Web Development in the Post-GDPR World

June 27, 2018

oomph

Special Thanks

mediacurrent

Dawn Aly
VP, Digital Strategy
Mediacurrent
@dawnashleealy

Mark Shropshire
Open Source Security Lead
Mediacurrent
@shrop

Think Your Website is GDPR-Compliant? Think Again!

DJ Kadamus

Digital Account Strategist

I work with clients on retainer and delivery projects, and fill the gaps with some SEO and GDPR Consulting.

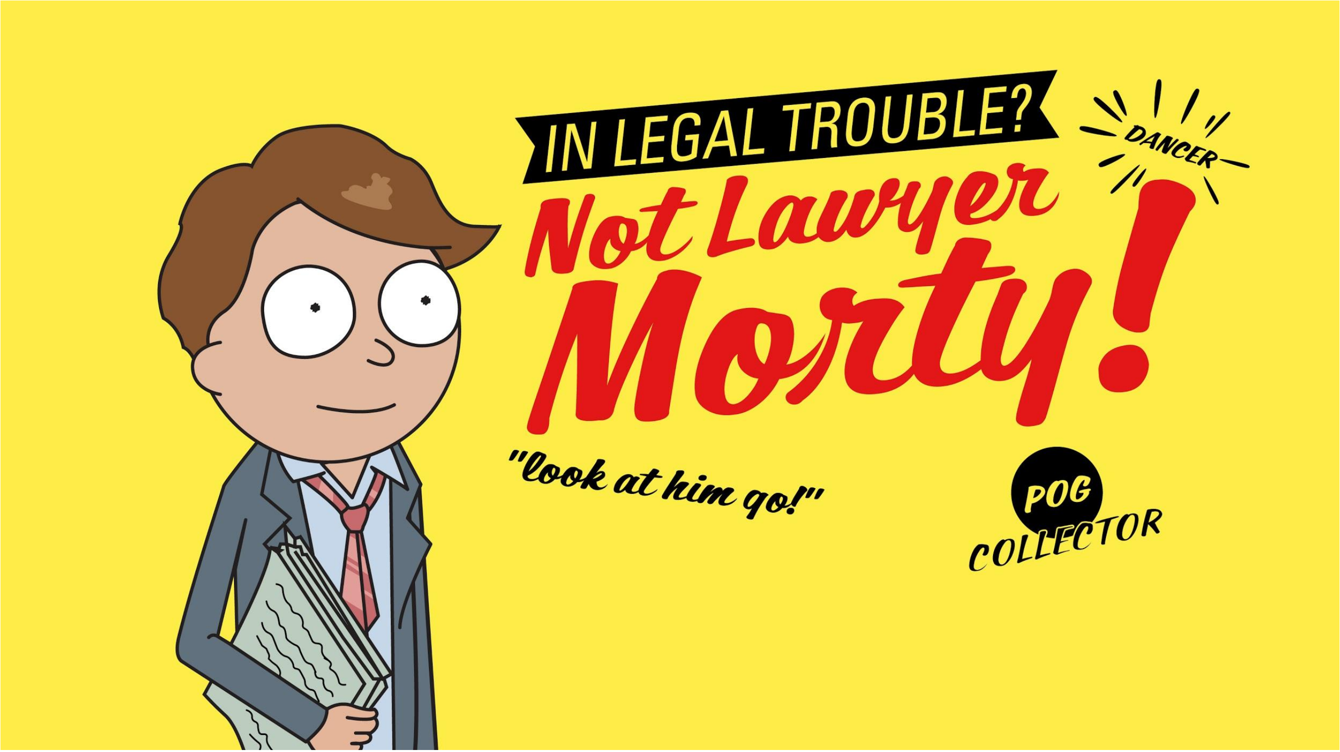
I also work on Drupal config when no one is looking.

Oomph is a great company to work for, check us out! ⬇

401-228-7660
72 Clifford Street,
Providence, RI 02903

oomphinc.com
oomph.is/dkadamus
dkadamus@oomphinc.com

Disclaimer


IN LEGAL TROUBLE?
Not Lawyer Morty!
DANCER
"look at him go!"
POG COLLECTOR

But first… a joke

What we’ll cover today

- Quick overview of GDPR
- What the regulations mean for US based companies
- How you can build a site with an enhanced Privacy Experience
- How you can use Drupal to continually improve your compliance
- Good and bad examples of compliance throughout

oomph

The important slides

GDPR Roles

Examples of actionable steps

Who are the troublemakers?

What is *Privacy Experience*?

