Microsoft

# Nonprofit Guidelines for Cybersecurity and Privacy

Microsoft Philanthropies

# Executive Summary

It's no wonder that digital security and privacy compliance are top of mind for many nonprofit leaders today. Cyber threats have never been so prevalent and data privacy issues so complex.

In the past, cybersecurity and privacy were often low on the list of nonprofit priorities—but times are changing. The stakes for nonprofits are increasingly high. Breaches, compromised data, and cyberattacks can put vulnerable beneficiaries at risk, disrupt nonprofit operations and services, expose nonprofits to liability, and tarnish the reputation nonprofits have so painstakingly built.

As a result, nonprofits are now paying attention. Yet many nonprofits are still unsure how to move forward. They often do not know how best to develop cybersecurity or data protection strategies that meet the evolving needs and challenges of today's online environment. Even when strategies are put in place, execution is inconsistent. Nonprofits often lack the budget, staffing resources, or management time needed to implement cybersecurity and privacy protections effectively, making their job far harder than it is for for-profit or public sector organizations.

This paper is designed to help nonprofits begin to tackle these challenges and to help them develop into digitally resilient organizations. It identifies key cybersecurity and data protection challenges for nonprofits, and outlines possible first steps nonprofits can take to bolster cybersecurity and protect data—including a shift to cloud computing, which offers built in security features, as well as data access and protection systems, that often far exceed what nonprofits could obtain through their own on premise IT systems. It also lists further resources for readers who want additional information.

After reading this paper, nonprofit leaders will be better able to articulate the importance of cybersecurity and privacy to their key stakeholders, and to communicate how a robust cybersecurity and data protection strategy will ultimately help the individuals and communities nonprofits serve. And they will have a well-marked path to help them move towards the development and implementation of that strategy—to better protect the nonprofit, its staff, its donors, and ultimately the beneficiaries they all seek to serve.

# Contents




Support provided by:

Microsoft Privacy: https://www.microsoft.com/trustcenter

Microsoft Cybersecurity: https://www.microsoft.com/security

Microsoft Philanthropies: https://www.microsoft.com/philanthropies

# Introduction

Around the world, nations, cities, and neighborhoods rely on nonprofit organizations to deliver critical community services, including primary health care, education, housing, emergency response, refugee and immigrant services, and senior services. Nonprofits have increasingly adopted technology to improve their effectiveness and to scale their services to extend their reach. Yet many nonprofit organizations have struggled to focus the same attention on their cybersecurity and data protection planning. This lack of attention could expose nonprofits to potential (and expanding) security and regulatory risks that most nonprofits simply cannot afford.

In 2016, four of the top **15 contractors** for the city of New York were nonprofits with contracts worth **$404 million dollars**. Governments regularly entrust nonprofits with significant financial and social responsibilities.

**Mayor's Office of Contract Services**

To minimize this risk, nonprofits should develop strategies to incorporate the concept of resiliency—the ability to withstand natural, manmade, and cyber threats. Specifically, they should work to ensure both the **security** and **privacy** of their IT systems to reduce the chance of exposing their beneficiaries, staff, or donors to online attacks. To start, organizations need to ask themselves two fundamental questions:

- Does the organization have the capacity to protect its staff and beneficiaries from malicious digital attacks?
- Is the organization ready to meet increasingly stringent data privacy standards and understand the serious penalties for compliance failure, nations and donors continue to demand?

Merely by asking these questions, nonprofits can build a head start on protecting their organization, staff, and beneficiaries. Yet many nonprofits are unsure of exactly how to find the answers. This paper intends to help and outlines:

- Why cybersecurity and data privacy are crucial considerations for any nonprofit,
- The actions necessary for nonprofits to improve their cybersecurity and data privacy measures, and
- How cloud technologies can support these efforts.

## A NOTE ON THIS PAPER'S INFORMATION SOURCES

Information presented in this paper has been drawn from Microsoft's corporate knowledge and external materials. In addition, data on the status of the nonprofit industry's has been drawn from partners and a small survey of 50 nonprofit organizations: 14 small (1–50 employees); 6 medium-size (51–250 employees); and 30 large organizations (with more than 250 employees). Respondents primarily included board members and information technology (IT) managers. With more than 1.5 million nonprofits registered in the United States alone, the survey is not a statistically accurate representation of the industry, but rather an indicator of the industry's current state. Although most respondents were from the United States and Europe, their answers can be considered relevant to nonprofits around the world, as they confront many of the same issues.

# Cybersecurity

Recent events have underscored the critical need to actively protect against cyberattacks on information technology systems, intrusions and thefts of sensitive information, and data breaches. Like their for-profit counterparts, many nonprofits handle sensitive information which may include refugee registration data, health data, information on human rights investigations, or other highly confidential matters. Holding such sensitive information can make nonprofits attractive targets for both state and criminal actors. At the same time, malicious actors know that many nonprofits lack the resources to modernize their technology and sufficiently protect themselves, making them easy targets for attack.

**The Cisco TacOps team** provides round-the-clock **advanced security protection** of more than 60 connectivity centers supporting over 400,000 refugees in Greece.

