

THESSALONIKI  
**digital analytics**  
MEETUP

# Practical steps to GDPR compliance

Thessaloniki Meetup #3

22 Nov 2017



# Data Collector's Obligations

What do you need to do, when you collect data?

# Data collector's obligations

## 1. Get clear consent from data subject before tracking

- Do you respect DNT option?
- Do you inform all new website visitors?

## 2. Keep records of consent from each data subject

- Can you prove when and if a data subject gave consent?

## 3. Respect sensitive data subjects and sensitive data

- Do you know what is considered sensitive?

## 4. Notify in case of data breach

- Do you have a process of notifying visitors if you any of the data get leaked?

## 5. Inform data subjects in “plain language”

- Is it easy for someone to understand how you use collected traffic data?
- Is it clear what type of data you capture?

# 1. Get clear consent

## Active opt-in

- No pre-ticked checkboxes
- User interaction to opt-in

## Granular consent

- Multiple consent checkboxes
- One checkbox for each processing type

## Named

- Explicitly mention 3<sup>rd</sup> parties
- Clearly mention your organization

## Up-to-date

- Previous consent (non-compliant with GDPR) is considered invalid

## Easy to withdraw

- Easy to find consent withdrawal
- Inform people about this option

## Unbundled

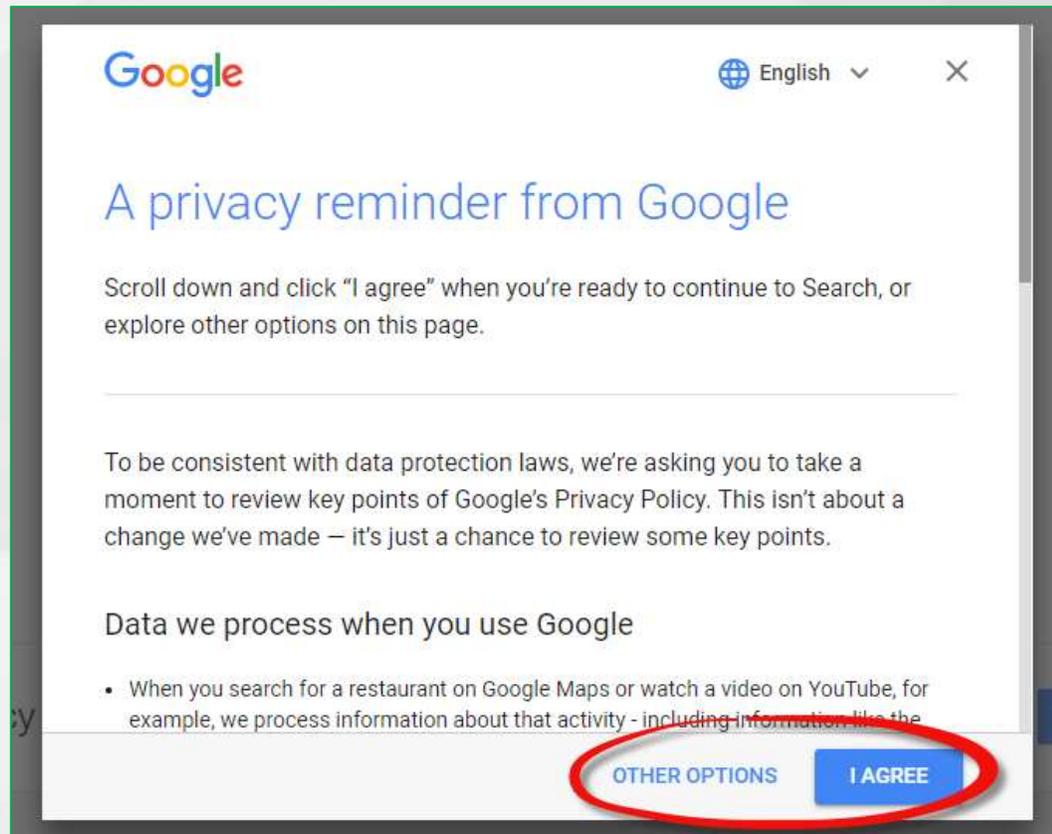
- Unbundle consent with terms & conditions
- Allow service usage even without consent

## Earn people's trust

- Organizations with strong customer relationships are favored

# Consent examples

## Compliant



The screenshot shows a Google privacy reminder dialog box. At the top left is the Google logo, and at the top right is a language selector set to "English" with a close button (X). The main heading is "A privacy reminder from Google". Below it, the text reads: "Scroll down and click 'I agree' when you're ready to continue to Search, or explore other options on this page." A horizontal line separates this from the next section, which states: "To be consistent with data protection laws, we're asking you to take a moment to review key points of Google's Privacy Policy. This isn't about a change we've made – it's just a chance to review some key points." The next section is titled "Data we process when you use Google" and contains a bullet point: "When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity - including information like the...". At the bottom, there are two buttons: "OTHER OPTIONS" and "I AGREE". The "I AGREE" button is highlighted with a red circle.

