consent manager

Webinar

Latest developments in data protection: Guidance from DPAs accross Europe

Visit us on www.consentmanager.net

Webinar
Overview

1. Welcome
2. Webinar, ca. 30-45 min
3. Questions & Answers, ca. 15 min

- ✓ Webinar will be recorded,
  Videos & PDF will be available at www.consentmanager.net/knowledge/videos/
- ✓ Put your questions in the ZOOM chat – we collect them and answer them in section 3 after the presentation.

DPA guidelines & court rulings

Best practices from various countries

TTDSG: Baden-Württemberg
FAQ on Cookies and Tracking

- ✓ Updated guidelines 03/2022
- ✓ No consent required: Necessary for the Purpose
  - Shopping basket, Language
  - Storing consent status (but without any ID!)
  - Security functions (e.g. prevent multiple submits of a form)
- ✓ Non-essential third party tools fall under GDPR/TTDSG
- ✓ Example recommendations on 3rd Party tools:
  - “2-click solution” (on-time notice & consent)
  - Insert Twitter feeds as Screenshot instead of HTML embed
  - Upload Videos to your own server instead of YouTube
  - OpenStreetmap as alternative to Google Maps
- ✓ No consent for Analytics required only if …
  - A) Logfile analysis
  - B) No external/3rd-Party vendor involved
  - C) No merge of data with other sources
  - D) No repurposing of data (e.g. no use for marketing)

- ✓ Recommendations / Examples of common mistakes
- ✓ Mistakes on consent requirements:
  - No non-essential cookies before consent
  - Consent must be as easy as rejection
  - Reject buttons must be visible – even on small screens
- ✓ Mistakes on information requirements:
  - German website must display consent message in German
  - Cookie Banner must include sufficient information (only a link to privacy notice is not sufficient)
  - Info on processing of personal data (not only cookies!)
- ✓ Mistakes on incorrect headlines:
  - “We love cookies”
  - “Welcome”
  - “We need your consent”
  - “Accept cookies”
  - “We respect your privacy”
- ✓ No “legitimate Interest” for Analytics, personalized Ads and device access

DVI: Latvia
Guidelines on using Cookies on websites

- ✓ No consent necessary:
  - 1st party cookies for shopping carts
  - Authentication cookies during a session
  - Security cookies, fraud prevention
  - Technical cookies for media elements / loadbalancing
  - User customization (language or other elements)
  - Sharing 3rd-party social media content (!)
- ✓ Clear language: Words like “may”, “could”, “some”, “often” or “possible” should be avoided
- ✓ Precise purpose descriptions. Example: “We will store your shopping history and use your information on previously purchased products to recommend other products that in our opinion are in your interests.”
- ✓ Opt-out must be possible via the cookie banner, deleting the cookies may not be the only way
- ✓ Cookie description necessary but simple. E.g.:
  “fbp” - Use Facebook.com to deliver ads – 3 months expire
  “_gat” - Use Google Analytics to adjust number of requests – 1 year expire

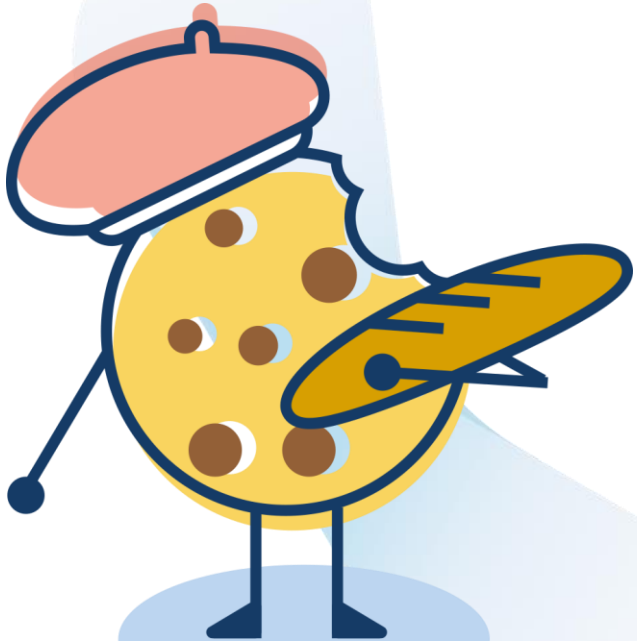
DSB: Austria
Google Analytics

- ✓ Austrian Data Protection Authority
- ✓ Use of Google Analytics violates “Schrems II” decision of ECJ
- ✓ Google is “FISA”-vendor, US agencies may access data
- ✓ SCCs and TOMs not sufficient protection against data sharing with US vendors