What you should strive for

Drupal and GDPR

Actionable Steps

Creating a Plan

Overview of the General Data Protection Regulation (GDPR)

June 27, 2018

oomph

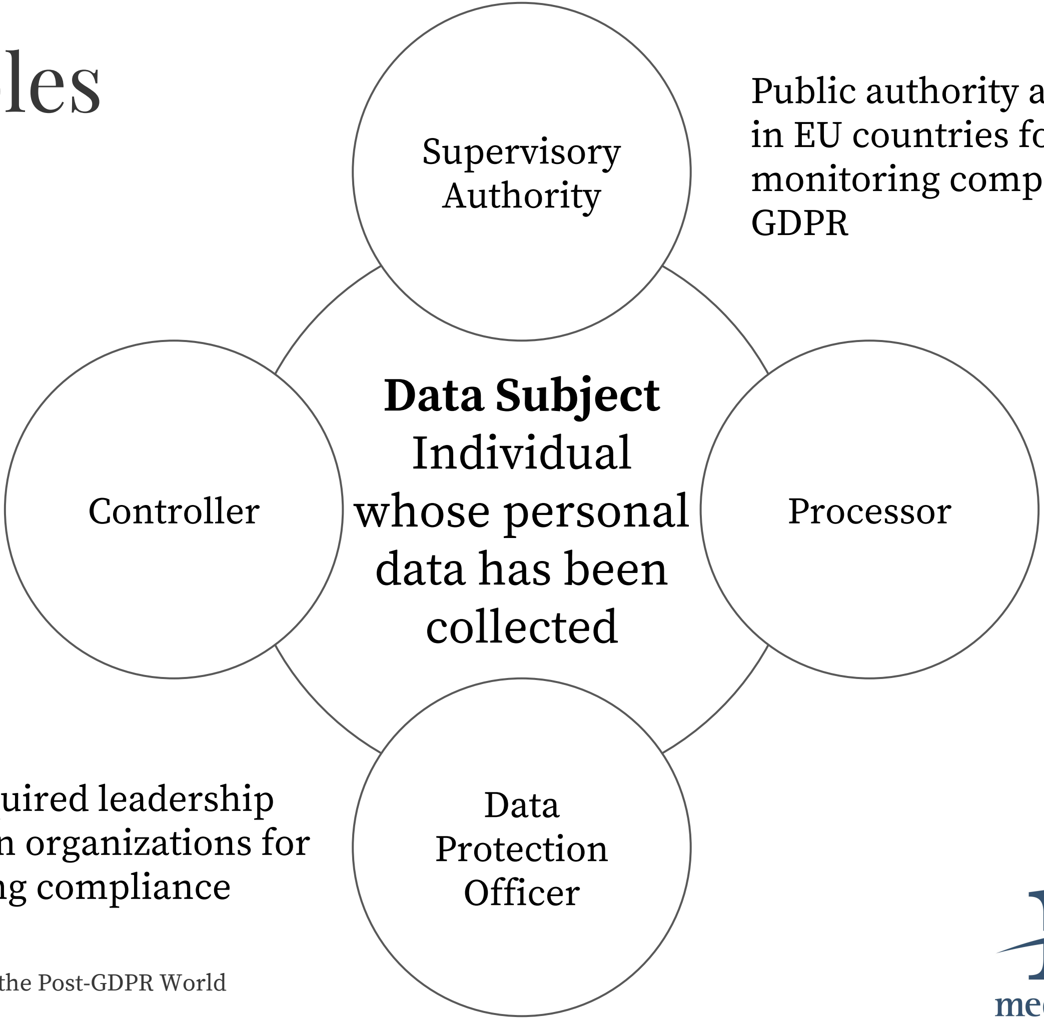
GDPR Definition

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).

GDPR was activated across the EU on **May 25, 2018.**

You can read the law in it's entirety here: gdpr-info.eu

GDPR Roles



Supervisory Authority

Controller

Data Subject
Individual whose personal data has been collected

Processor

Data Protection Officer

Public authority appointed in EU countries for monitoring compliance of GDPR

Legal entity or person determining the need and means for processing personal data - website managers

Legal entity or person processing the actual data on behalf of the controller - third-party like GA or Marketo

GDPR required leadership position in organizations for monitoring compliance

User Rights and Requirements

- Breach Notification
- Right to Access
- Right to Erasure
- Data Portability
- Privacy by Design
- Data Protection Officers

So what?

Why should we even bother?

- Fines* up to 20 million EUR

  OR

- 4% annual global turnover

** Fines can be levied on both Controllers and Processors*

Now I'll make you feel a little bit better...

I'm not trying to scare you!

The EU is looking for sites which have *gross negligence* for the law. Making changes in good faith is sufficient, for now.

oomph

What the regulations mean for US-based companies?