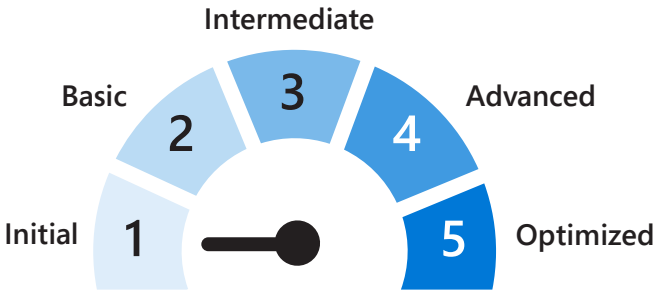
In 2016, they reported blocking **320,000 intrusion** attempts a **month.**

Although nonprofits confront the same cybersecurity risks as their for-profit counterparts, recent studies demonstrate that nonprofits generally lag for-profit organizations in adopting the robust policies, practices, and tools needed to adequately secure their environments.

NetHope, an international member-based nonprofit that focuses on promoting and supporting technology for nonprofits, commissioned a study[1] which looked at ten of its nonprofit members, all of which are considered well-respected and possess dedicated IT departments. These nonprofits were evaluated on eleven criteria related to cybersecurity and dtat protection policies and procedures.

Utilizing interviews and self-assessment surveys, nonprofits were evaluated on a scale of 1 to 5, where 1 indicated initial maturity and 5 indicated optimized maturity. NetHope evaluators believe that nonprofits need to achieve an intermediate maturity score of **3.8** to be considered to have sufficient cybersecurity infrastructure to adequately respond to the constantly evolving cybersecurity challenges they confront. In the 10 nonprofits evaluated, the average maturity for all eleven criteria was **1.8** and no nonprofit ranked above **2.2** in any of the eleven[2] evaluation criteria. Assessors gave the lowest scores in the areas of data retention and destruction, and of managing the lifecycle of hardware and software.

CYBERSECURITY MATURITY SCALE




[1] *See* John Ghent. "Data Protection (DP) Checkpoint Benchmark Report". Innovation Value Institute and Sytorus Data Protection Specialist. November 2016.

[2] In addition, nonprofits ranked staff awareness of cybersecurity and data privacy protection procedures as most important, yet their ability to deliver these protections scored only an average of **1.5**.

In addition to the NetHope research, Microsoft conducted a survey of fifty nonprofits through its partners TechSoup and NTen. Although most of the respondents reported that their organization had a modern IT infrastructure, Microsoft's survey identified that most respondents did not use important cybersecurity controls.

## SPECIFICALLY:

- **60 percent** stated that they did not have or know of an organizational digital policy that would identify how their organization handles cybersecurity risk, equipment usage, and data privacy.
- **74 percent** reported that they did not use multifactor authentication to access agency email and other business accounts. This is a critical security step in ensuring accounts are not compromised even if passwords are stolen.
- **46 percent** reported that they regularly used wireless printers, webcams, and other Bluetooth and wireless devices. Unsecured wireless devices on a network provide an entry for attackers; these devices must be actively managed and regularly updated with required software patches to ensure security.
- **92 percent** stated their staff could access organizational email and files using their personal devices. The remaining **8 percent** that did not permit staff to use personal devices for work reported staff did it anyway.

These surveys demonstrate many nonprofits struggle to manage their IT infrastructure and data, which is a critical step in ensuring organizational assets are secured and monitored. It is also clear from both surveys even large nonprofits with dedicated IT staff have a significant amount of work to do to bring their cybersecurity and privacy practices up to date. The authors of the NetHope report also point out that it can take 18 to 24 months for an organization to raise its maturity by one level[3], so nonprofits need to have a realistic understanding of the scope of work and time required to increase their capacity.

## CYBERSECURITY RESOURCES

Although it can take significant time for an organization to improve its capacity to respond to cybersecurity challenges, existing resources can help. There is no nonprofit-specific standard for cybersecurity; nonprofits are expected to use the same well-established risk-based approach to cybersecurity management other organizations use. Accordingly, nonprofits can rely on the voluminous guidance and best practices found in the business world, regulatory guidelines, and international standards to perform risk analyses, conduct internal assessments, effectively allocate resources, and formulate sound long-term security strategies.

Internally, Microsoft uses the **U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework**[4] and, consistent with regulatory guidance, encourages its use for organizations of all sizes, including nonprofits. The framework is an authoritative resource that provides a common taxonomy and mechanism to help organizations identify risks and make management decisions to mitigate those risks. Ultimately this helps organizations align their cybersecurity activities with their business requirements, tolerance for risk, and available resources.

[3] *See* John Ghent. "Data Protection (DP) Checkpoint Benchmark Report". Innovation Value Institute and Sytorus Data Protection Specialist. November 2016.

[4] *Framework for Protecting Critical infrastructure Cybersecurity,* NIST, 2014
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

## OTHER HELPFUL GUIDES INCLUDE:

- **Strategies to Mitigate Cybersecurity Incidents** is the Australian Department of Defense's guidance on the top four strategies to prevent over 85 percent of intrusions.[5]
- **UK Cyber Essentials** provides guidance to protect organizations from "the most common Internet threats", and is designed to be suitable for all organizations, including nonprofits.[6]
- Nonprofits handling information of Californian consumers are expected to look to the **Center for Internet Security 20 Critical Security Controls (CIS CSC)**[7] for guidance.
- Various additional resources provide additional cybersecurity guidance and requirements applicable to specific types of data, e.g., Payment Card Industry (PCI)[8] or **Health Insurance Portability & Accountability Act (HIPAA)**[9].