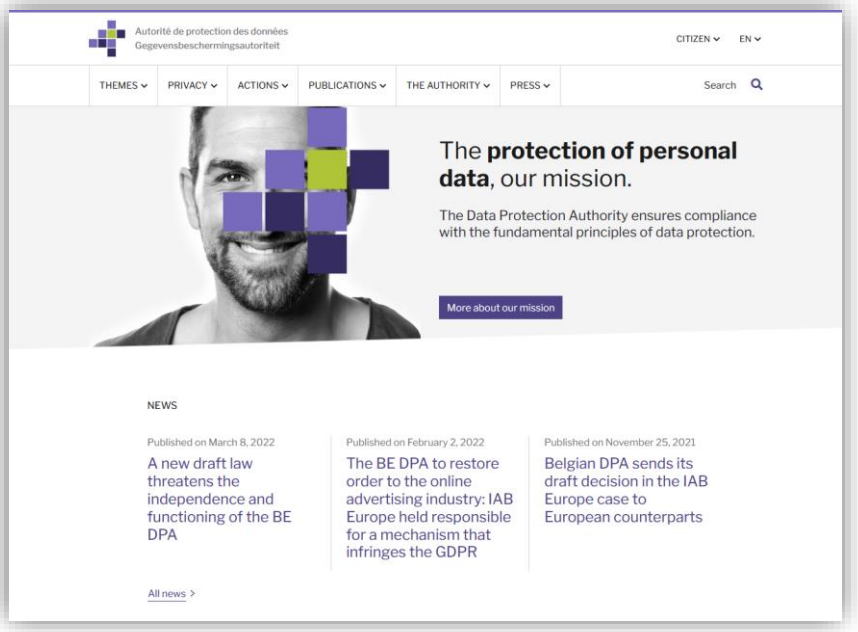
- ✓ → similar cases all over Europe: “noyb” issued 101 complaints in almost all EU countries

CNIL: France
Guidelines & Analytics

- ✓ Similar recommendations to what other countries say
- ✓ Accept & reject must be present (“tout accepter” & “tout refuser”) and of same size/font
- ✓ Continue without accepting (“continuer sans accepter”) can be used for rejection
- ✓ Change your choices (“gérer mes cookies”) via button on bottom left side
- ✓ Google Analytics does not provide sufficient guarantees for US data transfers → Analytics probably not GDPR compliant



APD: Belgium
IAB Transparency & Consent Framework



- ✓ IAB TCF Standard for advertising industry
- ✓ Standard was found to be in violation of GDPR
- ✓ IAB Europe (managing organization) fined for 250,000 EUR
- ✓ Several issues (among others):
  - Legal basis missing
  - Transparency on purposes missing
  - Insufficient mechanisms to prevent fraud
  - IAB Europe is seen as controller but misses to appoint DPO, DPIA missing and missing to create data processing directory
- ✓ Next steps:
  - IAB Europe required to submit “Action plan” describing how the TCF can become GDPR compliant
  - IAB Europe to appoint DPO and provide required legal documentation
  - Once approved, IAB has 6 months to implement the action plan
  - Next steps expected for end of June