June 27, 2018

oomph

Let's determine what this means in *actuality*, 1

Example 1

You are a Massachusetts-based nonprofit with no e-commerce

- 95% of traffic US-based
- All CTAs are contact forms
- Donation CTAs lead off-site to a third party
- Only uses Google Analytics

Example 2

You are an international corporation with offices in Boston and Munich

- 35% of traffic EU-based
- Sell products in US and EU
- E-commerce on site
- Integrations with third-party marketing software & Google Analytics

Let’s determine what this means in *actuality*, 2

Example 1, nonprofit

1. Update Privacy Policy
2. Notify users of changes
3. Add on-page notice to users about anonymous tracking
4. Appoint Privacy Officer

Example 2, international company

All the same as example 1, plus:

1. Wrap all trackers in IF so nothing fires without consent
2. Add notice to users on all forms
3. Develop system to comply with data rights of users
4. Create the same experience for opted-out users

Compliance will vary for all US companies

- It’s unreasonable to expect a small nonprofit to have the same resources as a multinational corporation to make all changes.
- The EU supervisory authorities are looking for gross negligence of the law
- A good metaphor is paying taxes, the *IRS* isn’t going to hit you over the head with a massive fine if you make a mistake acting in good faith, but if you disregard the law, they’ll come knocking

Who's gotten in trouble so far?

- *British Telecommunications* fined £77,000 by ICO in UK after it sent nearly 5 million nuisance emails to customers without consent
  - *BT* failed to take reasonable steps to prevent the violation
- *Yahoo!* fined £250,000 in UK after systematic failures put customers data at risk
  - This was due to the data breach in September 2016
- *OPTICAL CENTER* fined €250,000 by CNIL for failure to secure data that lead to a data breach with PII and PCI, including health data

Building a site with an enhanced *Privacy Experience*

June 27, 2018

oomph

What is *Privacy Experience*?

We already build sites with the user-experience in mind, now we need to build with the privacy experience in mind. The pillars of PX are:

- Transparency of data collection
- User consent for all data collection
- Sufficient protection of user data
- Intelligent collection of user data
- Security and privacy by design

