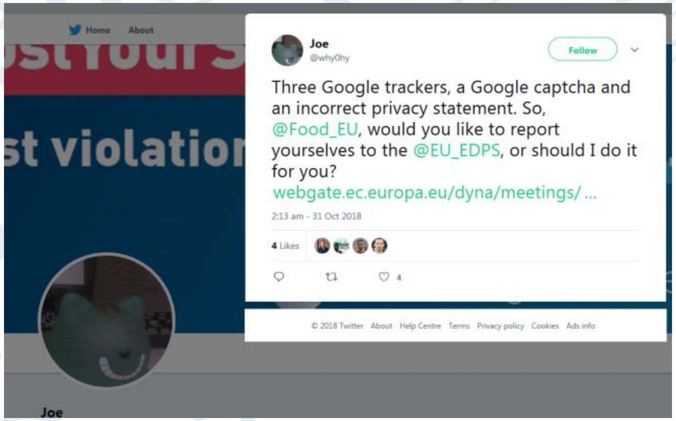
PREMIUM

Technology Intelligence

'Embarrassing' leak shows EU falls short of own GDPR data law

share

Save 123



Home About

Joe
@why0hy
Follow

Three Google trackers, a Google captcha and an incorrect privacy statement. So, @Food_EU, would you like to report yourselves to the @EU_EDPS, or should I do it for you?
webgate.ec.europa.eu/dyna/meetings/ ...

