GDPR:

What it means for organizations in the US

Mac Clemmens | Heather King

Welcome!

Mac Clemmens

Heather King

DIGITAL DEPLOYMENT

What we'll cover

1. What is the GDPR?
2. What does the GDPR cover?
3. To what extent does it affect your organization?
4. Steps you can take to be compliant!

Note: This is not legal advice!

Check with your own legal counsel.

Today's webinar is informational only, and to report the trends and tools we are seeing used.

What is the GDPR?

What is the GDPR?

- The GDPR is the **General Data Protection Regulation**.
- The GDPR codifies and unifies data privacy laws across all European Union member countries.
- It is applicable to any citizen of the European Union and, most importantly, to any company doing business with a citizen of the EU.

Why does the GDPR matter?

- Any organization that collects data from EU customers is potentially subject to the provisions of the GDPR, and therefore is also subject to the strict penalties associated with non-compliance.

Who does the GDPR affect?

- Collecting and accepting personal information from any citizen of the EU will invoke the GDPR, **regardless of your organization's country of origin**.

- For all intents and purposes, if your organization has a presence on the internet in the form of a website, and if your enterprise collects personal data from EU customers regardless of where those customers are currently located, it is subject to the provisions of the GDPR.

When will the GDPR take effect?

- The EU granted a two-year grace period before beginning enforcement of the provisions in the law.

- Enforcement went into effect **May 25, 2018**.

8 things covered by the GDPR

1. Consent

- ✓ The GDPR specifically prohibits the use of long, convoluted terms and condition statements, particularly statements that contain legalese.
- ✓ Any request for consent, declaration of terms, or statement of privacy must be presented clearly and concisely, and without any ambiguity of meaning.
- ✓ It must be as easy to withdraw consent as it is to give it.

2. Breach notification

- ✓ Compliance with the GDPR requires companies to notify all data subjects that a security breach has occurred within 72 hours of first discovering it.
- ✓ The method of this notification will include as many forms as deemed necessary to disseminate the information in a timely manner, including email, telephone message, and public announcement.

3. Right to access

- ✓ The GDPR requires companies to provide, at the data subject's request, confirmation as to whether personal data pertaining to them is being processed, where it is being processed, and for what purpose.
- ✓ Companies must also be able to provide, free of charge, an electronic copy of the personal data being processed.

4. Right to be forgotten

- ✓ Under the GDPR, companies will erase all personal data when asked to do so by the data subject.
- ✓ At that point, the company will cease further dissemination of the data, and halt all processing.
- ✓ Valid conditions for erasure include situations where the data is no longer relevant, or the original purpose has been satisfied, or merely a data subject's subsequent withdrawal of consent.

5. Data portability

- ✓ The GDPR requires companies to provide mechanisms for a data subject to receive any previously provided personal data in a commonly used and machine-readable format.
- ✓ Under this provision, the data subject also has the right to request the company transmit the data to another processor, free of charge.

6. Privacy by Design

- ✓ Companies must follow Privacy by Design principles and implement appropriate technical and organizational measures.
- ✓ In practical terms, this provision means that companies will process only the data absolutely necessary for the completion of its business and limit access to personal data to only those employees needing the information to complete the process consented to by the data subject.
- ✓ What is privacy by design? A deeper dive into this GDPR requirement

7. Data Protection Officers (DPOs)

- ✓ Large organizations will maintain thorough and comprehensive records pertaining to the collection, processing, and storage of personal data.
- ✓ These organizations will designate a Data Protection Officer (DPO) to oversee the application of the GDPR and to protect personal data from misuse and unauthorized access and other security breaches.
- ✓ If an enterprise meets the criteria, a designated DPO is a requirement, not an option.

7. Data Protection Officers (DPOs)

- ✓ Unfortunately, the specific criteria for when an organization is required to designate a DPO is still in flux.
- ✓ A general rule of thumb to follow, based on the EU Commission's writings on the topic, is that a DPO is required for any organization with over **250 employees** or for any organization processing the personal data of over 5,000 data subjects in any 12-month period.
    - US Companies Need to Know: Do You Need a Data Protection Officer?
    - Does My Company Need a DPO for GDPR Compliance?

8. Penalties for noncompliance

- ✓ Organizations found to be in violation of the provisions of the GDPR can be fined up to 4% of annual global turnover or 20 million Euros, whichever is greater.
- ✓ Other violations are assessed on a tiered basis depending on the infraction.
- ✓ How the EU can fine US companies for violating GDPR

To what extent does it affect your organization?