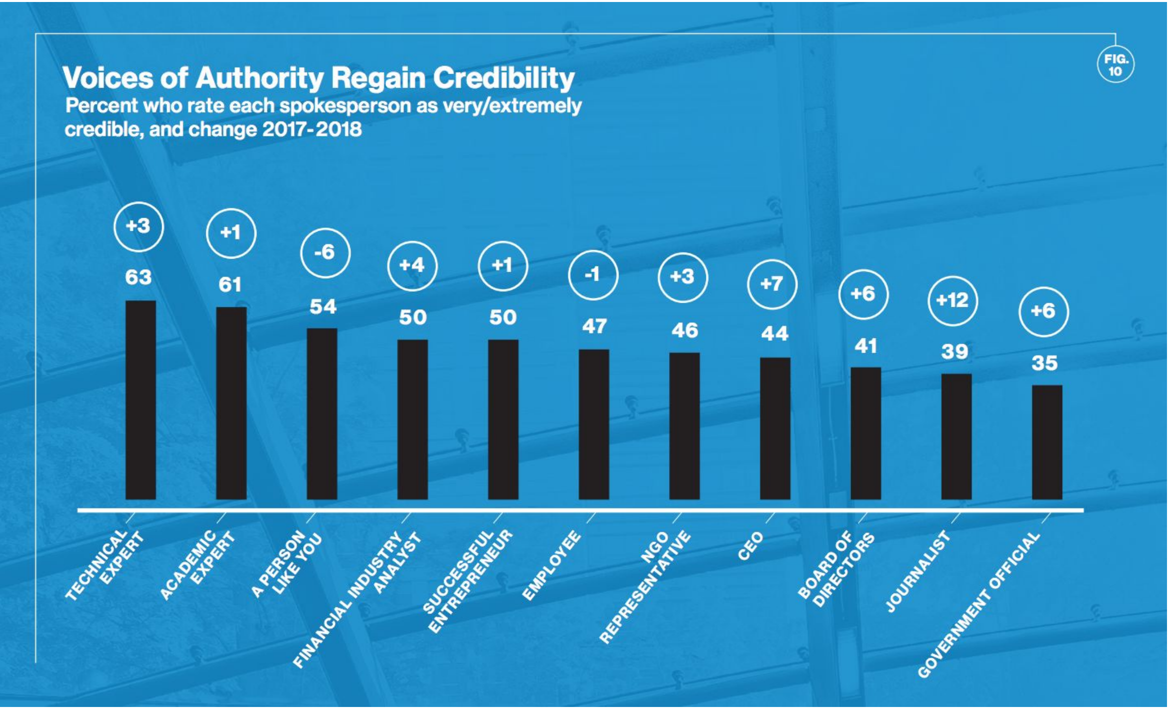


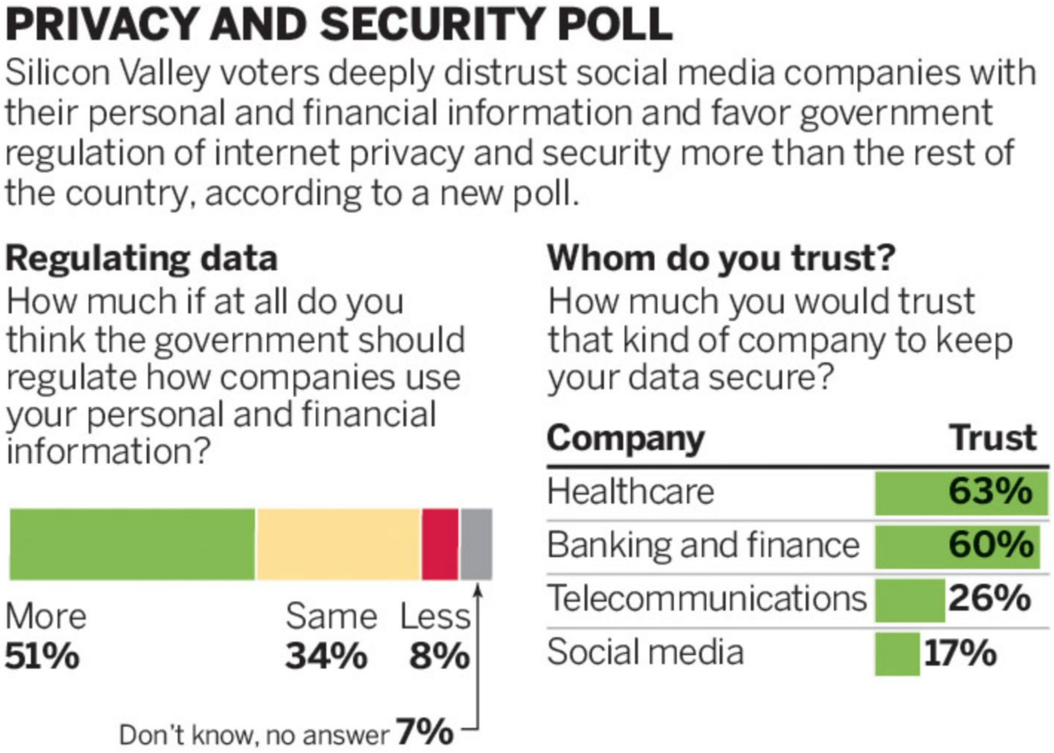
FIG. 10

Voices of Authority Regain Credibility

Percent who rate each spokesperson as very/extremely credible, and change 2017-2018

[2018 Edelman Trust Barometer]()

First step, build trust with your users!



PRIVACY AND SECURITY POLL

Silicon Valley voters deeply distrust social media companies with their personal and financial information and favor government regulation of internet privacy and security more than the rest of the country, according to a new poll.

Regulating data

How much if at all do you think the government should regulate how companies use your personal and financial information?

Whom do you trust?

How much you would trust that kind of company to keep your data secure?

Company	Trust
Healthcare	63%
Banking and finance	60%
Telecommunications	26%
Social media	17%

Who do users not trust currently?

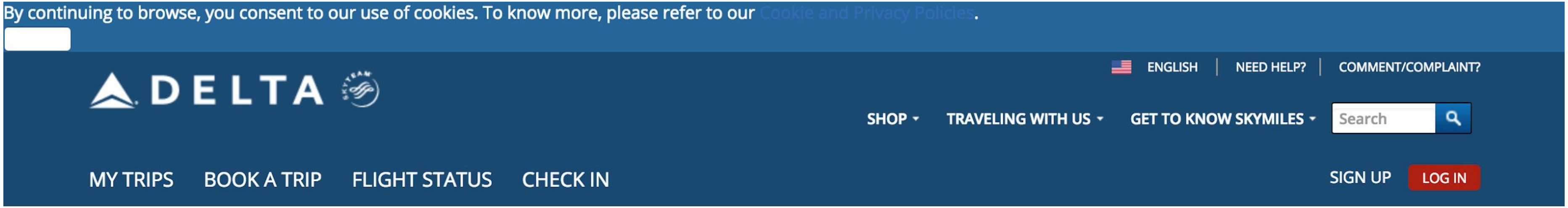
How does this change our thinking?

Silicon Valley distrusts social media with personal data, poll finds, *The Mercury News*. June 24, 2018

Designing a good Privacy Experience

- Make any on-page notices accessible for all users
- When writing content, use easy to understand copy
- Understand that consent must be given, not assumed
- Build a “Privacy Preferences” page and add to utility navigation
- Educate and empower the user