2:13 am - 31 Oct 2018

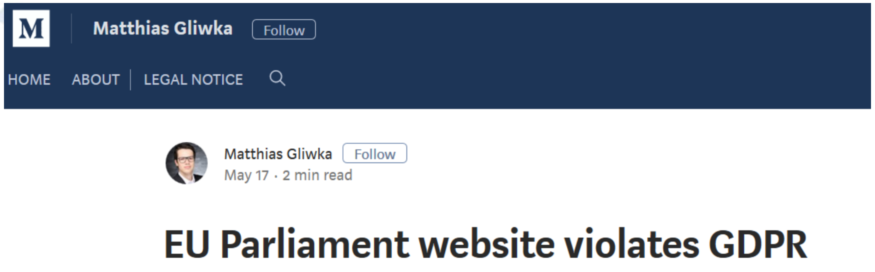
4 Likes

4

© 2018 Twitter About Help Centre Terms Privacy policy Cookies Ads info

st violation

Joe



M Matthias Gliwka Follow

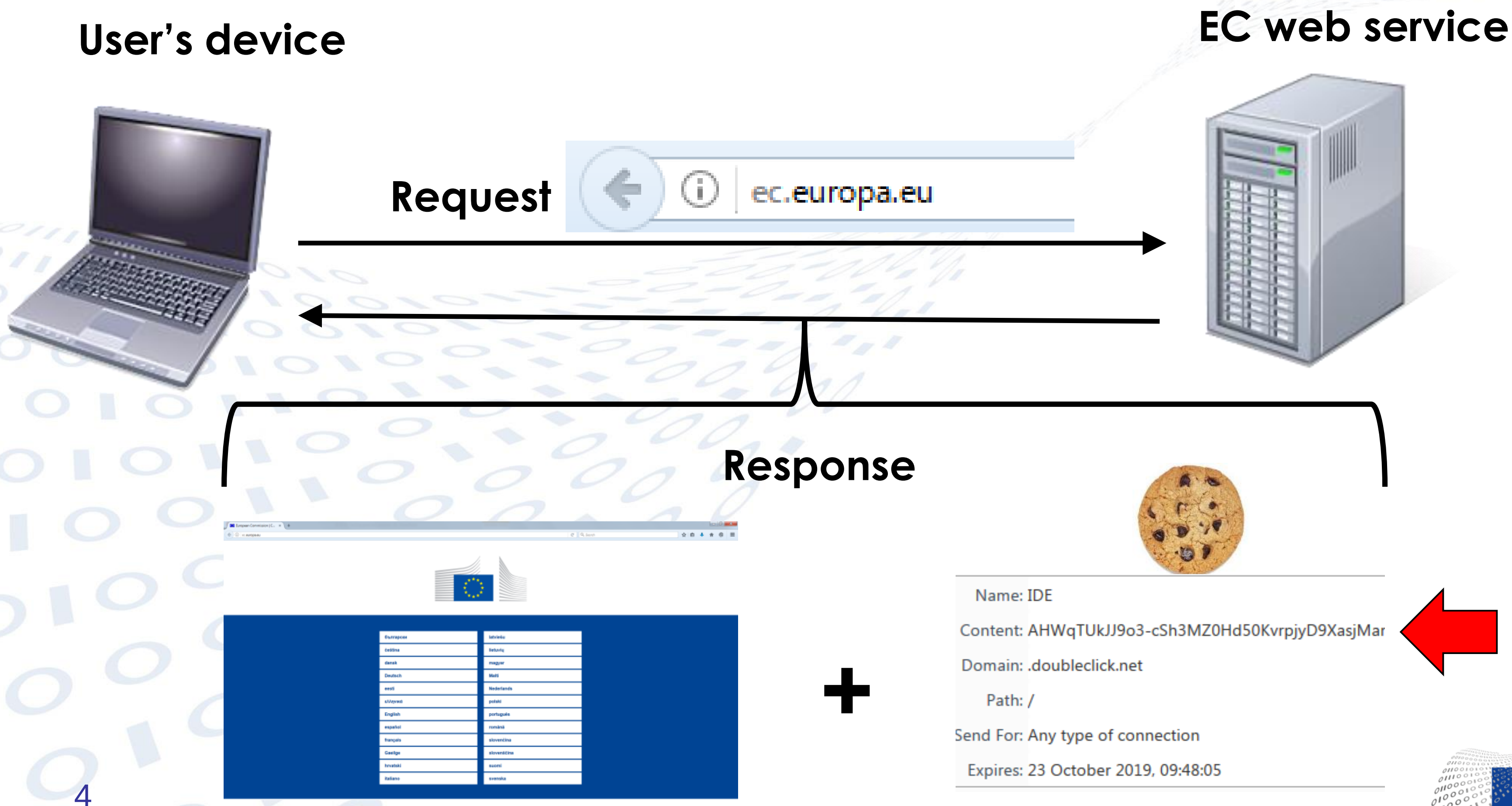
HOME ABOUT LEGAL NOTICE

Matthias Gliwka Follow
May 17 · 2 min read

EU Parliament website violates GDPR

COOKIE BASED TRACKING

When visitors access web services, they could receive one or more cookies with a web page.



Name: IDE

Content: AHWqTUkJJ9o3-cSh3MZ0Hd50KvrpjyD9XasjMar

Domain: .doubleclick.net

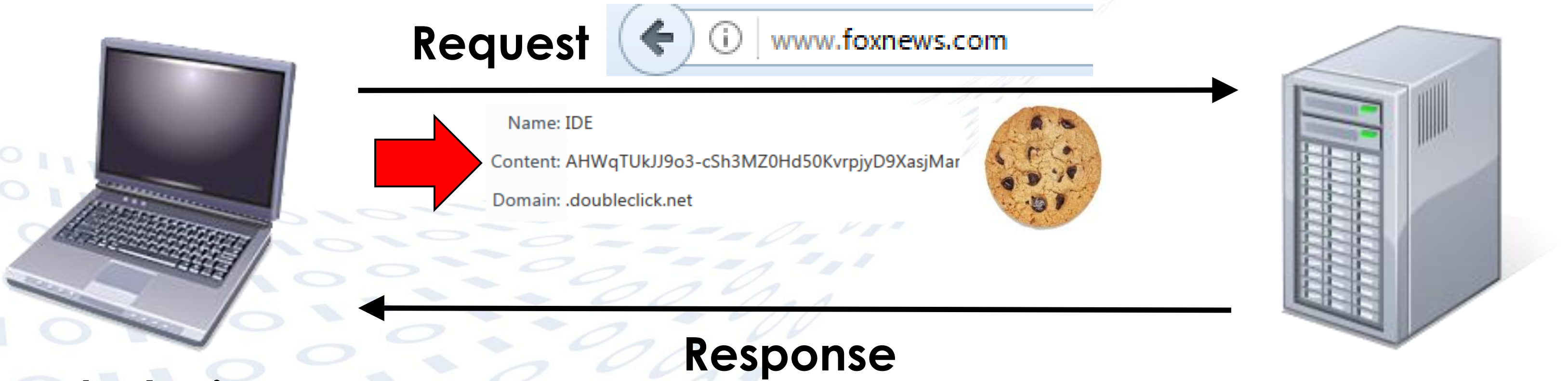
Path: /

Send For: Any type of connection

Expires: 23 October 2019, 09:48:05

COOKIE BASED TRACKING

The cookie previously downloaded is sent every time a resource from doubleclick.net is embedded in a visited web page. That way DoubleClick can register all the websites visited using the unique identifier in the DoubleClick cookie “IDE”.

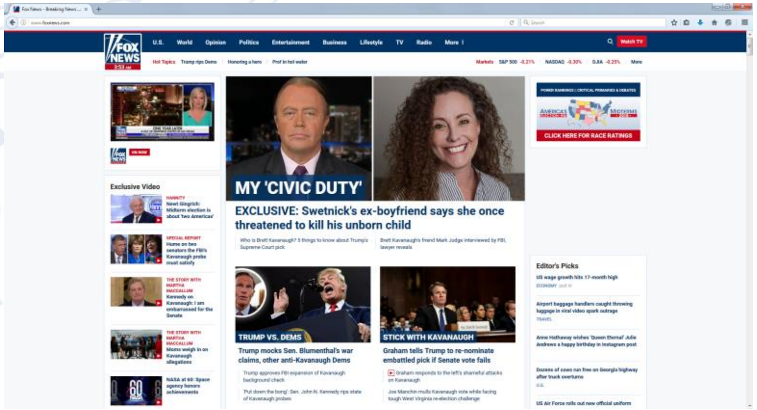


Name: IDE

Content: AHWqTUkJJ9o3-cSh3MZ0Hd50KvrpjyD9XasjMar

Domain: .doubleclick.net

User’s device



MY 'CIVIC DUTY'