[5] *Strategies to Mitigate Cyber Security Incidents,* Australian Department of Defense 2017 http://www.asd.gov.au/infosec/mitigationstrategies.htm.

[6] *Cyber Essentials,* HM Government 2016 https://www.cyberaware.gov.uk/cyberessentials/.

[7] *Center for Security Controls,* Center for Internet Security. https://www.cisecurity.org/controls/

[8] *Assessing the Security of Your Cardholder Data,* NPCI Security Standards Council, https://www.pcisecuritystandards.org/pci_security/completing_self_assessment.

[9] *The HIPAA Security Rule,* U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/security/index.html

# Achieve greater resiliance



To achieve greater resilience, nonprofits can leverage the **NIST Cybersecurity Framework**, a set of industry standards and best practices to help organizations manage cybersecurity risks. The framework is not intended to be a prescriptive, one-size-fits-all approach. Instead, it is designed to allow organizations to reduce and better manage cybersecurity risks in a cost-effective way based on business needs[10]. When using the framework to bolster their own cybersecurity preparedness, organizations should focus on the following six programmatic goals:

### 1. Identify cybersecurity risks

Develop an understanding of the cybersecurity risks confronting the organization, including the risks to systems, assets, data, and capabilities. Doing so will allow the organization to better manage risks by focusing and prioritizing its cybersecurity efforts consistent with the organization's risk management strategy and business needs. As part of this process, organizations should:

- Ensure all relevant stakeholders understand the organization's business environment, including its mission, objectives, roles, and activities. This understanding can then be used to inform cybersecurity roles, responsibilities, and risk management decisions.
- Establish a cybersecurity governance structure through the development of information security policies, procedures, and processes to manage the organization's cybersecurity risk, including any applicable legal and regulatory requirements. Although cybersecurity is not currently as heavily regulated as data privacy, it is likely to become increasingly important for nonprofits to comply with legal and regulatory requirements soon. For example, in the United States, individual states have enacted data breach notification obligations, the European Union has recently enacted the Network and Information Security (NIS) Directive, and Canada, China, and Germany have all recently enacted cybersecurity laws. In addition, some have argued that directors and officers of nonprofits could soon face greater personal liability for breaches of security and their impact on a nonprofit[11].
- Conduct risk assessments to better understand organizational cybersecurity risk—including risks to mission, function, image, and reputation—and cybersecurity risks to its organizational assets, information, and individuals.
- Establish an asset management program to allow the organization to identify and manage assets—including data, personnel, devices, systems, and facilities—consistent with their relative importance to the organization and the organization's risk management strategy.

### 2. Protect against cybersecurity threats

Develop and implement safeguards to protect against cybersecurity threats by implementing practices that will help limit or contain the impact of a cybersecurity event. For instance:

- Establish access control procedures to limit individuals' access to what employees need to perform their jobs, adjust it when they change positions, and immediately revoke access when a staff member leaves the organization.
- Conduct training for staff and partners to ensure all users are informed and trained on cybersecurity awareness. This can include ensuring users develop an understanding of cybersecurity threats to them and the devices they use; how to recognize common types of cybersecurity attacks (e.g., phishing); and how to report a suspected cybersecurity incident.

[10] *Framwork for Protecting Critical Infrastructure Cybersecurity* at 1, NIST, 2014 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[11] Vignola, Susan M. Bell, Megan E. "Managing Cybersecurity Risk for Nonprofit Oranizations: A Fiduciary Duty?" *Data Security Law Blog,* 13 May 2016, *available at:* https://datasecuritylaw.com/managing-cybersecurity-risk-of-nonprofit-organizations-a-fiduciary-duty/.

Microsoft research shows it will take an average of **80 days** (11 weeks) to fully recover after detection of a cyber intrusion.

- Establish data security practices, which can help mitigate the impact of any potential cybersecurity incident or data breach. For example, many U.S. state data breach laws provide a safe harbor and do not require organizations to report breaches of personally identifiable information (PII) if only encrypted data was disclosed and the encryption key was not also compromised.
- Ensure cybersecurity is considered when implementing information security policies, maintenance and repair procedures, and any technical security solutions (e.g., by maintaining and reviewing audit records).

### 3. Detect cybersecurity incidents

Cybersecurity incidents are often difficult to detect. Microsoft security researches have shown on average, attackers spend **146 days** (20+ weeks) on a network before detection[12]. However, implementing certain processes and monitoring solutions makes it much easier to timely detect anomalies or security events impacting the organization's information systems.

### 4. Respond to cybersecurity incidents

Once a cybersecurity incident is detected, the organization needs to have a plan in place to efficiently and effectively respond to and contain the impact of an incident. Important components of cybersecurity incident response are:

- Planning for the incident response, including developing and testing an incident response plan.
- Coordinating incident response activities between internal stakeholders—including legal, information technology, communications, human resources, and others—and external stakeholders. Important external stakeholders can include, for example, outside counsel, forensic investigators, law enforcement, donors, and the organization's insurance agency[13].
- Conducting analysis—either internally or with the support of external stakeholders—to ensure the organization adequately responds to the cybersecurity incident. This analysis can also help support recovery by providing more detail about what occurred during the cybersecurity incident.
- Containing and mitigating an existing cybersecurity incident, including analyzing the circumstances or vulnerabilities that led to the incident to mitigate the risk of future incidents.
- Improve the organization's incident response activities based on lessons learned from the cybersecurity incident.