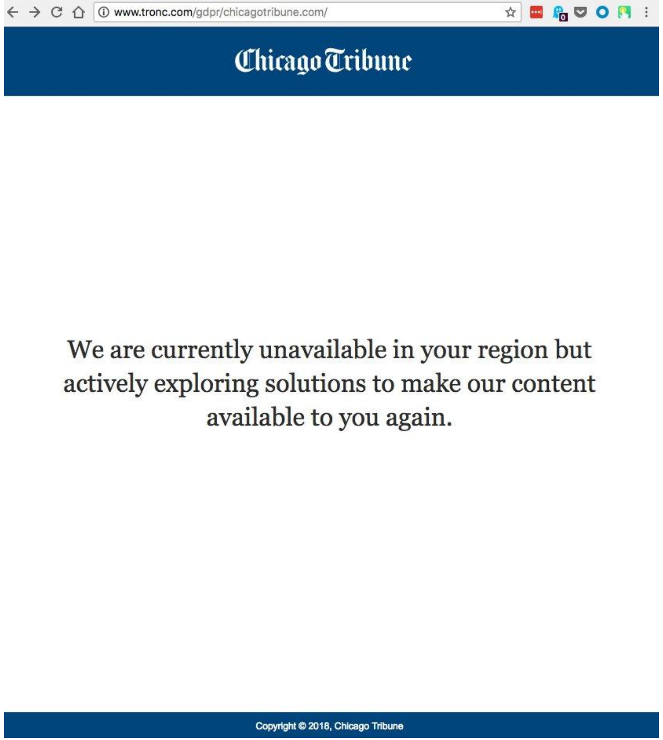
Bad example 1, *Delta*



By continuing to browse, you consent to our use of cookies. To know more, please refer to our Cookie and Privacy Policies.

- Blue on blue and a white button is inaccessible for just about all users
- Delta is an international company, they should have an opt-in consent
- When you get to their Privacy Policy, it is very difficult to understand without a law degree

Bad example 2, *Tronc, Inc.*

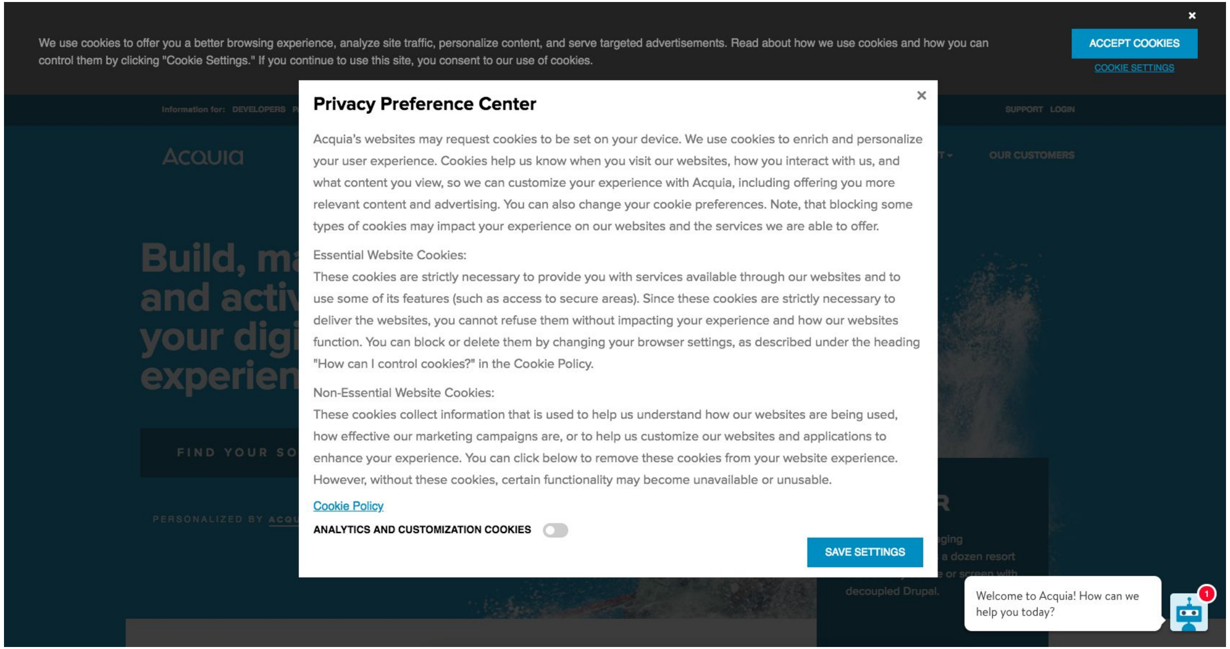


We are currently unavailable in your region but actively exploring solutions to make our content available to you again.

Copyright © 2018, Chicago Tribune

- Blocking content is definitely not the answer
- Users who have opted-out of data tracking are afforded the same experience as users who have opted-in
- Blocking traffic through IP geo-fencing is fruitless because IP addresses are constantly changing
  - Also, VPN's which can mask a EU citizens IP address

Good example 1, *Acquia*



We use cookies to offer you a better browsing experience, analyze site traffic, personalize content, and serve targeted advertisements. Read about how we use cookies and how you can control them by clicking "Cookie Settings." If you continue to use this site, you consent to our use of cookies.