EXCLUSIVE: Swetnick's ex-boyfriend says she once threatened to kill his unborn child

TRUMP VS. DEMS

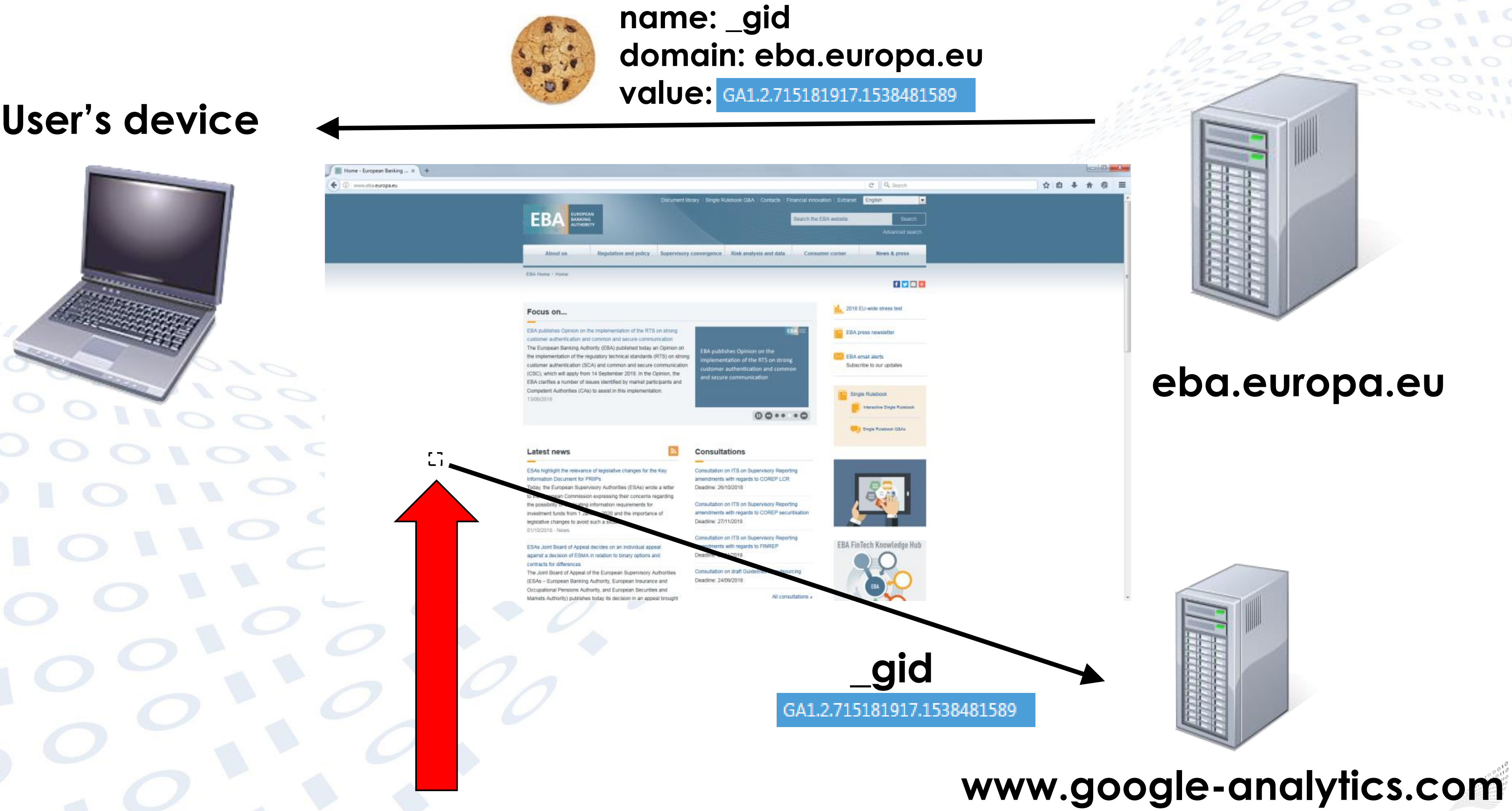
Trump mocks Sen. Blumenthal's war claims, other anti-Kavanaugh Dems

STICK WITH KAVANAUGH

Graham tells Trump to re-nominate embattled pick if Senate vote fails

Fox News

WEB BEACONS AND TRACKING



name: _gid
domain: eba.europa.eu
value: GA1.2.715181917.1538481589

User's device

eba.europa.eu

_gid
GA1.2.715181917.1538481589

www.google-analytics.com

Focus on...

