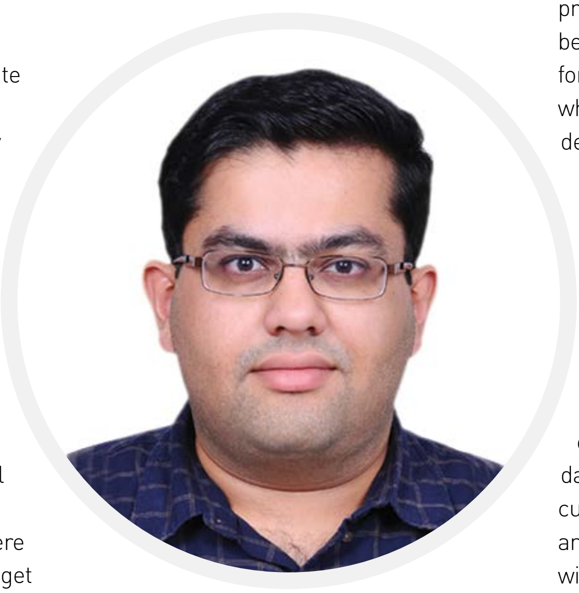
SIX STEPS TO ACHIEVE PRIVACY COMPLIANCE GOALS

Privacy is a relatively subjective term in corporate environments. For most companies, contemporary privacy compliance rests squarely on the shoulders of the IT department, as other departments consider privacy to be a technology issue. But, let's be practical; how can one department single-handedly manage the privacy compliance of an entire company?

While addressing the plethora of data protection laws worldwide, as well as specific regulations like the General Data Protection Regulation (GDPR), there are many opportunities for IT teams to get lost. Adhering to privacy regulations is no longer a marketing hook; it's a serious obligation, and companies can't afford to have the "it-can't-happen-here" approach anymore. If you work for a tech company, here are six steps you can take to achieve privacy compliance.



Chandramouli Dorai, Marketing Analyst, ManageEngine

Strict privacy settings by default

Any action that involves the processing of consumers' personal data must be handled with privacy in mind, and companies should enable the strictest privacy settings by default. For example, by removing the tracking code on websites and applications, you can achieve the highest level of compliance. Although tracking codes are useful for marketing and product development teams' decision-making, you should remove them. Also, sharing customers' behaviour patterns with Google Analytics, Crazy Egg, Hotjar or others without customers' consent invites unwanted trouble for your company.

Department-level DPOs

With new regulations, such as the GDPR, it's vital to have a data protection officer (DPO). That said, appointing one DPO for the whole company won't help you completely achieve your compliance goals. In our case, we decided to appoint individual DPOs for every department, with one centralised DPO for the entire company. This helped us understand the various privacy-related use cases of each team, as well as how to address these use cases according to our compliance standards—all under one common framework.

Risk-driven development

Emerging research and development are the lifelines of every technology company. However, by using data mining and AI techniques to analyse user behaviour, tech companies' privacy concerns are exacerbated. In our case, we began adopting a risk-driven model to our R&D, which helped us identify and mitigate pressing privacy risks well before we rolled out anything into production. This model allowed our developers to prioritize risks, apply the right mitigation techniques, and save a lot of time.

Using the right language

When it comes to privacy compliance, there's a lot of jargon used across various departments. To tackle this situation, we decided to translate all commonly used privacy terms into plain English. Also, we began awarding privacy points to teams for achieving internal compliance goals, which they can redeem as cash, and deducting points whenever there was a violation. This helped our employees use the right terms, understand things quick and easy, and solve privacy issues together.

Automate privacy controls

Knowingly or unknowingly, employees end up breaching privacy policies; for example, leaving papers with customer data in a printer tray, loosely sharing customer information on internal forums, and sharing event participants' details with other internal teams.

To combat this, our company built intelligent bots into our internal chat service, Cliq, which helped us quickly identify privacy violations. Now, if an employee tries to share information that appears to contain personal data, such as phone numbers and email addresses, a bot automatically pops up awnd warns the user not to share personally identifiable information. By building such automated intelligent controls, we helped our employees learn privacy rules contextually.

Maintain an activity register

It's important to document who handles which tasks in order to monitor who is accountable; this can be done using a responsibility assignment matrix (RACI). By using RACI matrices at the department level, we were able to significantly improve the overall success rate of our compliance programs. As an example, our developers listed their top 20 routine tasks in an internal RACI matrix document. If there were any deviations from their respective routines, privacy teams would reach out to the relevant developer as quickly as possible.