ACCEPT COOKIES

COOKIE SETTINGS

Privacy Preference Center

Acquia's websites may request cookies to be set on your device. We use cookies to enrich and personalize your user experience. Cookies help us know when you visit our websites, how you interact with us, and what content you view, so we can customize your experience with Acquia, including offering you more relevant content and advertising. You can also change your cookie preferences. Note, that blocking some types of cookies may impact your experience on our websites and the services we are able to offer.

Essential Website Cookies:
These cookies are strictly necessary to provide you with services available through our websites and to use some of its features (such as access to secure areas). Since these cookies are strictly necessary to deliver the websites, you cannot refuse them without impacting your experience and how our websites function. You can block or delete them by changing your browser settings, as described under the heading "How can I control cookies?" in the Cookie Policy.

Non-Essential Website Cookies:
These cookies collect information that is used to help us understand how our websites are being used, how effective our marketing campaigns are, or to help us customize our websites and applications to enhance your experience. You can click below to remove these cookies from your website experience. However, without these cookies, certain functionality may become unavailable or unusable.

Cookie Policy

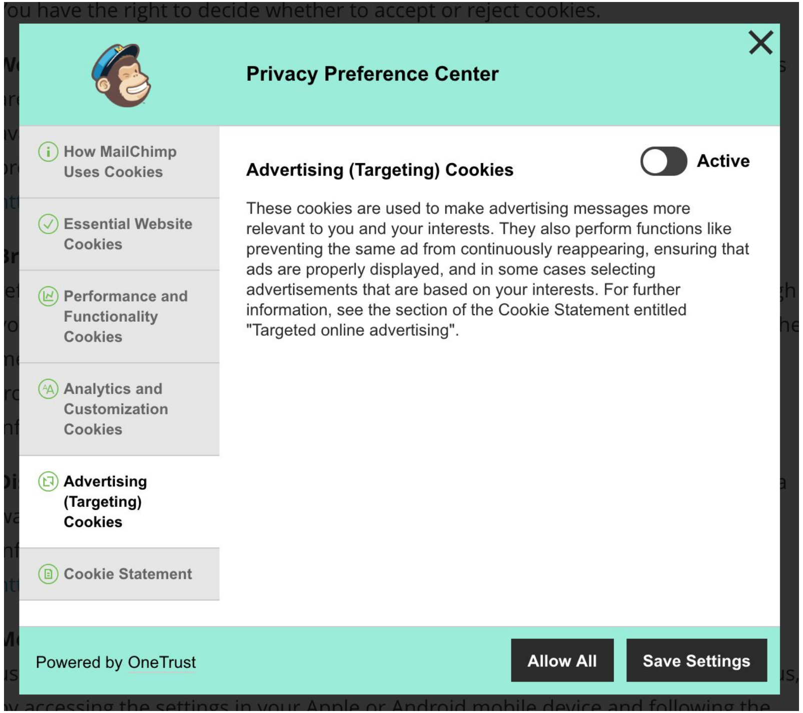
ANALYTICS AND CUSTOMIZATION COOKIES ○

SAVE SETTINGS

Welcome to Acquia! How can we help you today?

- Noticeable and accessible message
- Gives the user the preference to enable non-essential cookies
- Makes it easy to access the Cookie Policy
- Copy is easy-ish to read

Good example 2, *MailChimp*



ou have the right to decide whether to accept or reject cookies.

Privacy Preference Center
How MailChimp Uses Cookies
Essential Website Cookies
Performance and Functionality Cookies
Analytics and Customization Cookies
Advertising (Targeting) Cookies
Cookie Statement
Active
Powered by OneTrust
Allow All
Save Settings

Advertising (Targeting) Cookies

These cookies are used to make advertising messages more relevant to you and your interests. They also perform functions like preventing the same ad from continuously reappearing, ensuring that ads are properly displayed, and in some cases selecting advertisements that are based on your interests. For further information, see the section of the Cookie Statement entitled "Targeted online advertising".

y accessing the settings in your Apple or Android mobile device and following the

- Privacy Preference Center educates the user on each cookie and empowers them to make a change
- Easy to understand language
- Accessible for all users
- One small issue, it was kind of difficult to find

What you should strive for

- Empower your designers to create a positive PX by designing with all elements (opted-in), and then think about how to display the site as best you can after removing some elements (opted-out)
- Design what the Privacy Policy banner/notice should look like
  - Talk to your development teams to make sure that certain site changes occur on click
- Design a Privacy Page with relevant information and consent options
  - An easy-to-understand privacy policy with bullets and video, along with the legalese