EBA publishes Opinion on the implementation of the RTS on strong customer authentication and common and secure communication

The European Banking Authority (EBA) published today an Opinion on the implementation of the regulatory technical standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC), which will apply from 14 September 2019. In the Opinion, the EBA clarifies a number of issues identified by market participants and Competent Authorities (CAs) to assist in this implementation.
13/06/2018

EBA publishes Opinion on the implementation of the RTS on strong customer authentication and common and secure communication

Latest news

ESAs highlight the relevance of legislative changes for the Key Information Document for PRIIPs

Today, the European Supervisory Authorities (ESAs) wrote a letter to the European Commission expressing their concerns regarding the possibility of duplicating information requirements for investment funds from 1 January 2020 and the importance of legislative changes to avoid such a situation.
01/10/2018 - News

ESAs Joint Board of Appeal decides on an individual appeal against a decision of ESMA in relation to binary options and contracts for differences

The Joint Board of Appeal of the European Supervisory Authorities (ESAs – European Banking Authority, European Insurance and Occupational Pensions Authority, and European Securities and Markets Authority) publishes today its decision in an appeal brought

Consultations

Consultation on ITS on Supervisory Reporting amendments with regards to COREP LCR
Deadline: 26/10/2018

Consultation on ITS on Supervisory Reporting amendments with regards to COREP securitisation
Deadline: 27/11/2018

Consultation on ITS on Supervisory Reporting amendments with regards to FINREP
Deadline: [illegible]/2018

Consultation on draft Guidelines on outsourcing
Deadline: 24/09/2018

All consultations »

THE “MOST WANTED” LIST

Some third-party components are well-known for tracking visitors of those websites they are embedded in. The most popular in EUI web services are:

- Video streaming
- AdNetworks
- Web Analytics
- Social networks and related
- Content delivery networks
- Other “free” services

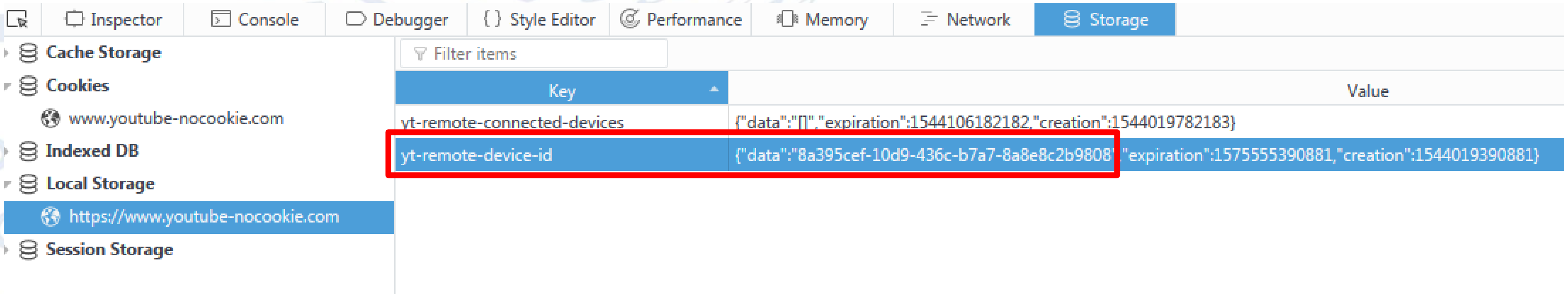
YOUTUBE TRACKING

- Trackers associated with the video streaming service YouTube have been found in the analysed EUI web services.
- If not properly configured, embedded YouTube players download 4 cookies on visitors’ devices.
- YouTube does not provide any information on the purpose of those cookies.
- At least 2 of the cookies contain identifiers that could be used to track users’ behaviour when browsing the Internet after visiting the EUI web service.

RECOMMENDATIONS

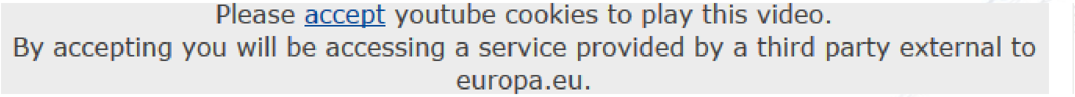
- Choose a video streaming service that does not track users by default and allows to fully shut down user tracking.

- YouTube has a privacy enhanced mode that uses no HTTP cookie. However, this mode still stores as a HTML 5 Local Storage a device identifier that allows to track the visitor.



Key	Value
yt-remote-connected-devices	{"data":"[]","expiration":1544106182182,"creation":1544019782183}
yt-remote-device-id	{"data":"8a395cef-10d9-436c-b7a7-8a8e8c2b9808","expiration":1575555390881,"creation":1544019390881}

BLOCKING PLUGIN



Please accept youtube cookies to play this video.
By accepting you will be accessing a service provided by a third party external to europa.eu.

A plugin that blocks the video streaming service until the user has explicitly consented the data storage could be a solution.

However, this option might not be privacy friendly, since it forces visitors to accept the privacy policy of a third party in order to access the content.

DOUBLECLICK TRACKING

- DoubleClick is an advertising company owned by Google.
- Trackers associated with DoubleClick have been found in the EUI analysed web services.
- DoubleClick also uses Google Analytics identifiers to track visitors.
- There is no reason to have EUI’s visitors tracked by any advertising company.

