GDPR: AN ANTI-CHECKLIST CHECKLIST

Compliance isn't a matter of quickly checking a few boxes. It requires big changes in your culture, with new ways of thinking and doing.

The General Data Protection Regulation (GDPR) will begin to be enforced in May 2018. Governing the European Union, as well as non-European companies with European data centers and audiences, GDPR is a game-changing law, giving individuals more privacy rights than ever before. Valid consent will be more difficult to obtain and keep, new rules around the "right to be forgotten" and data portability will demand faster processes, and fines of up to 4% of annual global turnover or €20 Million (whichever is greater) for non-compliance will be possible. You'll need to rethink how your business deals with data and the consumers associated with it.

There are no quick fixes, no easy checklists, no simple tweaks to policy statements. Instead, here are five major changes your business needs to make. Think of these bedrock changes as an anti-checklist checklist.

□ 1. Get personal with your data subjects.

To comply with GDPR, you need to have a thorough understanding of where data comes from and what it can be used for. Creating a complete view of the customer, across marketing channels and devices, will enable you to identify and understand the customer better, so you can better manage the legal grounds under which you use and share data. You'll also be able to respond faster to consumer requests to access, correct, port, suppress, and erase data. It will speed compliance and the creation of a complete customer view, and also allow for the delivery of a better customer experience.

□ 2. Define a customer data owner.

Too often organizations store customer relationship information in silos. That means customer data gets siloed too, making an erasure request an Olympic decathlon of stakeholder buy-in and coordination. Designate a single team as your data owner and source of truth. It will speed compliance and the creation of a single customer view.

□ 3. Hire privacy engineers.

Or at least train engineers to think about privacy. With new requirements like data protection impact assessments, and privacy by design, the employees in your data protection office need more than traditional privacy and compliance knowledge. The ability to understand sophisticated engineering diagrams, map data from collection throughout its lifecycle, and design secure solutions that automate demonstrable compliance are now the critical skills a GDPR-ready company needs. Example: certain processing operations require more data de-identification. If you can work with hashed data, do it!

□ 4. Get agile.

Integrate your data protection office into your engineering organization's systems development lifecycle to keep up with your rapidly changing data collection and use. This ensures privacy is considered by default, not as an afterthought. It also lets you: a) stay on top of portfolio development, all the way through the product lifecycle issues, identifying defects and bugs that could affect data subjects and b) course-correct as early as possible to minimize the impact. For higher-risk offerings, consider wider stakeholder engagement such as consumer research. Plus, if you get the privacy engineer you hired to write up business rules, complete with user stories and test cases, you can automate the implementation and testing of your privacy guidance (a.k.a., demonstrable compliance).

□ 5. Stop data hoarding!

Not every last bit of data is useful in perpetuity. And while the cloud has made storing it cheaper and more secure, it doesn't magically make it useful. Data minimization is not just a fair information practice principle, it's good business. Data you've already deleted can't be affected by a security breach! Only invest in the collection and storage of data that drives value for you and the data subject, not that MAC address collected ages ago from a first-generation iPad that can't update past iOS 5.

Get started on your journey and conduct a privacy impact assessment that evaluates and provides recommendations for implementing data ethics at your organization. Contact info@acxiom.com for more details.

acxiom®