### 5. Recover from a cybersecurity incident

After a cybersecurity incident is over, the organization needs to recover and resume normal operations. Although a full recovery can take time, being prepared before an incident happens makes it easier for an organization to restore any capabilities or services that were impaired or lost and reduce the impact of a cybersecurity event. In particular, nonprofit organizations should consider developing procedures to execute recovery plans; ensure sufficient backup capabilities exist; update recovery plans based on lessons learned from the cybersecurity incident; and coordinate with internal and external stakeholders to safely and securely restore normal operations.

[12] Microsoft "Advanced Threat Analytics Data Sheet", 2017, Available at: https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

[13] Nonprofits may wish to consider obtaining liability insurance spedifically for a cybersecurity incedent in which data is damamged or stolen; this can help provide financial support as the organization recovers from a cybersecurity incident and help make compliance part of normal business practices.

Procedures for **managing the product lifecycle** are important as outdated hardware and software present significant risks to organizations. Hackers and other malicious actors can exploit unreparied holes in thesecurity of obsolete technology and expose networks to attack.

### 6. Implement specific, high-value security controls

While nonprofit organizations move towards strengthening their digital security strategies, Microsoft recommends that nonprofits implement a subset of identified security controls as soon as practicable.

- **Create backups of all data regularly** to reduce the risk of data loss after a natural disaster or cyberattack. In addition, organizations should ensure that staff know how to use backups to resume business operations.
- **Update software and hardware regularly** to manage the product lifecycle of hardware and software.

  **SPECIFICALLY:**

  - Ensure hardware is included in a procurement cycle that includes the regular retirement and replacement of old hardware.
  - Update software regularly and replace any that is no longer supported by the technology company that created it. If software is not set to update automatically, make sure the updated are actively managed by IT staff or the agency's IT provider.
  - Monitor devices connected to the network to ensure they are running the most up-to-date software.
- **Implement multifactor authentication** to provide greater security when users are accessing the organization's network. Multifactor authentication uses additional factors beyond a password to verify a user's identity when accessing a network[14] and can help keep a network secure even if a user's password has been compromised.
- **Use virtual private networks for remote access** to provide greater security when users are accessing the organization's network remotely. Virtual private networks (VPNs) allow for encrypted communications and afford users secure access to network resources even when they are not physically connected to the organization's on-premises network.
- **Enable endpoint protection** to provide greater protection to the organization's devices. Endpoint protection can monitor users' devices to help identify threats—such as phishing links—and block them so that the network is not exposed. In addition, endpoint protection can scan the system regularly and automatically identify and remove malware, which protects the network from further infection.
- **Monitor devices** to provide additional protection to the organization's devices. Implementing enterprise data protection to register and actively monitor all devices that access the network provides confirmation that all equipment adheres to organizational IT policies. In addition, it allows the organization to remotely encrypt or wipe a lost or stolen device.
- **Restrict usage of personal mobile devices** to reduce the number of devices an attacker could attempt to exploit to gain access to the organization's network. Specifically, organizations should allow mobile access only to specific applications on a network that employees need to do their jobs.

[14] Some examples of multifactor authentication include use of a cryptographic token, using a staff member's ID card to create an online ID, or even biometric verification such as fingerprint and iris scans.

### Leverage nonprofit It initiatives and forums

In addition to improving internal cybersecurity practices, nonprofits can also leverage the experience of others to bolster their cybersecurity awareness. There are many groups around the world whose express purpose is to help nonprofits navigate the world of IT management. They offer many resources, such as staff training, that may be especially helpful to small or mid-sized nonprofits that have no or few dedicated IT staff. These groups are valuable platforms for learning best practices, discussing cybersecurity with other nonprofits, and sharing information about cyber threats, cyberattacks, and vulnerable information.

## CYBERSECURITY RESOURCE LIST

| | | |
|---|---|---|
| *Strategies to Mitigate Cybersecurity Incidents,* Australian Department of Defense | Gives guidance on the top four strategies to prevent over 85 percent of intrusions. A helpful list of activities to undertake. | http://www.asd.gov.au/infosec/mitigationstrategies.htm |
| ISO/IEC 27001 | ISO Information Security Management Guidance. | http://www/iso.org/iso.iso27001 |
| Innovation Value Institute | Provides assessments and trainings for professinal IT staff to develop their critical IT capabilities. | https://ivi.ie/ |
| *Protect your business against cyber threats, UK Government Cyber Essentials* | A simple cybersecurity self-assessment tool for smaller businesses developed by the government of the United Kingdom. | https://www.cyberware.gov.uk/cyberessentials/ |
| The NIST *Framework for Protecting Critical Infrastructure Cybersecurity* | An authoritative resource that can help with making risk-based security decisions. | https://www.nist.gov/cyberframework |
| *Assessing the Security of Your Cardholder Data,* PCI Security Standards Council | An online tool for a business to self-validate their security for card holder data. | https://www.pcisecuritystandards.org/pci_security/completing_self_assessment |
| *The HIPAA Security Rule* | U.S. Department of Health and Human Services' resources on the HIPAA Security Rule. | https://www.hhs.gov/hipaa/for-professionals/security/index.html |

# Privacy



Nonprofits, like their for-profit counterparts, collect and use personal data for a wide array of purposes, from employee and donor management to the administration of services[15]. As a result, just like for-profits, nonprofits also bear legal and ethical responsibility for the handling and protection of this data.