RECOMMENDATIONS

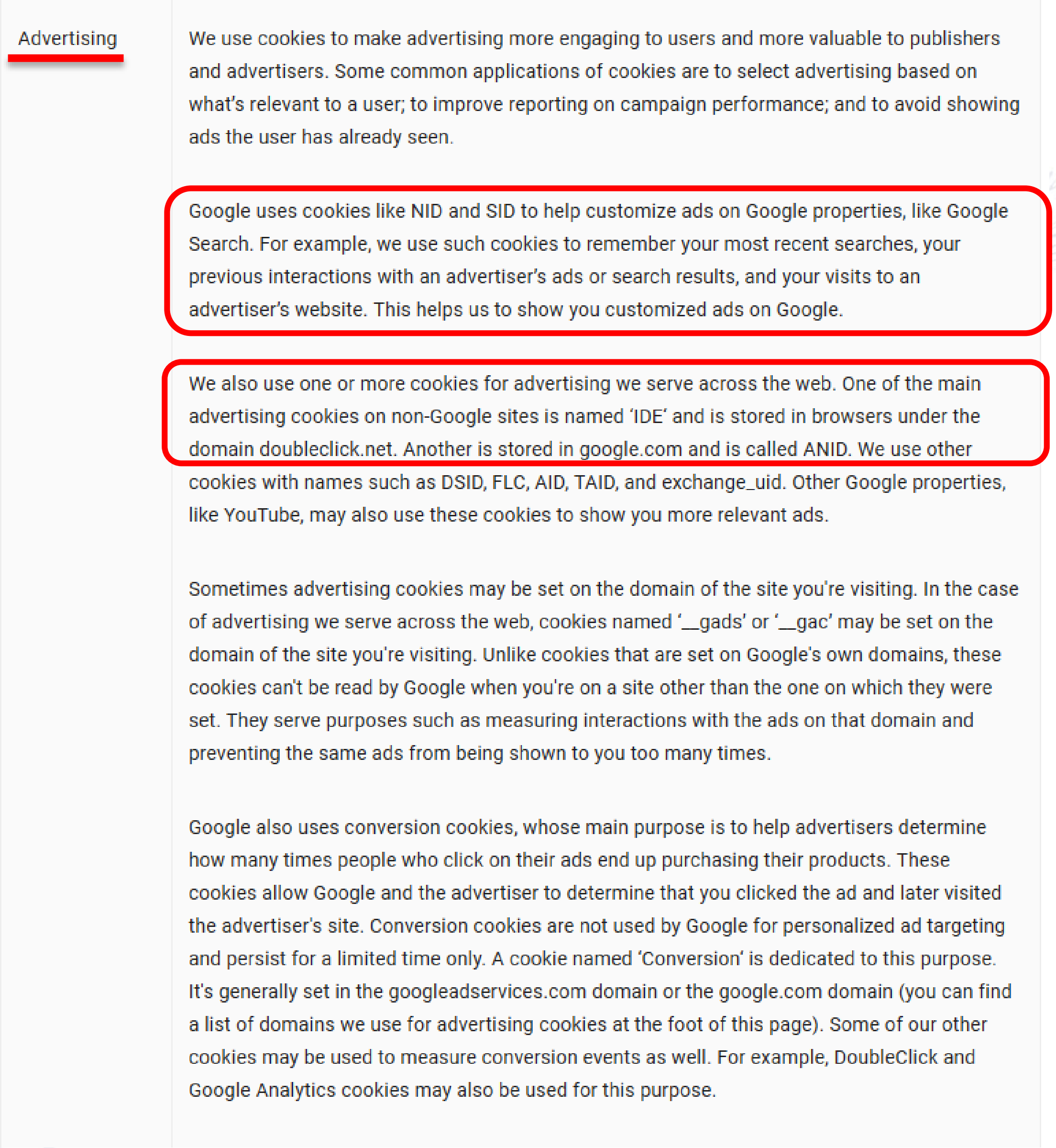
- No cookies or HTTP requests should be made to DoubleClick or other known advertising services.
- DoubleClick is often embedded in web services by other third-party services without the knowledge of the controller.

EUI's should closely check the behaviour of third-party components included in their web services to ensure that no unwanted trackers are included.

GOOGLE MAPS TRACKING

- Google Maps is a widely used mapping service, but it also installs cookies on visitors' devices.
- Google has declared that at least one of those cookies is used for profiling and advertising.
- Trackers associated with the cookie used by Google Maps to track users have been found in the EUI analysed web services.

2 – NID'S PURPOSE IS ADVERTISEMENT AND PROFILING



Advertising

We use cookies to make advertising more engaging to users and more valuable to publishers and advertisers. Some common applications of cookies are to select advertising based on what's relevant to a user; to improve reporting on campaign performance; and to avoid showing ads the user has already seen.

Google uses cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, we use such cookies to remember your most recent searches, your previous interactions with an advertiser's ads or search results, and your visits to an advertiser's website. This helps us to show you customized ads on Google.

We also use one or more cookies for advertising we serve across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. We use other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show you more relevant ads.

Sometimes advertising cookies may be set on the domain of the site you're visiting. In the case of advertising we serve across the web, cookies named '__gads' or '__gac' may be set on the domain of the site you're visiting. Unlike cookies that are set on Google's own domains, these cookies can't be read by Google when you're on a site other than the one on which they were set. They serve purposes such as measuring interactions with the ads on that domain and preventing the same ads from being shown to you too many times.