Recommendations

Designing your cookie banner

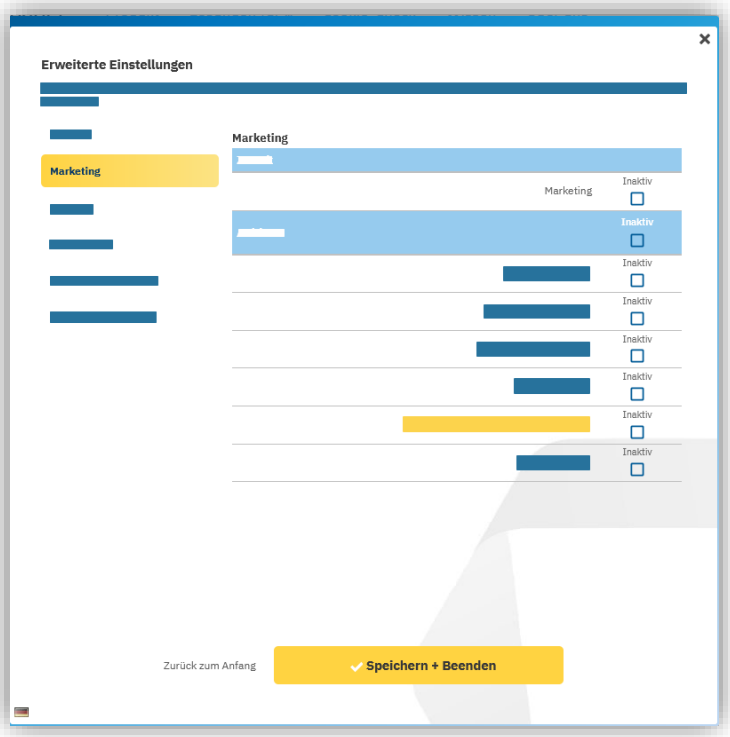
Recommendations
First layer

- ✓ Accept AND reject visible on first layer
- ✓ Accept and reject with same design, same size and color
- ✓ Clear labels (“Accept” / “Reject” instead of „Ok“)
- ✓ No dark patterns!

- ✓ Clear headline regarding consent for data processing & cookies
- ✓ Sufficient description in text (third parties (amount?), purposes, personal data, cookies, how to reject, ...)

- ✓ No pre-ticked checkboxes
- ✓ Links to privacy notice, T&C, imprint and more

Recommendations
Second layer



- ✓ Only use „Function“ / „Essential“ for <u>really</u> essential cookies & vendors
- ✓ Marketing, Analytics, Social Media are usually not essential and require consent
- ✓ Limit the amount of vendors (<50)
- ✓ Only use IAB TCF if really necessary

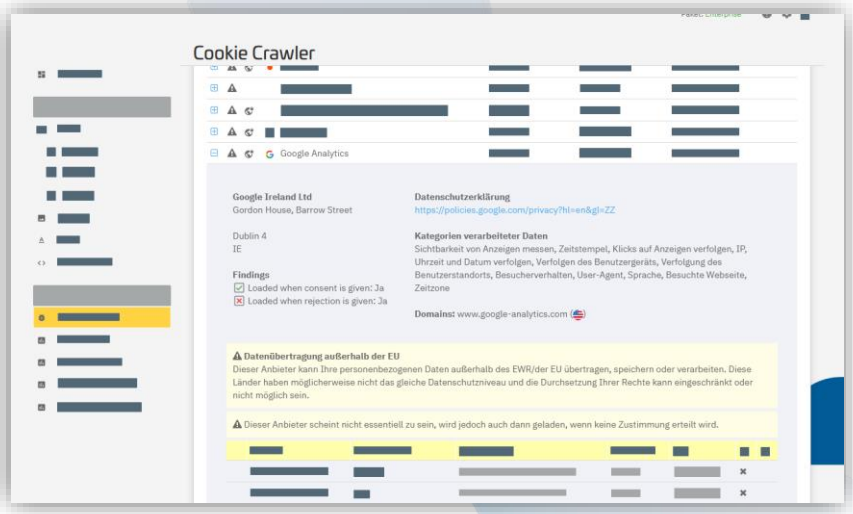
- ✓ Required info on second layer:
  - Clear and explicit description of purposes
  - List all vendors with name, address, legal bases, purpose(s), description and categories of processed data
  - List all cookies with name, storage duration (expire) and purpose
  - Granular choices (purposes AND vendors)
  - Information about company (controller) and DPO if possible

Recommendations
Non-EU Data transfers

- ✓ Add note if vendors are located outside of the EU
- ✓ Add note if vendors transfer or process data outside of the EU
- ✓ Transferring or processing data outside of the EU may require (additional) consent

- ✓ Important: Use of a data-center/server that belongs to a US-vendor may not be GDPR-compliant and/or require consent <u>even if the servers are located in the EU</u>

