TEALIUM

Data Governance Checklist

5 Steps for Balancing Customer Experience with Privacy & Security

In May 2018, the General Data Protection Regulation (GDPR) will take effect, enforcing all organizations to abide by a new set of guidelines and protocols. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's legal emphasis will be critical for businesses operating across borders in today's digital economy.

This is a massive opportunity for companies to differentiate their brand and safeguard consumer confidence by proactively embracing security and privacy. From the vendors you choose to work with, to the policies and procedures in place, take these five steps to jumpstart your data governance strategy and prepare for successful integration across your organization.

☐ STEP 1: Perform Due Diligence

Audit data flows to know where and who have access.

Business Team

- ☐ Identify vendors in use
- ☐ Validate vendor access
- ☐ Review current contracts

Technology Team

- ☐ Audit vendor technology
- ☐ Review vendor policies
- ☐ Remove non-compliant or unused vendors

☐ STEP 2: Start a Data Inventory

Take an inventory to understand what type of data is being processed and if it is required.

Business Team

- ☐ Agree on data sensitivity both from a legal and experience perspective
- ☐ Agree on the data needed to run marketing vs. operations
- ☐ Document data requirements for running the business

Technology Team

- ☐ Document where the data is stored:
  - ☐ Customer ☐ Campaign ☐ Enterprise (Financial/HR)
- ☐ Ensure that data handling is in compliance with business policies and legal requirements
- ☐ Check vendor integrations

☐ STEP 3: Build Controls

Develop procedures to provide clear and accurate notice of data usage both internally, with policy and process, and externally, through notification, terms and conditions.

Business Team

- ☐ Verify proper contracts with vendors
- ☐ Create governance policies and processes
- ☐ Update external and internal communication

Technology Team

- ☐ Configure vendors for 'least-access'
- ☐ Create data audit guidelines and tests
- ☐ Test and audit internally for compliance

← Ensure employee training across the organization →

☐ STEP 4: Form a Data Governance Panel

Activate against internal processes for both business and technology teams to move forward.

Business Team

Communicates with Technology team on:

- ☐ Needs to drive marketing and customer experiences
- ☐ Legal ramifications of non-compliance
- ☐ Expectations of the business on technology

Technology Team

Communicates with Business team on:

- ☐ Best practices with access, transmission and storage of data
- ☐ Protection of the data and the customer from 'bad' players
  - ☐ Internal ☐ External ☐ Partner
- ☐ Enablement of the business within reason

☐ STEP 5: Provide Clear and Accurate Notice

Communicate your data policy across the organization, and to customers and vendors. It's everyone's responsibility!

Business Team

- ☐ Update Privacy Policy to reflect data usage (ex. cookie policy, IP usage)
- ☐ Provide means for opt-out across all marketing
- ☐ Communicate with Technology team on evolving data usage

Technology Team

- ☐ Provide customers with Explicit Opt-In/Out
- ☐ Ensure 'Right to be Forgotten' and general data deletion directives
- ☐ Communicate to Business team and vendors of compliance changes or lack of

As new laws and large financial penalties emerge around data privacy, having Tealium as a trusted partner builds confidence in your business' ability to appropriately and legally manage data. Contact us today to learn more: www.tealium.com

Tealium Inc. | 11095 Torreyana Road, San Diego, CA 92121 | p: 858-779-1344 | f: 858-345-3844 | www.tealium.com