Google also uses conversion cookies, whose main purpose is to help advertisers determine how many times people who click on their ads end up purchasing their products. These cookies allow Google and the advertiser to determine that you clicked the ad and later visited the advertiser's site. Conversion cookies are not used by Google for personalized ad targeting and persist for a limited time only. A cookie named 'Conversion' is dedicated to this purpose. It's generally set in the googleadservices.com domain or the google.com domain (you can find a list of domains we use for advertising cookies at the foot of this page). Some of our other cookies may be used to measure conversion events as well. For example, DoubleClick and Google Analytics cookies may also be used for this purpose.

https://policies.google.com/technologies/types

RECOMMENDATIONS

There is no reason to have visitors of EUI’s web services tracked for advertisement purposes.

- Choose a mapping service that does not track users (e.g. EC Webtool Map or OpenStreetMap).
- Substitute the interactive maps for images of he maps.

GOOGLE ANALYTICS

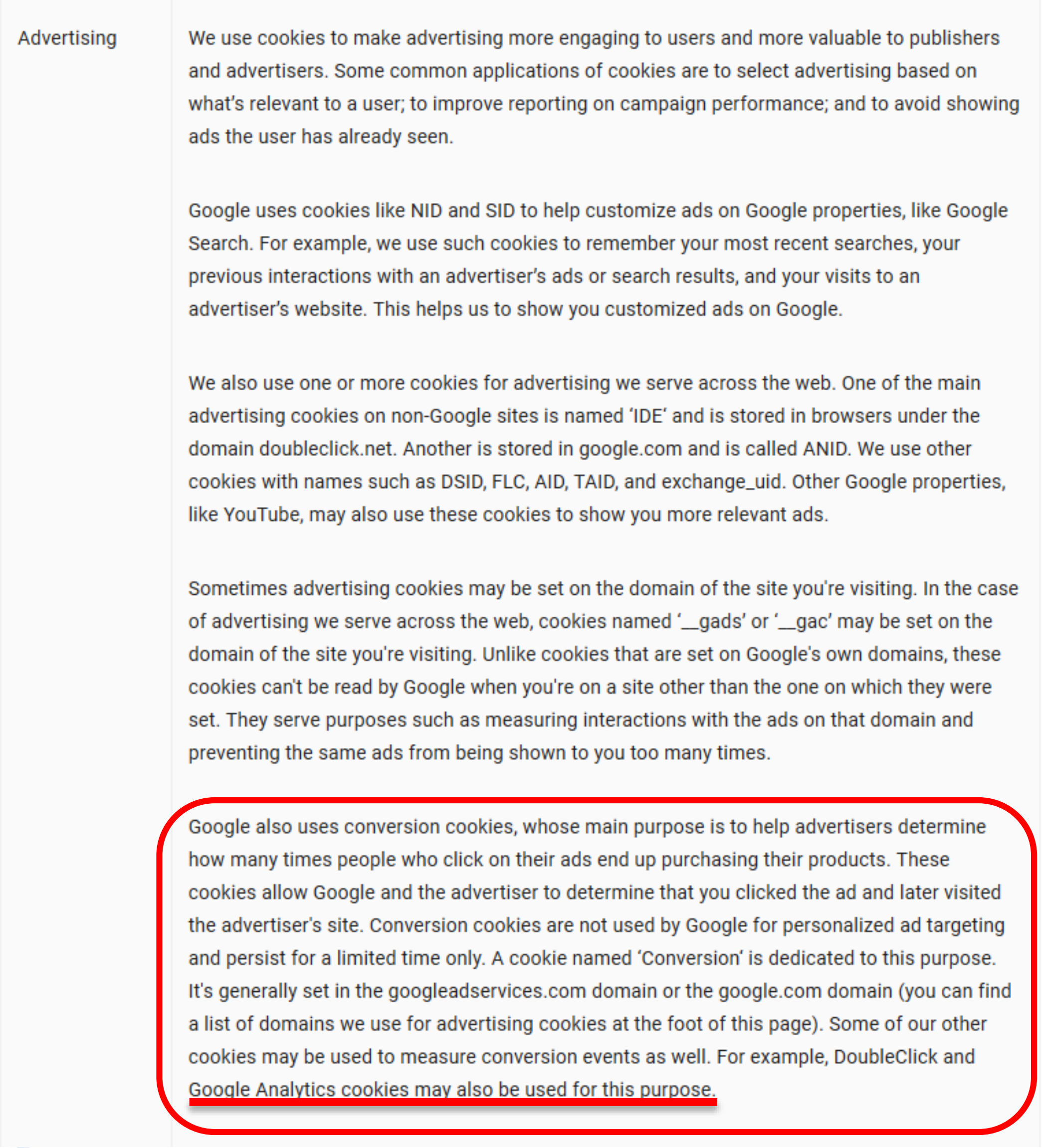
- Google Analytics is used by some of the EUI analysed web services.

- Even if Google Analytics identifiers are stored in cookies on the EUI’s domain, they are controlled by a third party and require the user’s consent

- Google Analytics is a service provider for millions of web sites. Google’s privacy policy does not prevent that data collected from visitors of all web sites is used for behavioural advertising.

- Since the cookies are stored on the EUI’s domain, there is no easy way for the users to reject their use.

