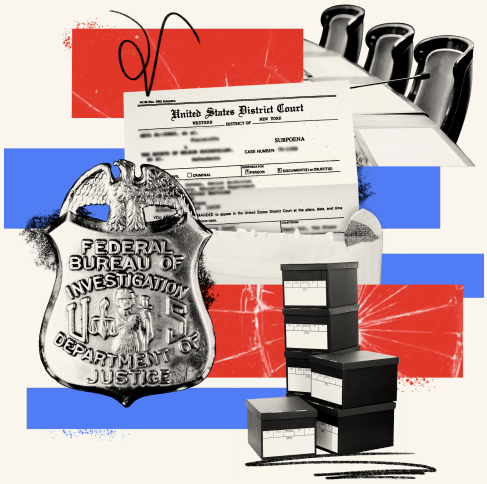
What if ... your organization receives a demand to disclose sensitive data?



OCTOBER 2025

Understanding data demands 1

Preparing for data demands 4

Responding to data demands 8

Protect Democracy

Understanding data demands

Background

Many nonprofit organizations routinely collect sensitive data. This may include sensitive personally identifiable information such as legal names, dates of birth or social security numbers; contact information including phone numbers or home addresses; demographic information; or information about marriages, employment, health information, household income, and more. Sharing sensitive data entrusted to an organization can be a serious breach of trust, as well as a breach of legal obligations.

Sometimes, an organization may receive a demand for sensitive data from a government actor, including in the course of a government investigation. This primer covers best practices for preparing and responding to data demands from the government in a way that takes seriously the duty of care an organization may owe to others.

What is a "data demand"?

A data demand is a request or order from the government that an organization provide certain information. Federal, state, and local government entities can initiate data demands.

Often, but not always, a data demand may take the form of a warrant, subpoena, civil investigative demand (CID), or regulatory or administrative summons. These formal, written demands compel testimony, documents, or other material to be turned over to the government. For example, the Texas Attorney General issued a civil investigative demand in 2024 for internal records and communications from the LGBTQ+ group PFLAG concerning its work with transgender adolescents in Texas.

Data demands may also come in the form of informal letter requests, or even verbal requests from government agencies or officials.

What laws govern *government* requests for sensitive data?

Unless it is clearly identified in the data demand itself, organizations should ask the government to identify the source of its legal authority to make the request. And even legally authorized government data demands must comply with applicable privacy laws that govern attempts to access sensitive data held by private entities, including nonprofits.

Organizations should inform legal counsel as soon as possible if they receive a data demand from a government entity. Legal counsel can then help determine whether the claimed authority is adequate and whether or not the government complied with applicable legal obligations before making the data demand. For example, if an organization determines that a data demand by the federal government is subject to the Paperwork Reduction Act, legal counsel may help

determine whether the government has complied with applicable obligations to provide public notice and an opportunity for public comment.

If the government has not identified adequate legal authority or satisfied its legal obligations, organizations can work with legal counsel to respond appropriately, such as by requesting further information or objecting to the data demand.

Federal laws that apply to the federal government's access to sensitive data are summarized in the table below. States may have additional laws that govern state or local requests for sensitive data. Recipients of demands from state or local government entities should consult with legal counsel to determine what state laws may apply.

The Privacy Act of 1974	The Privacy Act requires federal agencies initiating a new data collection to publish a public "system of records" notice in the Federal Register identifying the purpose for which information about an individual is collected, from whom, what type of information is collected, and how that information will be shared with other agencies. *See*: 5 U.S.C. 552a, DOJ Overview of the Privacy Act, October 2022.
The Paperwork Reduction Act of 1980	Under the Paperwork Reduction Act, federal agencies must conduct an independent review of any proposed collection of information and seek public comment on the proposed collection by publishing a 60-day notice in the Federal Register. *See* 44 U.S.C. 3501 et seq., OPM Paperwork Reduction Act (PRA) Guide, April 2011.
The E-Government Act of 2002	The E-Government Act of 2002 requires federal agencies to conduct a Privacy Impact Assessment (PIA) prior to initiating a new collection of information, which includes detailing what information will be collected, why it is being collected, and how the information will be collected, used, shared, and secured. *See* Public Law 107-347, section 208, codified at U.S.C. 3501 note, DOJ Overview of the E-Government Act, February 2019.
Stored Communications Act	The Stored Communications Act (SCA) establishes a legal framework limiting how state and federal governments can access stored electronic communications. *See* 18 U.S.C. 2703.

