BASS BERRY + SIMS

GDPR Top 5 Actions You Should Take NOW

The EU's General Data Protection Regulation (GDPR) goes into effect on May 25. As most organizations are aware, the GDPR applies not only to EU businesses but also many companies in the U.S. While the deadline is quickly approaching, most organizations are still grappling with the implications of the regulation on their business. Even if your readiness efforts are behind the curve or the May 25 date has passed, the following five actions will help you begin your efforts toward compliance and help mitigate your organization's risk in the short-term.

1. Perform an assessment of data processing activities.

Assemble a team of stakeholders across the organization and ask the following questions:

- **What personal data* do we collect?**
- **Where do we get the data?**
- **How does our system protect the data we receive?**
- **What is the risk involved in the collection process and what lawful basis do we have for processing the data?**

Understanding the kind of data you have and how it is processed and shared is essential to understanding your compliance obligations and prioritizing solutions for the most high-risk areas.

2. Update external privacy notices, internal data policies and consents.

- **Privacy Notices.** These policies are highly visible to regulators and can easily be checked and verified. In fact, many data protection authorities have specifically identified transparency and privacy notices as an enforcement priority.
- **Data Policies.** As you update your privacy notices to data subjects, also address internal policies for how your organization handles data and responds to security incidents, including documenting security protocols, data classification and how you will comply with data subject requests.
- **Consents.** Where you rely on consent (e.g., for marketing communications), update your consent mechanisms to make sure they meet the GDPR's enhanced requirements. "Refresh" consents for your existing database if they were obtained in a manner that does not meet the GDPR standard, such as by sending a re-permissioning email or upon users' next account login.

**Keep in mind that "personal data" is broad and includes any information about an identified or identifiable individual, even where the data may be stripped of identifiers such as name and social security number (e.g., location data, online identifiers, etc.).*

3. Update vendor and third-party

Start with third parties who perform processing activities for personal data that may pose a significant risk to individuals or your organization. Assess what kinds of documentation you have on file regarding their security controls, and update or enter into new contracts with clauses that address the requirements under Article 28 of the GDPR. Add a layer of due diligence for current and new third parties who have access to personal data.

4. Review and update security controls.

The GDPR requires "appropriate technical and organization safeguards to ensure a level of security appropriate to the risk." Start by ensuring you have the right procedures and controls in place to detect and remediate security threats. Then evaluate and update technical and organization safeguards for the highest-risk data and processes first. Compare your efforts against publicly available standards like NIST, PCI-DSS and others. These measures may include the following:

» **Disaster recovery and business continuity plans**

» **Internal data handling policies and procedures**

» **Internal education and awareness efforts**

5. Establish governance and demonstrate accountability.

Set up a form of governance with ongoing responsibility across the company. This process will involve education and awareness-building, and require ongoing documentation and refreshed assessments. The initial set-up of your compliance framework will take time and resources – you can't afford to let that work go to waste! You will need to continue and maintain those systems and policies by creating a culture of privacy management and accountability across your organization.

Preparing for the GDPR can be a complicated and confusing process, and understanding where to invest your compliance efforts to mitigate risk has never been more important. **For assistance with your GDPR compliance plan, click here.**

The Intellectual Property & Technology practice at Bass, Berry & Sims is a full-service, nationwide practice for technology-related transactions, litigation and regulatory matters, as well as commercializing and protecting IP rights. Whether negotiating complex technology agreements, securing and enforcing patents or trademarks, or advising on privacy and data security matters, our sophisticated intellectual property group works closely with clients to provide business-minded solutions and achieve results in an efficient manner. **To learn more, click here.**

Shelley R. Thomas
Member

615-742-7900
srthomas@bassberry.com

Jaime L. Barwig
Associate

615-742-7832
jbarwig@bassberry.com