However, many nonprofits are unaware of this responsibility, de-prioritize it, or believe they lack the resources to comply with the complex and nuanced requirements of applicable data privacy rules. This challenge is made even more acute by the proliferation of data protection laws around the globe in recent years, and the strengthening of such laws in jurisdictions such as Europe. But ignoring data privacy obligations poses real risks. Many privacy regulators, tasked with the objective of protecting the privacy of their constituents, are keen to ensure that no organization—even one with charitable aims—is above the law.

Nonprofits can mitigate this risk with a few basic steps. This includes determining when and for what purposes they collect and store personal data; identifying applicable data protection laws and assessing their requirements; and adopting appropriate policies, procedures, and organizational safeguards for data. Cloud computing and other technical solutions can often help to facilitate these processes.

Due to their lack of awareness, nonprofits are particularly exposed to enforcement risk for breaching data protection laws.

To take just one example, between December 2016 and April 2017, the UK's privacy regulator publicly "named and shamed" and **fined,** eleven large charities for failing to comply with UK privacy rules regarding the usage of donor information[16].

## TACKLE THE FIRST CHALLENGE: AWARENESS

One of the most significant challenges posed to nonprofits by data protection law is simply a lack of awareness. Studies over the years have consistently shown that most nonprofits lack sufficient awareness of data protection obligations and risks of non-compliance, and that their knowledge of how to properly manage personal data falls significantly behind that of their for-profit counterparts.

In a NetHope-sponsored study that assessed awareness across a range of different organizations, the ten nonprofits in the survey received the lowest maturity score for data protection activities, such as data retention and destruction[17]. The survey results show that even large nonprofits face challenges in understanding and complying with applicable data privacy rules. This is not a new phenomenon: in 2011, the Data Protection Commissioner of Ireland, writing in specialized guidance, noted that its survey of charitable and voluntary sector organizations also recorded a "worrying lack of knowledge or awareness of data protection principles."[18]

### A MORE RECENT MICROSOFT SURVEY OF FIFTY NONPROFITS REINFORCES THIS CONCLUSION:

- **62 percent** of respondents reported they did not have, or were unaware of, policies that clearly identify personal data (whether of staff, beneficiaries, or donors) among the other data the nonprofit collects.
- **64 percent** of respondents also reported that they either did not have, or were unaware of, educating beneficiaries or donors on how their data was used and stored.

[15] Although jurisdictions vary in how they define *personal information*, the term generally refers to oinformation or data relating to an "identified or identifiable natural person".

[16] Information Connissioner's Office, "ICO Fines Eleven More Charities", April 2017, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/04/ico-fines-eleven-more-charities/.

[17] John Ghent. "Data Protection (DP) Checkpoint Benchmark Report". Innovation Value Institute and Sytorus Data Protection Specialist. November 2016.

[18] Office of the Data Protection Commissioner of Ireland, "Data Protection in the Charity & Volunteer Sector", April 2011, *available at:* https://www.dataprotection.ie/documents/guidance/Charity_Guidance.pdf.

## MAP THE LEGAL LANDSCAPE

The first step, therefore, for nonprofits is to educate themselves on the data protection laws that apply to them, and the obligations that these laws impose.

For many nonprofits, however, this is easier said than done. Laws governing the use of personal data have proliferated globally in recent years. Such laws —which can apply even to organizations based abroad—tend to either be specific (regulating either certain industries or certain types of information, such as health data or electronic communications) or comprehensive.

Although both types of laws can affect nonprofits, comprehensive data protection laws often pose the biggest challenges to nonprofits, given their broad reach and complexity. Dozens of jurisdictions have adopted comprehensive data protection laws—including Canada, Brazil, Japan, Australia, Russia, the EU, and many others—and tracking and applying them can be a headache even for data protection specialists.

However, compliance is important. These laws frequently include strict requirements and are aggressively enforced, which can affect nonprofits even if they do not actively operate in the relevant jurisdictions.

Fortunately, there are ways to quickly build an understanding of these laws within organizations such as nonprofits. Many of these laws have a single foundation upon which they were modelled, the EU Data Protection Directive, and for this reason (and because the EU Directive can apply extraterritorially in certain circumstances), nonprofits operating internationally often pay special attention to the European Union's data protection regime.

## CONSIDER EU DATA PROTECTION PRINCIPLES

The European Union is currently reforming its data protection regime. The Data Protection Directive will be replaced in May 2018 by the General Data Protection Regulation (GDPR), a stricter and even more comprehensive law. The GDPR introduces a host of new obligations with which entities will need to familiarize themselves. But while there will be a range of new and prescriptive obligations, many of the fundamental principles that underpin the regime will not change. Nonprofits should inform themselves about these principles, as they will be responsible for compliance with them if EU or other similar regimes apply to them or their activities.

In the United States, there is no comprehensive data protection law. Instead, the United States maintains a patchwork of sector-specific laws such as:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Children's Online Privacy Act (COPPA)
- The Electronic Communications Privacy Act (ECPA)

State laws, such as California's Shine the Light law, or state data breach laws, may impose additional obligations on organizations that handle personal data.