## Non-compliant

WE'RE USING COOKIES TO IMPROVE YOUR EXPERIENCE. [CLICK HERE TO FIND OUT MORE.](#)

Amazon uses cookies. [What are cookies?](#)

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. [Find out more here](#) ✕

### Privacy policy and cookies

We use [cookies and similar technologies](#) ("cookies") to help give you the best experience on our site and to show you relevant advertising. If you continue to use this site, we'll assume that you're happy to receive all cookies.

[Accept & close](#) ✕

# Consent and monitoring workarounds

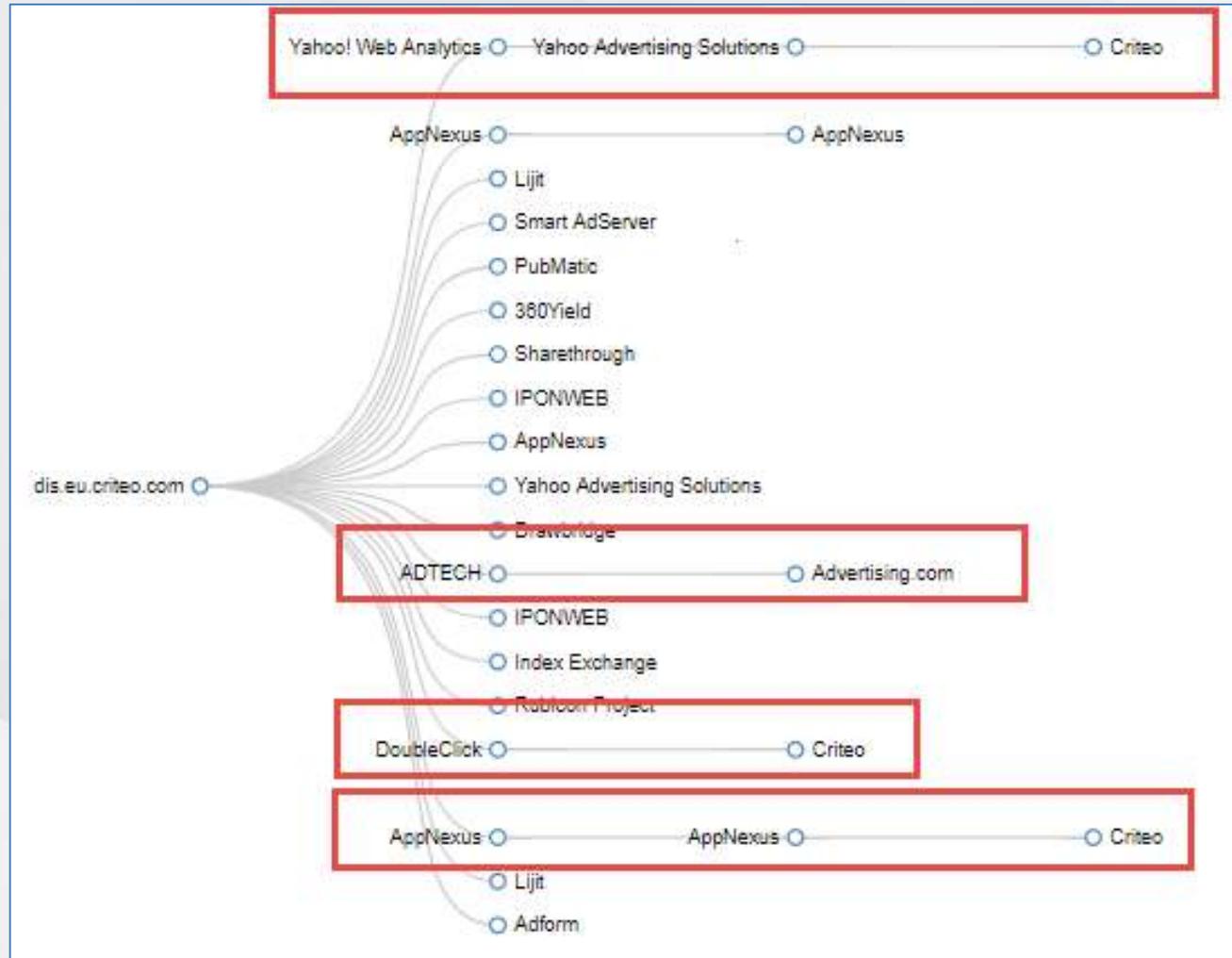
## Solutions available

- Enshighten [privacy](#)
  - Firewall-like approach
- Tealium [privacy addons](#)
  - Intuitive tag management
- Evidon's [consent form](#)
  - Auditing tools
  - Consent form generator

## Web tracking issues

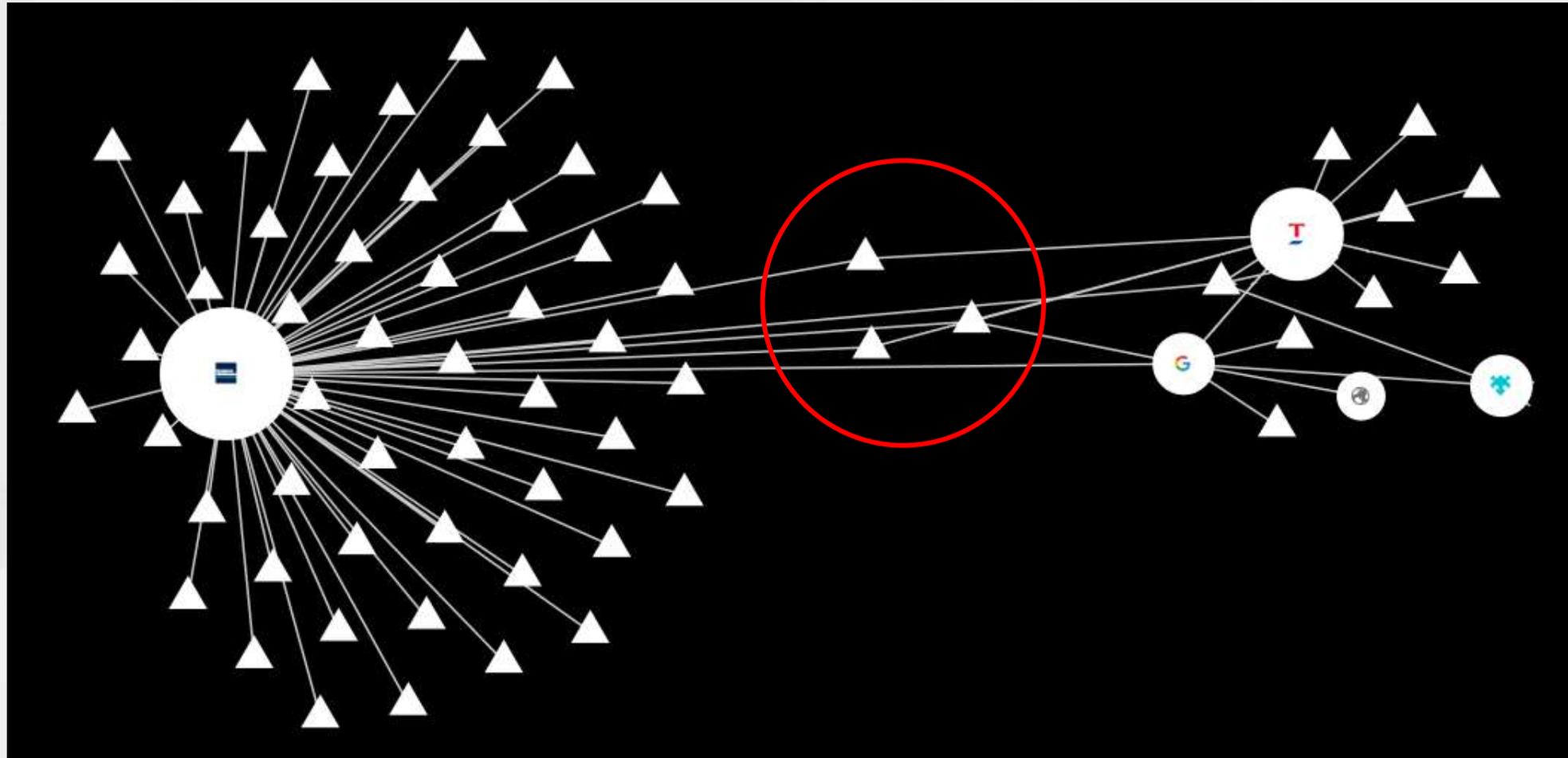
- Data leakage
- Tag piggybacking
- Personal data capturing
- Sharing with 3<sup>rd</sup> parties