Does the GDPR apply to every business with EU ties?

- It depends. The GDPR will affect all companies, individuals, corporations, public authorities or other entities that offer goods or services to individuals in the EU or that monitor their behavior there.

- The GDPR even applies to charities and nonprofit organizations that collect information from individuals in the EU.

Does the GDPR apply to every business with EU ties?

- For example, the GDPR applies to:
    - An American company whose website is made available to people in the EU.
    - A Boston-based HR manager in an international organization that collects data centrally from EU-based applicants and employees.

What we're seeing

- ✓ **California or regional associations:** Deal with member data which is EU consumer data
- ✓ **Pension systems:** Especially those with a regional focus decided that it did not apply to them
- ✓ **Private organizations, some nonprofits:** Have taken steps to update their privacy policies, scan their lists, and add a cookie notice.

4 steps you can take

1. Update your privacy policy

- ✓ Include clear privacy policy directions on the website, including what information is being collected, how data is stored and how to contact the organization.
- ✓ For example, Expedia.com's privacy policy page is clearly worded, straightforward, and comprehensive.
  - See example on next slide.
  - All categories are outlined with links that drop to the appropriate section; this is better than putting that information on one long page, as seen on many websites.

Expedia.com Privacy Policy

Below you will find the updated Privacy Policy for www.expedia.com. We value your trust, and make it a high priority to ensure the security and confidentiality of the personal information you provide to us. Please read this policy to learn about our privacy practices. By visiting this website, you are accepting the practices described herein.