Using Drupal to continually improve compliance and data security

June 27, 2018

oomph

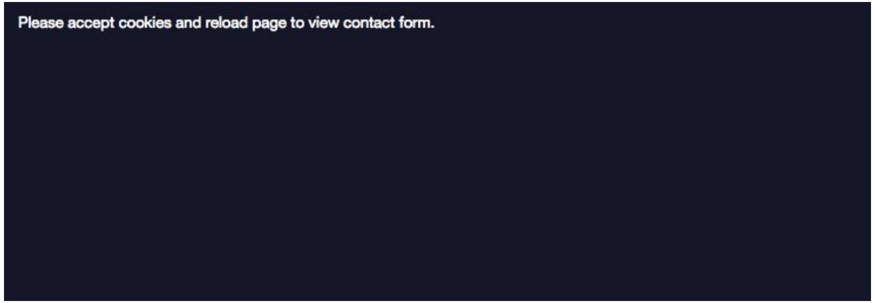
Technical Recommendations

- Use the recommended modules to get you 90% of the way there
- Leverage IF wrappers to ensure cookies only fire after consent
- Single Encryption Key per user (a lockbox)

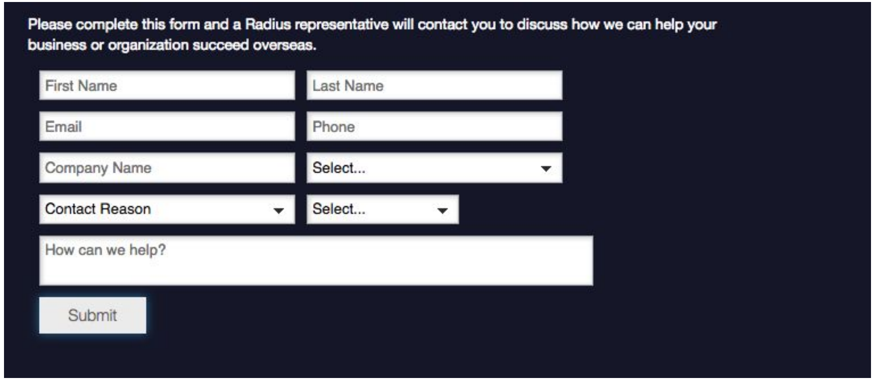
Drupal and GDPR

- EU Cookie Compliance Module
    - This is the module that we recommend, it has the most functionality out of the box, and is customizable
- Drupal GDPR Team
    - Coordinated effort by the Drupal community to continually improve Drupal's framework for GDPR Compliance
- We strongly recommend contributing back to the community to help all Drupal users grow together and standardize security/privacy as best we can

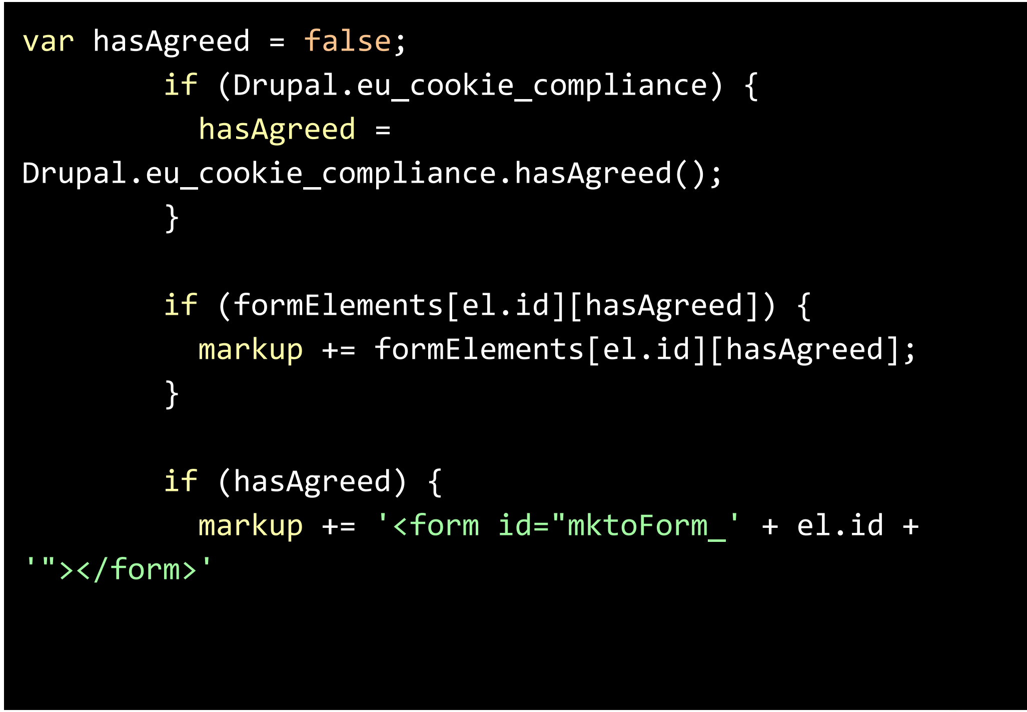
IF Wrappers



Please accept cookies and reload page to view contact form.