- ✓ => Use the recommendations our cookie crawler gives you



Data protection worldwide

Quick view outside of the EU

CCPA/CPRA: California & the US

- ✓ Consent usually not necessary
- ✓ “Opt-out” mechanism required for many things
- ✓ Applies to companies that do business in California or receive personal data of California residents
- ✓ Applies to companies that have +25M USD revenue or process data on +50,000 consumers/year or +50% of revenue from processing data.
- ✓ Privacy notice may be required on page visit
- ✓ “Do not sell (or share) my personal information” link must be present
- ✓ Already enforcement actions ongoing

- ✓ Similar laws in more US states

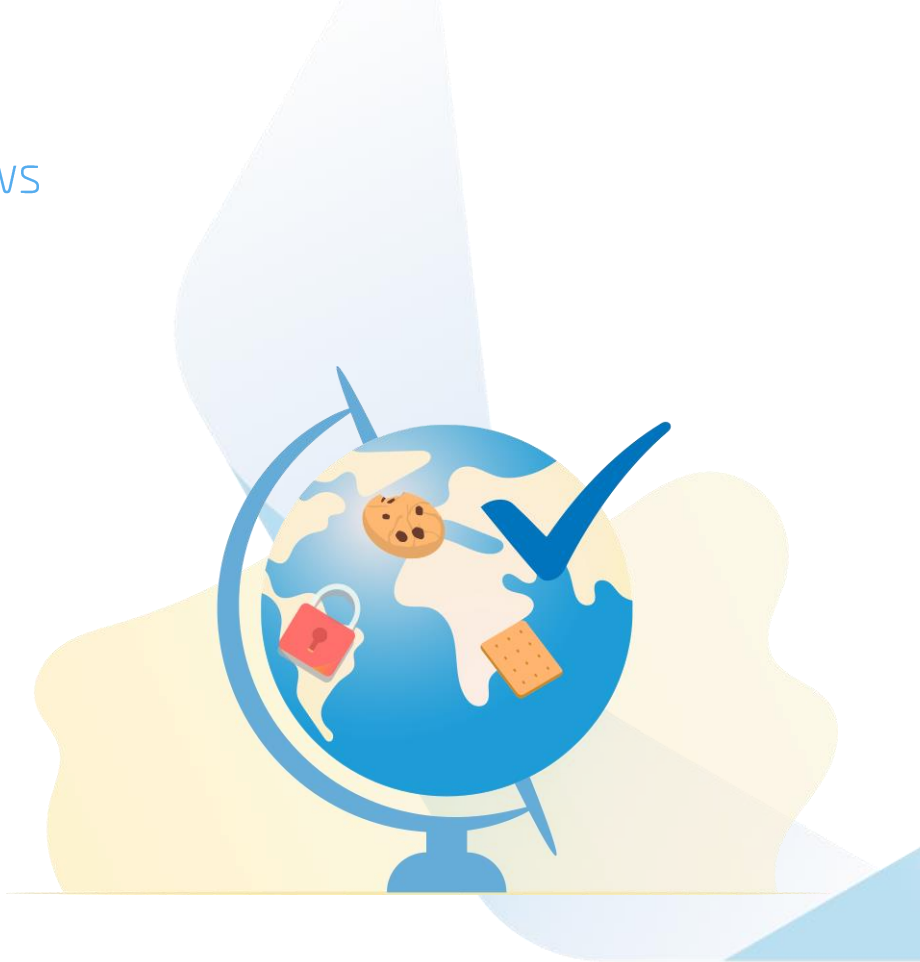
PIPEDA / CPPA: Canada

- ✓ PIPEDA / CPPA
- ✓ Consent as default basis
- ✓ „Implied consent“
- ✓ Similarities to GDPR
- ✓ Scope: Organisations in Canada and organisations with „real an substential connection to Canada“ (e.g. targeting CA users)

Data protection world wide

Other countries with significant privacy laws

- ✓ America:
  - Brasil (LGPD)
  - Mexico (LFDPPP)
  - Argentinia (PDPA)
- ✓ Africa:
  - Nigeria (NDPR)
  - South Africa (POPIA)
- ✓ Asia:
  - South Korea (PIPA)
  - China (PIPL)
  - Thailand (PDPAT)
- ✓ Europe / Middle east:
  - Turkey (PDPL)
  - Russia (RPDL)
  - Israel (PPA)
- ✓ And many more ...



Thank you!

Please recommend us:

www.consentmanager.net