# Tag piggybacking



Tag explorer addon: <https://chrome.google.com/webstore/detail/tag-explorer/obhceflecohdhjjomleeakkogaichoo>

# Sharing with 3<sup>rd</sup> parties



Lightbeam addon: <https://addons.mozilla.org/en-US/firefox/addon/lightbeam/>

# What to keep when documenting 3<sup>rd</sup> parties dependencies

1. Technology
2. Vendor
3. Vendor Contact
4. Business Owner
5. Purpose
6. Where is data stored?
7. Who has access?
8. What PII does this contain?
9. Compliance status
10. Last Verified

*\*Include all details in DPA (Data Processing Agreement)*

[Sample DPA](#)

## 2. Keep record of consent



### Possible workarounds:

- Track consent & consent type in analytics tools
- Create easy process to exclude visitors with no consent
- Ensure consent type is compatible with each data analysis

# 3. Respect sensitive data

- Special rules apply when collecting:
  - Genetic / biometric data / Health data
  - Data for users under 16 years old ([Silicon valley S04E03](#))
  - Political / racial / religious personal data

# 4. Data breach notification

## Possible workarounds:

- Enforce strong password policies
- Restrict access to personal data
- Monitor access / usage logs for data breaches
- Create process for data breach notifications
- Assign DPO (Data Protection Officer)

*\*In case of data breach inform impacted people within 72 hours*

# 5. Inform in “plain language”

- Readability testing [algorithms](#):
  - Flesch Reading Ease
  - Flesch-Kincaid Grade Level
- Scoring based on average number of syllables per word and sentence length
- Use online tool to evaluate content

The image shows a screenshot of the Hemingway editor interface. At the top, there is a 'Write' and 'Edit' button. Below it, a 'Readability' section shows a green-to-red gradient bar with a green triangle indicating a score of 'Grade 7' and 'Good'. To the right, a box displays statistics: 'Paragraphs: 6', 'Sentences: 10', 'Words: 123', and 'Characters: 584'. The main text area shows a sample paragraph with various highlights: yellow for long sentences, red for complex sentences, blue for adverbs, and green for passive voice. On the right side, a list of issues is shown with colored boxes: '1 of 10 sentences are hard to read.' (yellow), '1 of 10 sentences are very hard to read.' (red), '1 adverbs. Aim for 2 or fewer.' (blue), '1 words or phrases can be simpler.' (purple), and '1 uses of passive voice. Aim for 2 or fewer.' (green). Red arrows point from the main interface to the summary boxes.

[Hemingway editor](#)

# Privacy policy readability analysis

## Google search

**Hemingway**  
*Editor*

---

**Readability**

Grade 9   
Good

---

Words: 378  
Show More ▾

- 1 adverb, meeting the goal of 6 or fewer.
- 2 uses of passive voice, meeting the goal of 5 or fewer.
- 1 phrase has a simpler alternative.
- 4 of 23 sentences are hard to read.
- 4 of 23 sentences are very hard to read.

**Compliant**

## Amazon UK

**Hemingway**  
*Editor*

---

**Readability**

Grade 13   
OK. Aim for 9.

---

Words: 941  
Show More ▾

- 5 adverbs, meeting the goal of 8 or fewer.
- 5 uses of passive voice, meeting the goal of 10 or fewer.
- 6 phrases have simpler alternatives.
- 6 of 49 sentences are hard to read.
- 17 of 49 sentences are very hard to read.

**Non-compliant**

# Data subject's rights

What can you request when someone collects your data?

# Data subject's rights

## 1. Right to be informed

- What data are you collecting on me?
- How are you using that data?

## 2. Right to access

- Show me the data you have on me!

## 3. Right to data portability

- Give me the data you have on me

## 4. Right to stop processing

- Stop doing that with my data

## 5. Right to erasure

- Delete the data you have on me

## 6. Right to rectification

- The data you have on me is inaccurate. Fix it!