Broadly, the EU data protection regime requires that organizations, including nonprofits, that collect or handle personal data (including names, email addresses, etc., but also any other information that makes identifiable a living person, including potentially electronic identifiers like IP addresses) observe the following principles, whether they are collecting, using, storing, sharing, or even deleting personal data or information:

- Transparency, fairness and lawfulness, in the handling and use of personal data. Nonprofits will need to be clear with individuals—be they donors, employees, or others—about how they are using their personal data, and will also need a lawful basis to process that data.
- Limiting the processing of personal data to specified, explicit and legitimate purposes. Nonprofits will not be able to re-use or disclose personal data for purposes that are not compatible with the purpose for which data was originally collected. Minimizing the collection and storage of personal data to that which is adequate and relevant for the intended purpose. Nonprofits will need to take steps to minimize data processing, by ensuring it processes data only as necessary.
- Minimizing the collection and storage of personal data to that which is adequate and relevant for the intended purpose. Nonprofits will need to take steps to minimizedata processing, by ensuring it processes data only as necessary.
- Ensuring the accuracy of personal data and enabling it to be erased or rectified. Nonprofits will need to take steps to ensure that the personal data it holds is accurate, and can be rectified where it is not.
- Limiting the storage of personal data. Nonprofits will need to ensure that it retains personal data only for if necessary to achieve the purposes for which it was collected, unless data is anonymized.[19]
- Ensuring security, integrity, and confidentiality of personal data. Nonprofits must take steps to keep personal data secure through technical and organizational security measures. A failure to observe this principle is the largest single source of fines under many data protection regimes.

The EU data protection regime—and some others around the globe—also require affected organizations to avoid transfers of personal data across certain international borders, to prevent circumvention of their requirements, except under specific circumstances set out in the relevant laws. Thus, even where a nonprofit has only minimal contacts with Europe, it may nevertheless have significant compliance obligations with respect to any personal data it holds on European citizens.

Nonprofits should also be aware that comprehensive style data protection laws also provide various rights for individuals that may require responses by organizations. For example, the Data Protection Directive and GDPR provide for a right for individuals to request that organizations disclose to them all personal data relating to them (the "data subject access right"), and in some cases to delete such information on request.

[19]This term is strictly interpreted by many regulators to mean that data can no longer be used to identify or make identifiable a living person—even if combined with other data or sources of information.

## ACHIEVE COMPLIANCE

Once a nonprofit has identified where and how it collects and stores personal data, and informed itself about the data privacy rules that may apply, the next step is to adopt internal policies and procedures to bring the organization into compliance. The steps below are intended to help nonprofits do so. These steps have been drawn from Microsoft guidance as well as advice issued by the Office of the Privacy Commissioner of Canada,[20] the Data Protection Commissioner of Ireland,[21] and the UK Information Commissioner's Office.[22] Although these steps do not cover the full breadth of EU (Data Protection Directive or GDPR) requirements, they provide a starting point. Smaller and medium-sized nonprofits should consult with privacy experts to help develop policies and design and implement procedures; larger organizations may require full-time staff to ensure compliance.

1. **Inventory personal data.** Nonprofits need to clearly identify what personal data they collect and store—including, for example, identifying names, email addresses, social media posts, and bank details held by the nonprofit—and in what databases such data is held. Nonprofits should then inventory how the data was collected, review how it is being used (and the purposes for which the data is being collected and used), shared (including where data is being shared or transferred across international borders), stored, and determine which data the organization no longer needs. As programs change, information is updated, regulations change, and new programs are implemented, this inventory should be regularly reviewed.

2. **Create an internal privacy policy.** The second step requires senior managers and decision makers to create or update the organization's internal data privacy policy as part of its overall digital strategy. This step should normally be undertaken together with legal advice (e.g., to determine the legal basis on which data is processed, if applicable laws require such a basis). The purpose of such a policy is to ensure that the nonprofit's handling of data is consistent internally and in line with legal requirements. Such policies often include security addendums or exhibits that set out specific safeguards, such as encryption or password protection, that must be used in relation to certain types of data. More advanced versions of these policies may also include procedures relevant to the design of new services or functions (i.e., "privacy by design" processes).

3. **Appoint an owner of data protection and privacy issues.** The organization should appoint a single person with responsibility to design, implement, and manage the data privacy program, including all procedures, training, monitoring, auditing, documenting, evaluating, and follow up. This person—who may even be a specialized "data protection officer" for larger organization— should fulfill these responsibilities in a coordinating role, involving board members, managers, IT staff, and other decision makers. This person should also be responsible for reporting data breaches to the authorities where the organization is legally required to do so.

[20] "Getting Accountablility Right with a Privacy Management Program", Office of the Privacy Commissioner of Canada, Ottawa, April 2012, *available at:* https://iapp.org/media/pdf/knowledge_center/Canada-Getting_Accountability_Right%28Apr2012%29.pdf

[21] "The GDPR and You: General Data Protection Regulation Preparing for 2018", Data Protection Commissioner of Ireland, *available at:* https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf

[22] "Preparing for the General Data Protection Regulation (GDPR)", Information Commissioner's Office, London, 14 March 2016, *available at:* https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

