Cheatography

General Data Protection Regulation (GDPR) Cheat Sheet

by [deleted] via cheatography.com/2754/cs/7064/

Introduction

The European Union agreed on a new privacy law, expected to set the worldwide standard for the collection and usage of data online. When the General Data Protection Regulation (GDPR) is passed, companies doing business in the 28 member states of the EU will have two years to shift their online strategies to accommodate opt-in and data transparency policies or face fines of up to 4% of their total revenues.

The new regulations will force online marketers to consider these critical points to be compliant by 2018.

Credit: http://www.dmnews.com/privacy/what-you-need-to-do-to-satisfy-the-eu/article/460921/

1. Do a privacy assessment

Benchmark your current strategy against existing laws and best practices, build a business case for future investments, and present your new privacy initiative to your company's board of directors.

2. Hire a data protection officer

If one of your core activities isthe systematic collection of personal data on a large scale, this is a must. Your DPO should partner with privacy peers to align controls and policies with an eye toward establishing privacy as a competitive differentiator.

3. Establish a breach notification plan

The law allows enterprises only 72 hours to issue notice of a significant data breach. It's tough enough to give proper notification to regulators, but tougher to communicate it in a sensitive fashion to customers. Plan for failure and be ready to leverage corporate communications and marketing staff—as well as third parties—to get the job done.

4. Reassess your outside data/analytics providers

Under GDPR, they too can be held liable for privacy violations. This changes the arrangement in two ways: They may charge more to allow for costs of compliance and they may need more visibility into your data, thereby exacerbating the risk of data leakage.

5. Know where all the data is

The GDPR's “right to be forgotten” clause gives users full access to and control of the data you keep on them. As a result, you have to know where personal data is at all times and be ready to delete it. Third-party contracts must also allow for immediate data deletion.

6. Think of the children

GDPR sets the age of digital consent at 16, though member states can decide to lower it to 13. What, however, will stop a 13-year-old from setting up accounts when visiting countries where they're digitally legal? Don't count on box-checking mechanisms to cover your liability here. Instead, institute initiatives to educate kids about privacy and security risks online.

EU General Data Protection Regulation (GDPR)

7. Home in on the opt in

Plenty of companies have complied with opt-in rules set in the EU, but regulators continue to snare some not following the letter of the law. One issue to watch out for: failing to get user consent to share their data with third parties.

8. Be specific and hold to it

Be specific about why you are collecting a person's data and what exactly you'll do with it. For instance, if your privacy policy states that a resume submitted by a job-seeker will only be accessed by your recruitment team, be sure to revoke access when the process is at an end.

9. International data transfers remain a question

GDPR doesn't set new rules for international transfer of business data. While waiting on a new Safe Harbor agreement, U.S.-based companies should evaluate this situation on a nation-by-nation basis.

10. Procedures to disclose data to law enforcement

GDPR has a rule stating that data controllers cannot disclose data in its entirety and must notify the relevant data protection authority when a request is made. Concerned companies can use encryption and data masking to make data unusable, but it's essential that they manage their encryption keys accurately

10. Procedures to disclose data to law enforcement

GDPR has a rule stating that data controllers cannot disclose data in its entirety and must notify the relevant data protection authority when a request is made. Concerned companies can use encryption and data masking to make data unusable, but it's essential that they manage their encryption keys accurately

Closing Remark

Another example of government creating regulations designed to drive small companies out of business. Many will not be able to afford the increased costs. Protecting consumers is important but so is protecting small businesses. It is the government's responsibility to ensure that our networks are secure for everyone.