Please complete this form and a Radius representative will contact you to discuss how we can help your business or organization succeed overseas.



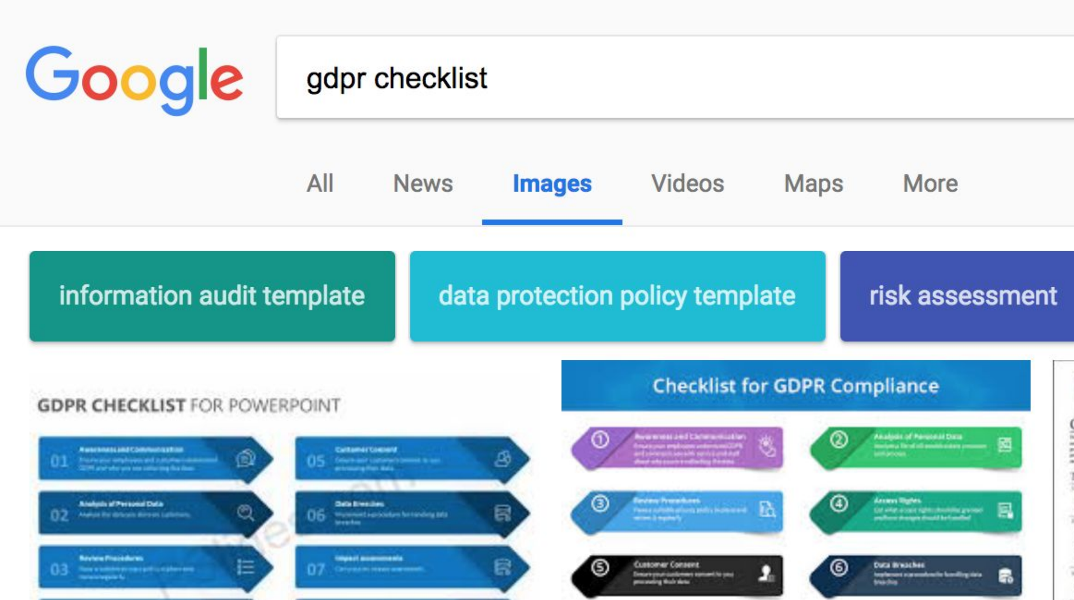
```
var hasAgreed = false;
        if (Drupal.eu_cookie_compliance) {
          hasAgreed =
Drupal.eu_cookie_compliance.hasAgreed();
        }

        if (formElements[el.id][hasAgreed]) {
          markup += formElements[el.id][hasAgreed];
        }

        if (hasAgreed) {
          markup += '<form id="mktoForm_' + el.id +
'"></form>'
```

Creating a lockbox

- Create a single, end-to-end, encryption key per user to easily access all data
- This is not mandatory, but idealistic
- The idea is to have one single lockbox per user
    - If someone wants their data, you can easily deliver it to them
    - If someone wants you to delete their data, it can easily be done
    - If some supervisory authority comes knocking, you can easily provide the data
- This could be its own talk, so to save time, here is a fantastic article on the subject

Actionable next steps for your teams

1. Assess risk and create your plan
2. Create and/or update security and privacy policies
3. Prioritize remediations
4. Implement remediations
5. Document your work
6. Rinse and repeat



gdpr checklist

Google
All
News
Images
Videos
Maps
More
information audit template
data protection policy template
risk assessment
GDPR CHECKLIST FOR POWERPOINT
Checklist for GDPR Compliance

Bonus Action Step!

Keep up with the news as these laws can change in Europe and there is a strong potential that this will be implemented in the US!

- Scoop: The White House looks to coordinate online privacy plan; *Axios*. June 20, 2018.

Creating a Plan

Data Collection Points

- What are we collecting & why?
- Active vs. Passive
- Storage & Encryption
- Integration points

Messaging and Consent

- Opt-in language
- Privacy policy & legal documents
- Internal messaging around value and marketing impact

User Control

- Data portability
- Revoking consent
- Data erasure

”

> *Data is a precious thing and will last longer than the systems themselves.*

TIM BERNERS-LEE

Special Thanks

mediacurrent

Dawn Aly
VP, Digital Strategy
Mediacurrent
@dawnashleealy

Mark Shropshire
Open Source Security Lead
Mediacurrent
@shrop

oomph

Thank You

Thank you for listening (and attending my first ever talk!), if you have any questions, please reach out to me at the information below!

/u/dkadamus   @_Kadamus   /in/davidkadamusjr

401-228-7660
72 Clifford Street,
Providence, RI 02903

oomphinc.com
oomph.is/dkadamus
dkadamus@oomphinc.com

oomph

Thank You

oomphinc.com

401-228-7660 | 72 Clifford Street, Providence, RI 02903

oomph