4. **Set up reporting systems.** In today's environment, nonprofits, like other organizations, need to quickly identify violations of their policies, such as unauthorized uses and access to personal data and be prepared to respond appropriately. Designing and implementing systems to detect these incidents and report them is critical to an organization's success. Stakeholders should be trained on these systems, review the reports often and regularly, and be prepared to act appropriately.
5. **Conduct privacy reviews.** Nonprofits should also set up processes to evaluate the impact new projects or initiatives have on the privacy of individuals. This evaluation will enable organizations to identify privacy issues before they arise and develop ways to mitigate risks.
6. **Communicate how personal data is handled.** Nonprofits should take steps to inform staff, donors, beneficiaries, and any others on whom they hold personal data, how this data will be stored, processed, and shared. This often takes the form of a public facing document, such as a privacy statement or policy, on the organization's website And, it may also include disclosures made to individuals through bespoke notices or contextual information, such as pop ups or text on the screen, provided before information is collected. Such policies identify, among other things, the types of data being collected, the purpose for which the organization is using the data, the entities or categories of entities with whom data may be shared, whether data is transferred internationally, the right that individuals have in relation to the data processing, and so on.
7. **Develop procedures that enable individuals to exercise their rights.** To comply with EU and other data protection rules, nonprofits will also need to develop procedures to respond to individuals who seek to exercise their data protection rights. For example, under the GDPR, an individual has the right to demand an organization holding her personal that such data is erased, corrected, restricted and/or ported to another service provider.
8. **Develop additional compliance mechanisms as necessary.** Depending on the types of personal data collected and how such data is used, a nonprofit may need to develop additional compliance processes and procedures. Special mechanisms may be needed for the collection of certain types of personal data, such as health data or kids' data, and for usage of personal data, such as determining an individual's credit worthiness.

[21] "The GDPR and You: General Data Protection Regulation Preparing for 2018", Data Protection Commissioner of Ireland, *available at:* https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf

[22] "Preparing for the General Data Protection Regulation (GDPR)", Information Commissioner's Office, London, 14 March 2016, *available at:* https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

## PRIVACY RESOURCE LIST

| | | |
|---|---|---|
| ***Getting Accountability Right with a Privacy Management Program.*** **Canada Office of the Privacy Commissioner of Canada** | Provides steps and recommendations on how businesses should build appropriate privacy policies. | https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/gl_acc_201204/ |
| **The European Commission's website on the protection of personal data** | Understand EU data protection law, individuals' rights, and obligations for those collecting and processing personal data in the EU. | http://ec.europa.eu/justice/data-protection/index_en.htm |
| **ISO 27018** | Code of practice for the protection of personal data where cloud service providers act as data processors. | http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498 |
| ***The GDPR and You,*** **Ireland Data Protection Commissioner** | Steps for businesses to take for the upcoming GDPR implementation. | https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf |
| ***Preparing for the General Data Protection Regulation,*** **UK Information Commissioner's Office** | Guidance to UK businesses on steps to take now regarding the upcoming GDPR. | https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf |
| **Transforming Government Cloud Policy framework for innovation, security, and resilience** | Microsoft document explaining why governments should engage a cloud-based model and the key principles to follow for such a deployment. | http://download.microsoft.com/download/7/2/F/72F-8CD03-D809-42B4-B6963E76E8FAC6FA/cloudsecurityprinciples.pdf |
| **Protecting Data and Privacy in the Cloud** | Microsoft explanation on how to use the cloud to better protectdata and privacy. | http://download.microsoft.com/download/2/0/A/20A1529E-65CB-4266-8651-1B57B0E42DAA/Protecting-Data-and-Privacy-in-the-Cloud.pdf |

# How the cloud can help



The sections above make clear the challenges nonprofits face in developing and implementing effective cybersecurity and data protection compliance. There are no magic solutions—nonprofits, like other organizations, need to invest the time and resources necessary to address these challenges. However, in many cases, cloud computing can help.

Although the term cloud computing can have different meanings in different contexts, for present purposes it refers to technologies that use the Internet as a platform to give users nearly ubiquitous access to highly scalable, flexible, and powerful computing resources through online services that are hosted in off site datacenters. Anyone who has used a search engine, online email service, or social network has already experienced a consumer version of cloud computing. Today, however, enterprises of all sizes are rapidly moving their own IT systems "to the cloud" and thereby making their operations more effective and efficient.

Cloud computing can help nonprofits achieve their cybersecurity and privacy goals in many ways.

- **Focusing resources.** First—and importantly, for many nonprofits—by allowing organizations to pay only for the computing resources they need, when they need it, cloud computing can help nonprofits save money, enabling them to invest more of their time and resources on their core missions.
- **Simplifying governance.** Because applications and services are hosted on datacenters that are operated and maintained by the cloud service provider, cloud computing reduces the burden on nonprofits to install, maintain, and update hardware and software. This reduces the complexity of systems and enables more informed, comprehensive governance. For example, by placing multiple databases within a single integrated system, and by enabling easy cataloging and identification of relevant locations of data, cloud computing can help nonprofits maintain better visibility and control over the types of data they collect and how it is handled.
- **Cloud security.** Perhaps most significantly, the cloud also delivers an immediate step change in security for nonprofits, without a large upfront investment. This is valuable for both cybersecurity and data protection compliance. Indeed, a key requirement of most comprehensive data protection laws, including the EU Data Protection Directive and the GDPR, is that organizations handling personal data must take technical and organizational steps to ensure the security of any personal data they collect or process. This requires implementation of systems and safeguards that adequately protect data from, among other things, malicious access or disclosure.