2 – GOOGLE ANALYTICS MAY BE USED FOR ADVERTISEMENT AND PROFILING



Advertising

We use cookies to make advertising more engaging to users and more valuable to publishers and advertisers. Some common applications of cookies are to select advertising based on what's relevant to a user; to improve reporting on campaign performance; and to avoid showing ads the user has already seen.

Google uses cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, we use such cookies to remember your most recent searches, your previous interactions with an advertiser's ads or search results, and your visits to an advertiser's website. This helps us to show you customized ads on Google.

We also use one or more cookies for advertising we serve across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. We use other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show you more relevant ads.

Sometimes advertising cookies may be set on the domain of the site you're visiting. In the case of advertising we serve across the web, cookies named '__gads' or '__gac' may be set on the domain of the site you're visiting. Unlike cookies that are set on Google's own domains, these cookies can't be read by Google when you're on a site other than the one on which they were set. They serve purposes such as measuring interactions with the ads on that domain and preventing the same ads from being shown to you too many times.

Google also uses conversion cookies, whose main purpose is to help advertisers determine how many times people who click on their ads end up purchasing their products. These cookies allow Google and the advertiser to determine that you clicked the ad and later visited the advertiser's site. Conversion cookies are not used by Google for personalized ad targeting and persist for a limited time only. A cookie named 'Conversion' is dedicated to this purpose. It's generally set in the googleadservices.com domain or the google.com domain (you can find a list of domains we use for advertising cookies at the foot of this page). Some of our other cookies may be used to measure conversion events as well. For example, DoubleClick and Google Analytics cookies may also be used for this purpose.

https://policies.google.com/technologies/types

RECOMMENDATIONS

- Third-party web analytics require visitors’ consent and EUI’s should ensure that such consent is obtained before collecting any visitors’ data.

- The European Commission provides a web analytics service, Europa Analytics, which is more privacy-friendly than commercial alternatives.

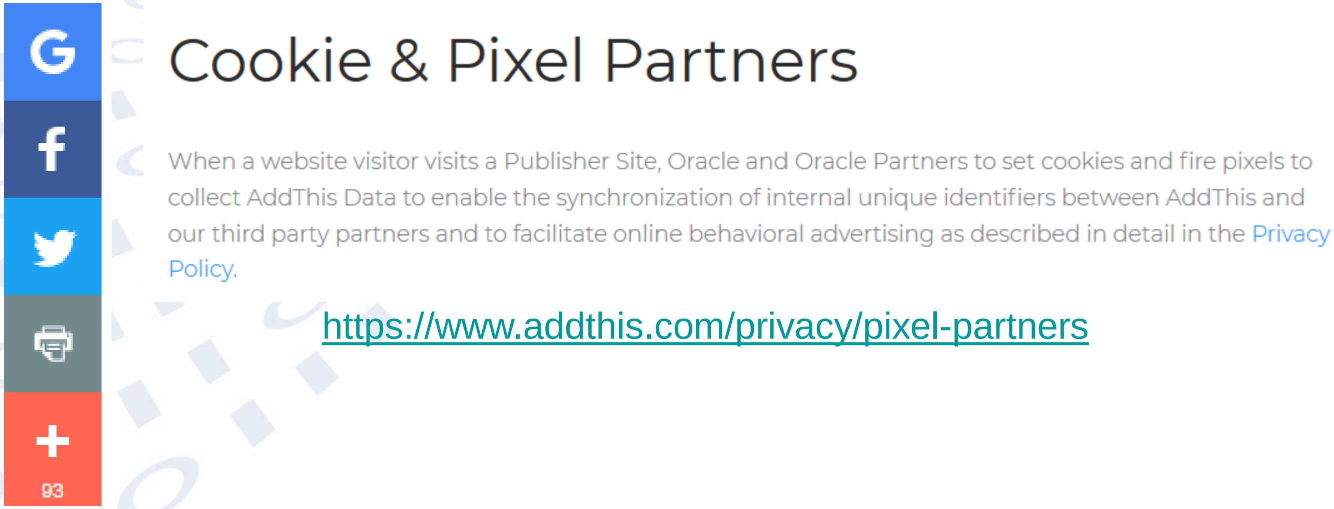
- If EUIs prefer commercial alternatives, the setup of the service must ensure that informed visitor consent is obtained prior to any tracking.

ADDTHIS TRACKING

- AddThis offers a tool to facilitate sharing online content of web.

- Trackers associated with AddThis have been found in some of the EUI analysed web services.

- The use of AddThis in an EUI web service implies not only the tracking of it’s visitors by AddThis, but also by 44 so-called “Pixel Partners” (advertising partners).



Cookie & Pixel Partners

When a website visitor visits a Publisher Site, Oracle and Oracle Partners to set cookies and fire pixels to collect AddThis Data to enable the synchronization of internal unique identifiers between AddThis and our third party partners and to facilitate online behavioral advertising as described in detail in the Privacy Policy.

https://www.addthis.com/privacy/pixel-partners

RECOMMENDATIONS

- AddThis is particularly harmful for the privacy of the web service visitors, because it allows many different advertising companies to track them.

- It is possible to share online content on social networks directly and without using third-party tools.

- In case EUI's prefers to have unique control to facilitate their online content sharing, they should choose a service provider that does not track their visitors.