## 7. Right to understand profiling or request manual processing

- Explain to me your data analysis algorithm
- Let a human profile me

*\*All requests must be processed and resolved within a month*

# 1. Right to be informed

No out of the box solutions

## Possible workarounds:

- Create consent popup / window
  - Explain in simple terms what's happening in the background
  - Event to track consent for each visitor
  - Customized consent popup for each region (non-EU / EU)
  - Do not track by default / Respect browser's DNT option
- Create inventory of all active website tracking vendors
  - <https://taginspector.com/>
  - [Ghostery extension](#)

## 2. Right to access

No out of the box solutions

### **Possible workarounds:**

- Custom data access tools using APIs and visitor identifiers
- Establish process to get data from 3<sup>rd</sup> party data handlers

# Fun fact on right to access



- Max Schrems was a pioneer on this topic
- Requested his information from FB in 2011
- 3 years of Facebook traffic resulted in 1200 pages of information (Friend requests, pokes, deleted messages etc.)

# 3. Right to data portability

No out of the box solutions

## **Possible workarounds:**

- Custom data access tools using APIs and visitor identifiers
- Create extracts using an open format (xml, JSON etc.)

# 4. Right to stop processing

Only opt-out options available

## Possible workarounds:

- Use a custom variable / segment to exclude from further data analysis
- Create an exclusion list in tag management systems, with visitors who opted-out, using visitor identifiers
- Establish process to inform 3<sup>rd</sup> party data handlers

# 5. Right to erasure

No out of the box solutions

## Possible workarounds:

- Raise request with vendor's technical team or delete upon request, using visitor identifier cookies
- Advise visitors to enable DNT option
- Establish process to inform 3<sup>rd</sup> party data handlers

# 6. Right to rectification

Previously recorded data not editable

## **Possible workarounds:**

- Raise request with vendor's technical team
- Overwrite data by manually uploading updates
- Manually update marketing segments, according to requests
- Establish process to inform 3<sup>rd</sup> party data controllers

# 7. Right to understand profiling or request manual processing

No out of the box solutions

## **Possible workarounds:**

- Detailed documentation of campaigns and profiling process
- Keep log of targeted visitors for each campaign
- Have a manual procedure in place

# Fun fact on right to profiling information

- In 2012 Target figured out a teen girl was pregnant before her father did
- Father called to complaint
- Manager wasn't could not understand what happened



# Summary

Where do I start?

# 5 Quick wins

- 1. Do not collect IP addresses**  
(See settings in analytics platforms)
- 2. Pseudonymize to identify anonymous user journeys and improve personal data handling**  
(Hashing)
- 3. Stop personal data collection**  
(Monitor for personal data, traffic filters)
- 4. Use major market vendors for data collection**  
(Reduce overhead using standardized processes)
- 5. Strict storage and collection rules for personal data**  
(Keep only what you need, Minimize overhead, minimize breach risks)

## **A. Discover**

1. Data flows to know who has access
2. Personal data identifying a person
3. Where data is collected & stored
4. 3<sup>rd</sup> party vendors collecting personal data

## **B. Manage**

1. Create a data inventory
2. Agree on data sensitivity with legal team
3. Document & prioritize data requirements
4. Define policies for personal data

# **First steps to compliance**

## **C. Protect**

1. Pseudonymize personal data\*
2. Stop tracking irrelevant personal data
3. Control access and block unused 3<sup>rd</sup> parties
4. Increase datacenter security

## **D. Continuous process**

1. Arrange recurring tests
2. Keep logs & records of changes
3. Frequent audit of 3<sup>rd</sup> parties
4. Educate organization on best practices

\*pseudonymised personal data can fall under the law

# Is it worth keeping personal data?

Hard work to comply comes with **several benefits:**

- Unlocking the power of services personalization
- Small number of compliant companies will have advantage
- Urges companies to earn user trust and form stronger bonds
- EU companies will have competitive advantage in the future

Evolving into a privacy by design organization, shows **respect for your audience**

# Useful resources

- Full GDPR text  
[EU website](#)
- Aurelie Pols - Data governance & privacy engineer  
[SlideShare](#)
- Independent online portal on GDPR  
[eugdpr.org](#)
- Article 29 Working Party resources  
[Official website](#)
- Piwik PRO  
[GDPR compliance options](#)

# Analytics blog of the month



**Simo Ahava**

[www.simoahava.com](http://www.simoahava.com)

- Expert in GA and GTM
- Google analytics mentor

# Analytics fun of the month



## Measure Slack

<http://join.measure.chat>

<https://www.measure.chat>

- Real-time social forum for digital marketers
- Discuss any issue with global experts