Deployment of robust security solutions is not always easy for nonprofits: They often lack the resources or know-how to implement full on premises security systems. In these cases, cloud solutions can deliver a major boost to nonprofit data security with a minimum of know-how, time investment, and cost. To take just a few examples, cloud systems often feature:

- End-to-end encryption, both internally, and in transmissions between the customer and cloud center;
- State-of-the-art physical security of data centers, including 24-hour surveillance, physical access controls, and multiple layers of perimeter protection; and
- Compliance with international security and data protection standards like ISO 27001 and ISO 27013.

These features can provide a much more robust cybersecurity infrastructure than many nonprofits could establish in on premises infrastructure.

# Using the cloud



Of course, there is no one-size-fits-all solution for the ways in which nonprofits should use cloud services. Identifying which cloud model is most appropriate depends on a nonprofit's needs, their data protection requirements, and the type of processing they require. Some nonprofits may be able to use "off-the-shelf" solutions for enterprises; others may need to take account of unique local legal requirements and internal procedures (for example, concerning medical or health information).

For that reason, nonprofits will have different approaches for cloud based solutions and the cloud can cater to that diversity. Cloud environments can be public, private, or hybrid, and the benefits vary with each model. For instance, the actual costs of public cloud services tend to be quite low because the cloud provider's physical and virtual computing resources are pooled and then assigned and reassigned to serve multiple consumers, thus allowing the provider and its customers to benefit from economies of scale. Customers sharing distributed resources achieve a lower variable cost than they could access on their own. A private cloud shares many of the characteristics of public cloud computing, including self-service, elasticity, and pay-by-use, in addition to dedicated resources that provide additional control and customization. Because private clouds are limited to only a small pool of customers their costs tend to be higher. The hybrid cloud combines positive elements of both public and private clouds, allowing customers to move data and applications seamlessly between public clouds, private clouds, and their on premises systems.

Deciding on the best model of cloud computing for an organization is not always easy. The right internal stakeholders need to be involved for any cloud-based solution development—the organization's IT department, of course, but also legal, procurement, finance, and other key business units. Microsoft offers a Cloud Service Due Diligence Checklist[23] for organizations to aid them in more clearly identifying their own performance, service, data management, and governance objectives and requirements. Once completed, the Checklist can be used to compare offerings from multiple service providers. It can also help provide nonprofits with better understanding of how a cloud-based solution would work for their operations.

Most nonprofits are already familiar with cloud services: 42 out of 50 survey respondents indicated that their organization already uses cloud-based tools. However, the gaps identified in cybersecurity and privacy awareness suggest that nonprofits would benefit from a more holistic understanding of how the cloud can help contribute to security and data protection compliance solutions. For those with the resources, many professional consulting companies offer discounted services for nonprofit organizations.

Understandably, many smaller nonprofits will have limited internal capacity not only to undertake the rigorous self-assessments that are required, but also to implement solutions identified. As a first step, they may wish to consult with nonprofit IT forums and entities that specialize in providing IT support to nonprofits. These sources often can help develop security and privacy compliance policies suited to the nonprofit's own needs, and can offer insight into how cloud-based tools and services can help nonprofits meet these requirements.

[23] Microsoft Could Service Due Diligence Checklist: https://www.microsoft.com/en-us/trustcenter/Compliance/Due-Diligence-Checklist

# Summary

Nonprofits have a responsibility to their beneficiaries, staff, and donors to create secure, resilient, and accessible IT platforms on which they conduct their activities. In addition, increasing legal requirements demand a secure environment that respects staff's and beneficiaries' right to privacy. Many government and private donors have already started mandating minimum standards for nonprofits in cybersecurity and data protection; they may cease funding agencies that fail to meet their standards.

An overhaul of a nonprofits' cybersecurity and data protection strategies (or creating one from scratch) may seem like an overwhelming task. But the steps outlined in this paper above are the right place to start.

Building an effective strategy is not something nonprofits can do alone. Importantly, donors and grant makers need to understand the digital infrastructure that the modern nonprofit needs to meet today's demands. Any organization operating on hardware and software developed many years or even decades ago will likely not have the capacity to respond effectively to their beneficiaries in a safe and secure manner. Although donors understandably are often not enthusiastic about nonprofits investing in large operational overheads, they need to understand that limits on this portion of the budget can hobble nonprofits that operate in today's digital-first world. Restricting resources to implement modern systems ready to cope with transformation and disruption may result in security breaches, interrupted services, and costly consequences.

Donors and the private sector must support nonprofits beyond just immediate program implementation and should provide support for developing cybersecurity and data privacy best practices.

"**Cybersecurity and data protection** is one of the most pressing issues not just for the CIO, but for executive teams and organizations boards. The problem is many have not realized that yet. We welcome any and all input in this space."

– Microsoft survey feedback

The risks associated with the digitization of the world are increasing as fast as today's technological transformations. Nonprofits have the capacity to become more efficient and responsive to their stakeholders by deploying modern, resilient technology solutions. Those that neglect to do so run the risk of not only failing their own staff and donors but exposing those they are meant to serve to even more risks. Organizations that successfully modernize their cybersecurity and data protection practices will not only become more efficient and cost-effective; they will gain the trust of donors and beneficiaries—and be better positioned to fulfill their mission.

Learn about nonprofit offers from Microsoft: microsoft.com/nonprofit