- The European Commission provides several privacy friendly Webtools that could be used for this purpose like Social bookmarking and networking or Social Media Kit.

CONTENT DELIVERY NETWORK TRACKING

- A Content Delivery Network (CDN) is a geographically distributed network of servers that allow to improve the availability and performance of web services.

- Trackers associated with CloudFlare, one of the main CDNs, have been found in some of the EUI analyzed web services.

- According to CloudFlare’s cookie Policy “*as part of our Service, we may place a “__cfduid” cookie on the computers of End Users (as that term is defined in our Privacy Policy). We do this in order* ***to identify malicious visitors to our Customers’ websites, to reduce the chance of blocking legitimate users, and to provide customized services.***”.

RECOMMENDATIONS

- Improving the availability and the performance of the EUI’s web services should not involve the tracking of its visitors.

- Tracking conducted by third parties like Content Delivery Networks requires the informed consent of the visitors and EUI’s should ensure that no tracking takes place before consent is obtained.

PERSONAL DATA SECURITY

- EUI’s must ensure the security of the personal data of their visitors both while being transmitted and while stored in the EUI’s servers.

✗ Any data transmitted over a non-secured channel (HTTP) can be accessed by other users sharing the network (e.g. an open Wi-Fi or a corporate network).

✓ Data transmitted over an encrypted channel (HTTPS/TLS) can only be accessed by the sender and the receiver.

PERSONAL DATA SECURITY

- The use of a HTTPS connection requires digital certificates that will also allow to ascertain that the visited web service is the right one and not a fake (phishing).
- Even if individual web pages of a web service do not process personal data as such, HTTPS connections prevent any potential attacker from monitoring the visitors browsing history.

RECOMMENDATIONS

- Provide secure connections to EUIs web services by using HTTPS and TLS protocols.
- Redirect any incoming HTTP connection to HTTPS.
- Provide secure connections to the entire web service and particularly to those pages processing personal data.
- Conduct regular vulnerability assessments to detect any potential threat to the personal data processed by the EUIs web services. Afterwards, evaluate de detected risks and elaborate an action plan to address any significant risks.

STEPS TO COMPLIANCE

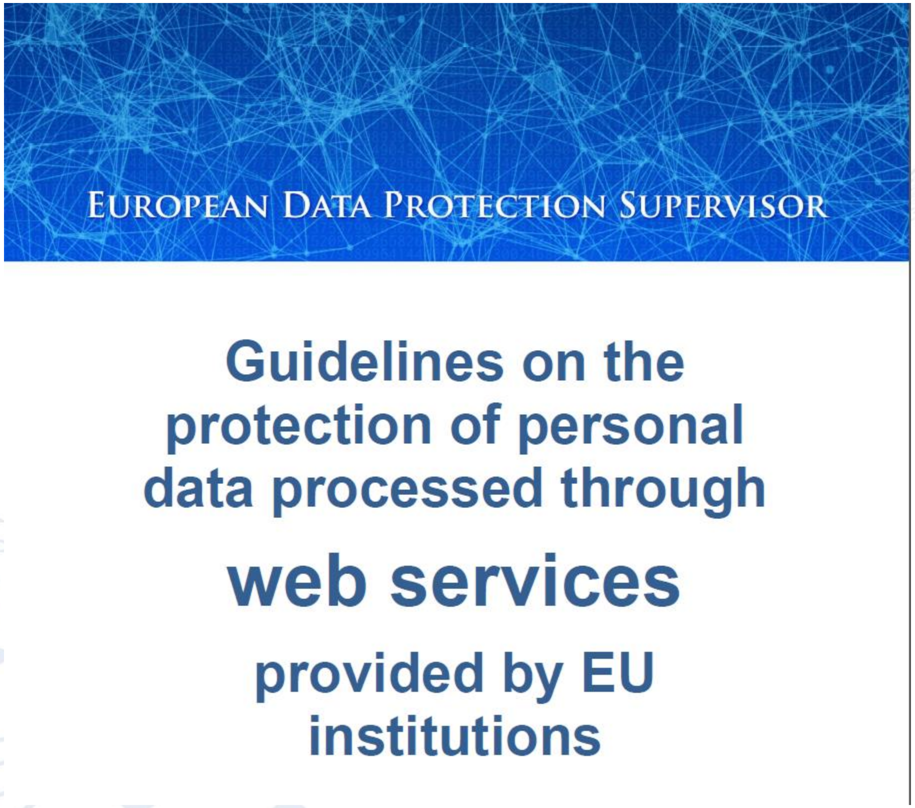
1. Minimize the personal data knowingly processed by EUI web services (e.g. collected by web forms).

2. Draft an inventory of third-party services embedded in EUI web services and analyse their privacy impact. Based on the analysis, take steps to ensure compliance with ePrivacy and data protection regulatory framework.

3. Provide HTTPS (encrypted) connections for the web service and ensure that any HTTP (non-encrypted) connection is redirected to HTTPS.

4. Conduct a vulnerability assessment on the servers that process personal data for the web service.

EDPS Guidelines



EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on the protection of personal data processed through

web services

provided by EU institutions

https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_web_services_en.pdf

Thanks!

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS