Privacy by Design for Nonprofits

By Gail Spielberger, CIPM, BDO USA

Copyright © 2021 BDO USA, LLP. All rights reserved. www.bdo.com

Privacy in the age of modern technology is a major concern for individuals and, moreover, is the focus of laws and regulations directed at organizations that use personal data. The fast-moving digital landscape has not only challenged current lawmakers, but has also resulted in an erosion of public trust in how data is used, stored, transmitted and protected. As organizations, including nonprofits, adopt new technologies, services and business operations, they must be proactive about their data policies and practices to assure individuals their personal data is safe, and likewise reduce the likelihood of data loss, unauthorized disclosure or misuse.

What Is Privacy by Design?

Privacy by Design (PbD) is an approach that considers privacy concepts from the moment a product, service or business process is designed or planned, from inception to implementation. This means that products, services and applications must be designed and developed to protect privacy from the beginning rather than applied later as an afterthought.

Some privacy laws and regulations, such as the General Data Protection Regulation, legally require organizations to apply PbD principles as part of their organizational data practices. As part of these regulations, organizations may be required to provide evidence that they have implemented PbD. This documentation not only demonstrates compliance to regulators, but it also allows your organization to recognize potential privacy issues so risks can be identified and mitigated as projects move forward. Further, these privacy implementations will provide your enterprise with a framework to comply with privacy and data protection laws and regulations, and can strengthen your reputation while differentiating your organization from the competition.

Privacy by Design (PbD) is an approach that considers privacy concepts from the moment a product, service or business process is designed or planned.

What Does This Mean in Practice?

There are seven PbD principles that serve as an overarching framework for organizations to insert privacy and data protection early, effectively and credibly into information technologies, services or business practices. The information below provides the foundation for your organization to implement PbD principles for new projects where personal data will be collected, used, processed or stored.

PRINCIPLE 1.
Proactive not Reactive; Preventive not Remedial

Anticipate and prevent privacy events before they occur by:

- Creating individual awareness and adoption at the highest levels of the organization, mandating and enforcing high standards as it relates to data protection.
- Promoting a culture of accountability.
- Establishing methodologies and processes to identify data protection risks to ensure they are remediated in a timely and systematic manner.

PRINCIPLE 2.
Privacy as the Default

Build privacy into systems and processes so that personal data is protected automatically, by default, with no additional action required by the individual. This principle can be achieved by:

- Collecting only the minimum amount of data actually needed for specific business purposes and destroying or anonymizing data once it is no longer necessary for those purposes.

- Ensuring personal data is used only for a specific defined purpose and not repurposed unless proper notification and/or consent is provided.
- Not using personal data without a legal basis or consent from the individual.
- Applying reasonable technical and organizational security measures to safeguard against unauthorized access, loss, destruction, modification or disclosure of data.

PRINCIPLE 3.
Privacy Embedded into Design

Integrate privacy into technologies, operations and information architectures to evaluate risks early in the ideation and design processes. Privacy should be embedded in the design and development process, not just considered after the fact. Consider:

- Adopting a systematic approach to embedding privacy in the design and development phases of each project, technology or business process.
- Systematically conducting Privacy Impact Assessments, Data Protection Impact Assessments and Vendor Risk Assessments to clearly identify and assess privacy risks.
- Measuring the risks and considering alternatives or mitigating actions.

PRINCIPLE 4.
Full Functionality – Positive-Sum, not Zero-Sum

Accommodate all business objectives, not just privacy goals, to achieve practical results and benefits for all parties and business units involved by:

- Embedding privacy in a way that does not impair the intended functionality, technical capability or business need.
- Carefully considering all requirements to achieve the optimal multi-functionality of each product.

PRINCIPLE 5.
End-to-End Security – Lifecycle Protection

Personal data needs to be protected throughout the entire information lifecycle from initial collection through destruction. Aim to collect, process, use, share, maintain and destroy personal data in a secure and timely fashion. Consider:

- Building protections for the secure destruction and disposal of personal data when it is no longer needed.
- Monitoring data transfers and ensuring appropriate safeguards and contractual arrangements are in place prior to doing business with third parties.
- Adopting appropriate access controls, encryption standards, data backups and continuous monitoring to ensure personal data remains accurate, with its integrity and availability intact.

Build privacy into systems and processes so that personal data is protected automatically, by default.

PRINCIPLE 6.
Visibility and Transparency

Establish accountability and trust through transparency by informing individuals what data will be collected, how it will be used, and with whom it will be shared. Transparency is not just displaying what the organization does, but also bridging the gap between expectations and reality. To meet this principle, consider:

- Making privacy notices easily accessible and written in clear and simple terms in order to avoid overwhelming the reader with information.
- Mandating and enforcing privacy-related policies for employees and ensuring that vendors are evaluated to identify and mitigate risk in a timely manner.
- Keeping accurate records of data, how it is being used, with whom it is being shared, where it is stored, how long is it being stored for and how the data will be destroyed when no longer necessary.
- Allowing individuals to access and correct their information.

PRINCIPLE 7.
Keep it User-Centric

Respect individual privacy and provide employees, customers and third parties with an effective privacy experience. This means providing them with clear choices about how and when your organization will communicate with them, as well as ways to opt out of having information shared with others and the right to have their data deleted. Consider the individual by:

- Obtaining consent to collect and use individual data in specific ways and allowing them the ability to modify or withdraw their consent if possible.
- Consciously designing products, systems and applications with the individual and their protection in mind.
- Limiting the amount of data your organization collects to reduce overall risk and liability for the individual and the organization alike.

Conclusion

As stated above, Privacy by Design is about examining how your organization uses personal data and what impact that use will have on individuals. By incorporating the aforementioned principles into your operations, your organization will be able to better: capture and mitigate risks, understand the data it possesses, demonstrate compliance to regulators and maintain respect for individual privacy.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.