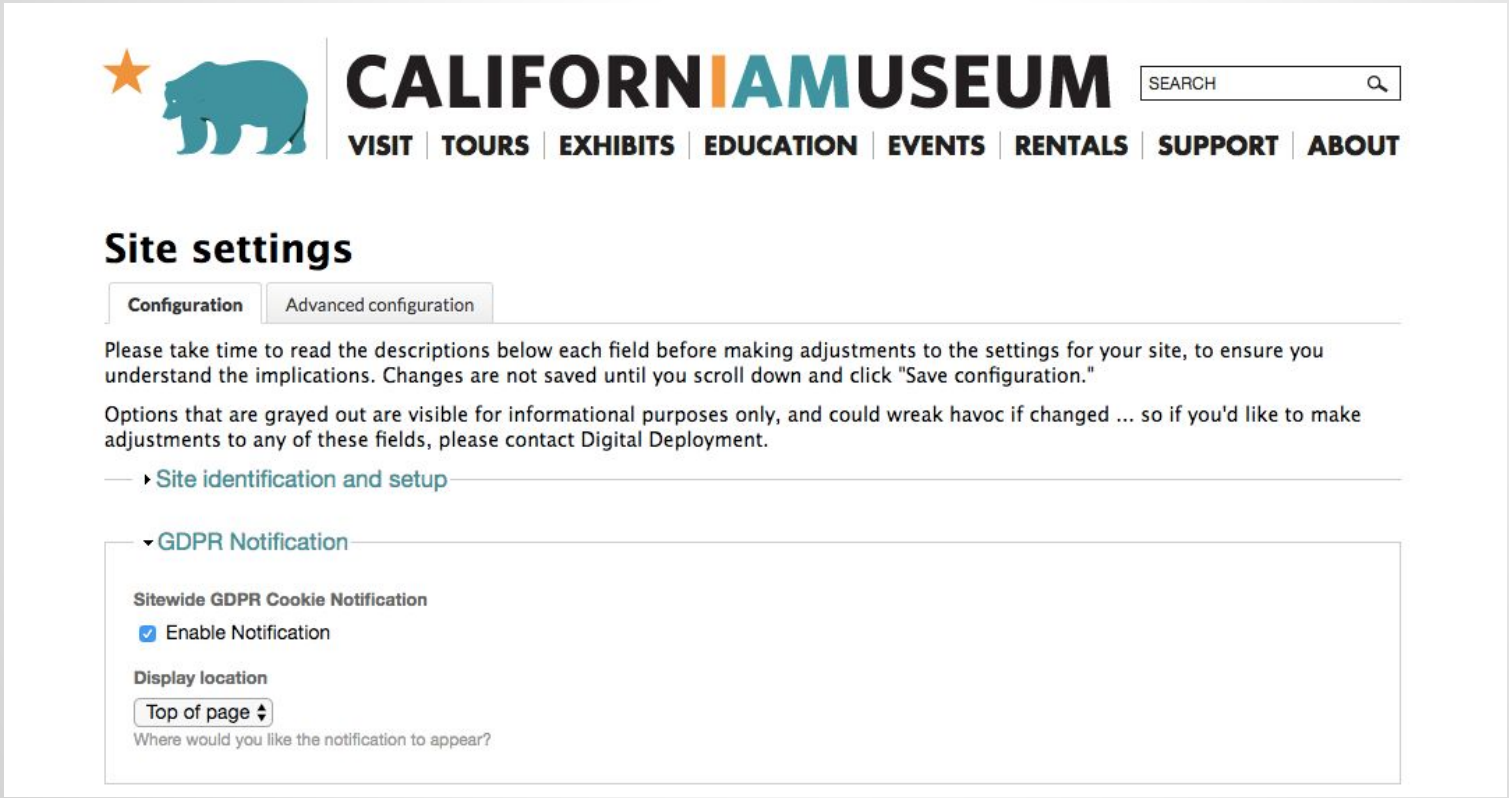
Privacy policy generators

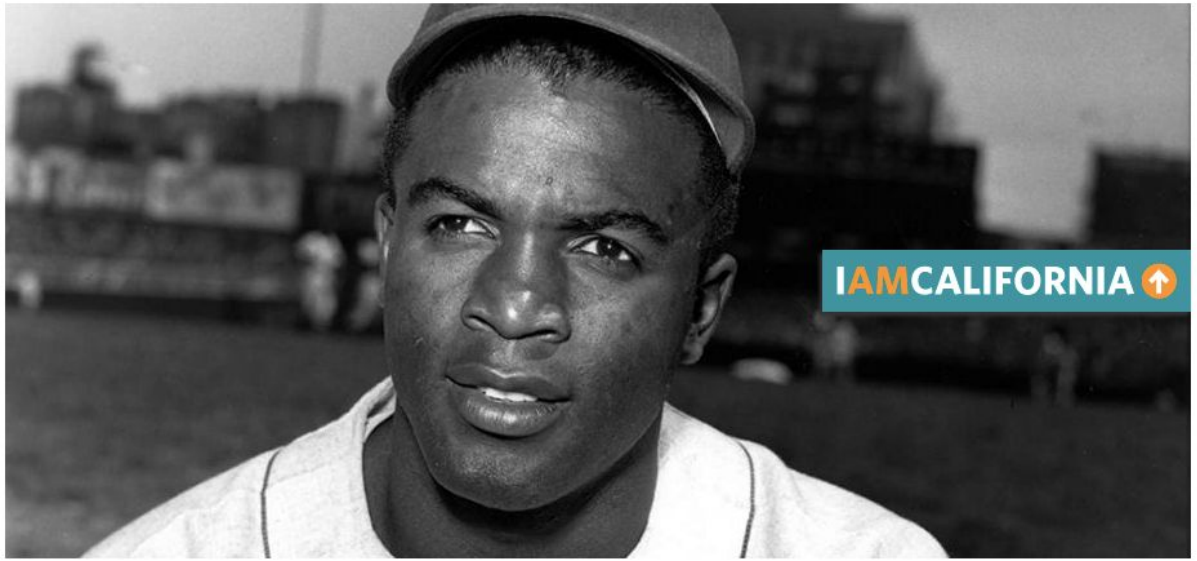
https://digital.com/blog/best-privacy-policy-generators/

2. Add a cookie notice

- ✓ A GDPR-compliant notice will be available in the July release. It will be enabled from your settings page.
  - If you would like to install this notice prior to the July release, please submit a support ticket with the request.
- ✓ Note: Your DD site does not serve cookies to your non-logged in visitors, however third-party services installed on your site (such as Google Analytics) do serve cookies.

New Setting Coming in July





3. Clean up MailChimp

- ✓ How to collect consent with GDPR forms.
- ✓ Scan for EU IP addresses. Send double opt-in notice to those subscribers and have them resubscribe.
- ✓ If you have EU subscribers, you should take GDPR seriously.

4. Check out these resources

- ✓ GDPR compliant? Here's a handy five-step preparation checklist
- ✓ GDPR: A cheat sheet
- ✓ 5 Actionable Steps to GDPR Compliance with Google Analytics

Thank you!

Mac Clemmens
mac@digitaldeployment.com

Heather King
heather@digitaldeployment.com

www.digitaldeployment.com