CONSTANGY DATA PRIVACY CHECKLIST

constangy.com

Constangy Data Privacy Checklist

1. Conduct a Data Inventory

Some laws require a record of processing, but even if the record is not legally required, it will help your organization better understand how data is handled and potential compliance gaps or risks:

- □ Identify the personal and sensitive data that your organization collects
- □ Catalogue the manner in which data is used and shared
- □ Understand where data is stored, who has access, how it is secured, and how it is disposed of

2. Review Governance Program

Robust governance programs help define what data privacy means for an organization, and promote consistency (and efficiency) in its application across organizations:

- □ Ensure policies and standards are up to date with applicable laws (e.g., California Consumer Privacy Act, the European Union General Data Protection Regulation)
- □ Clearly communicate policies to employees, and supplement them with quick guides and other ways of helping make the standards easier to put into place in their day-to-day job performance

3. Train employees

Employees should be regularly trained and tested on their understanding of how to maintain data privacy:

- □ Ensure all employees receive annual or more frequent training on key data privacy principles, such as safeguarding sensitive data and recognizing phishing or other cyber threats
- □ Make sure certain employee groups receive specific training relevant to their jobs. For example, training for marketing on consent requirements, or for customer service on handling individual "rights requests"

4. Update notices and disclosures

Privacy policies and disclosures are highly visible indicators of your organization's understanding and commitment to its compliance obligations—regulators and litigious individuals often look here first:

- □ Make sure notices fully inform individuals of how their personal data is collected, used, and shared
- □ Make sure privacy policies accurately describe your organization's data practices, especially in areas such as cookies and other tracking technologies

Constangy Data Privacy Checklist

5. Streamline rights and preference management

Enabling individuals to have freedom of control over managing their personal information goes beyond compliance. It also promotes a positive impression of your commitment to data privacy:

- □ Make sure "rights request" processes are easily found, easy to understand, and easy to navigate and complete
- □ Make sure your organization has established processes in place to efficiently receive and complete requests (many laws have tight deadlines)

6. Strengthen data sharing management

Regulations are requiring organizations to impose tighter control over how data is shared, not just externally, but internally as well:

- □ Update contracts to include data protection agreements
- □ Audit third-party vendors for compliance with data privacy regulations
- □ Identify any international transfers of data from one jurisdiction to another (using inventories) and determine if additional legal requirements apply

7. Enhance data security controls

When it comes to data privacy and security, privacy is like closing the blinds whereas security is putting locks on the doors:

- □ Perform a security audit to check for vulnerabilities
- □ Strengthen access controls by implementing role-based access to limit data exposure and regularly review/update access permissions
- □ Update protections such as ensuring software and systems are up to date with latest patches, and enabling multi-factor authentication

Constangy Data Privacy Checklist

8. Prepare to minimize breach impacts

It's well-known that incidents are a matter of "when" not "whether"---make sure your organization is able to be more proactive than reactive:

□ Assign roles and responsibilities for breach management

□ Develop and test an incident response plan

9. Implement positive data hygiene

Good data practices not only reduce risks, but also improve the effectiveness and efficiency of the organization:

□ Implement data minimization practices; less data equals less risk

□ Enforce data retention standards and dispose of data when there is no longer a purpose for keeping it (does not always mean purging data; consider other options like anonymization)

10. Promote accountability

"Excellence is not an act, but a habit"—compliance with data privacy must go beyond one day of the year:

□ Stay informed about evolving privacy regulations and updates in your jurisdiction

□ Consult with legal experts to ensure ongoing compliance

□ Data privacy affects all parts of an organization—be a champion for "Privacy by Design" regardless of whether you work in legal, compliance, information security, or are a business lead in your organization