mediastead

Digital Marketing Rocket Fuel

Jason Tweed
jason@mediastead.com
215-253-3737

1

Best Practices in Website Privacy

DEVELOPING PRIVACY POLICIES AND PROCEDURES FOR YOUR SMALL BUSINESS

2

Why?

Why is it important to establish policies and procedures regarding privacy on your website?

- California and European Union Laws
- HIPAA and PCI compliance
- Inevitable laws protecting other citizens
- Consumer confidence
- Mitigate risk
- Mitigate Civil Liability

3

The Laws

GDPR	CCPA
(General Data Protection Regulation)	(California Consumer Privacy Act)
Effective May 25, 2018	Effective January 1, 2020
Applies to all companies doing business in the EU	Applies to all residents of California, regardless of location of transaction
Strict compliance protocols	Strict consumer protection
Substantial penalties for noncompliance	Civil and governmental penalties may apply

4

Personal Data

What is considered Personal Data?

- Name
- Address, Phone, Email
- Government ID numbers (SSN, drivers license, etc.)
- Age, gender, ethnicity, national origin, religion
- Location, GPS, IP address
- Health , Financial data, employment history
- Usernames, pseudonyms, passwords, security questions
- Photos or descriptions of physical characteristics
- Comments, opinions, affiliations, political or social leanings, occupations, hobbies, and more.

5

Protected Rights

What rights do consumers have?

- Transparency: What do you collect? How do you use it?
- Simplicity: Policies must be clear and concise.
- Right to Access
- Right to Rectification (GDPR)
- Right to be Forgotten
- Rights to Limit Processing and Portability (GDPR)

6

Your Risk

Your real risk is relatively small; however penalties are substantial.

GDPR

- All businesses doing business in EU
- Maximum fine 4% of global revenue or €20 million, whichever is GREATER
- Fines for privacy breaches and/or noncompliance
- Member states are permitted to penalize individually and additionally

CCPA

- Businesses over $25 million or 50,000 users
- Penalties of $2500-$7500 per user
- Civil liability of $100-$750 per user
- Individual civil suits may also apply

7

Identifying a Data Protection Officer

Under GDPR every business must assign a Data Protection Officer, an individual or organization that is specifically knowledgeable and responsible for data collection, storage and use. The DPO can be an employee or a third-party organization.

Your Data Protection Officer must:

- Be knowledgeable and qualified regarding data collection, security and storage.
- Be publicly identified with contact information
- Report directly to senior level management
- Have the ability to access, update, and remove personal data

8

Responsibilities of your DPO

- Respond to Requests within 72 hours
- Rectify requests within 30 days (CCPA)
- Identify and assess security breaches
- Report security breaches to DPA (GDPR)
- Disclose security breach to consumers within 72 hours with specific actions if necessary
- Report and cooperate with law enforcement in the event of a criminal security breach
- Rectify gaps in security

9

Words of Wisdom

From Jason Tweed

- Transparency is paramount.
- Data collection and processing is useful to your clients but deserves respect.
- *Transfer liability wherever possible.*
- *Prevention always beats rectification.*
- *Be good stewards of the Internet.*

10