Constitutional Right to Privacy	Both state and federal data demands are subject to privacy protections in the U.S. Constitution, including the individual right to privacy under the Fourth Amendment. Even where an individual discloses private information to a third party, that information may still be constitutionally protected from the federal government in some circumstances. *See* *Carpenter v. United States*, 585 U.S. 296 (2018).

What laws govern when and how *recipients* of government demands produce sensitive data?

Recipients of data demands must also comply with legal requirements when they produce data to government actors. Federal law restricts the dissemination of various types of sensitive data, including:

- **Health information.** The Health Insurance Portability and Accountability Act (HIPAA) safeguards protected health information by setting national standards for the privacy and security of this data, and by limiting its use and disclosure without a patient's authorization. *See* 45 C.F.R. Parts 160 and 164, HHS Summary of the HIPAA Privacy Rule.
- **Student education information.** The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records by restricting the circumstances in which schools may disclose personally identifiable information from a student's education record without consent. *See* 20 U.S.C. 1232g.
- **Children's information**. The Children's Online Privacy Protection Act (COPPA) protects the personal information of children under 13 collected online by limiting the circumstances in which website operators and providers of online services may disclose such information, including data such as a child's name, address, email address, and photos. *See* 15 U.S.C. 6501–05.

In addition, many states have enacted their own comprehensive data privacy and consumer protection laws, which may give individuals the right to know what personal information is being shared by private entities or to opt out of that sharing.

Importantly, **receiving a government data demand does not negate an organization's legal obligation to comply with data protection laws**. While some of these laws may contain exceptions allowing data to be shared with the government in some circumstances, organizations should consult with legal counsel to ensure that sharing data in response to a government data demand does not itself violate any laws.

Preparing for data demands: best practices

Any time an organization is sharing data there are accompanying risks, especially in terms of data privacy and security. The following offers practices and processes to help organizations proactively manage the risks that can be associated with data demands.

Planning ahead

Planning ahead can help mitigate risks for an organization, and the people and communities it serves, in the event of a government data demand. Organizations should have a 'playbook' written in advance to be used in the event of a data demand. If an organization has in-house legal counsel, it should consult with them to develop a plan for the possibility of a government demand for sensitive data. If it does not have in-house counsel, it should seek legal advice from outside counsel for the same purpose.

Part of this playbook may include designating specific staff to handle a request for data. This should include an organization's IT supervisors and technology experts who are equipped to handle information stored in computers, servers, handheld devices, etc. Alongside legal counsel and technology experts, organizations should also plan for how to involve senior leadership, third-party vendors who handle or store the requested data, and internal experts on communications and government affairs. Organizations should also consider whether and how they will alert clients whose personal data is impacted.

This playbook should also cover basic operational questions about the receipt of the demand and how to handle it, such as:

- **How will staff be trained to respond to a data demand?** If a request is received by more junior staff, who should they alert?
- **What parts of the organization need to be involved in the response?** Typically, this will include legal counsel, leadership, and staff responsible for IT and cybersecurity. Organizations may also want to consider tapping communications and government affairs experts in their response plan.
- **Are there external parties to alert?** These may include third-party vendors who also handle or store an organization's sensitive data and clients whose personal data may be impacted. Depending on context, local or national media may also merit consideration. Additionally, if groups have insurance, they should consider contacting their broker to inquire about applicable coverage and how to proceed with notifying their carrier.

Answering these questions in advance can help organizations better manage and respond to data demands.

Getting a lawyer

Consulting with legal counsel before responding to a data demand is critical. Legal counsel can help evaluate an organization's options in a privileged and confidential way, including determining what data sought may be protected from disclosure. Counsel can and should help craft an organization's response to a data demand. Additionally, many rules governing data demands vary depending on the type of information sought and whether a state or federal government entity is issuing the demand. Legal counsel can help organizations navigate these specific rules.

If an organization has in-house counsel, that should be the first call. If not, organizations should have a list of outside lawyers ready ahead of time so they can reach someone quickly.

Establishing and maintaining consistent data security policies

Clear, consistent written policies minimizing the collection, handling, and retention of data are one of the best ways to mitigate risks associated with a data demand. Effective data security policies also may help shield organizations from cyberattacks.

Data minimization

While organizations may be bound by law, grant agreements, or the type of services they provide to collect some forms of sensitive data, collecting or retaining unnecessary data may lead to overcompliance with data demands. Simply put, organizations cannot turn over data that they do not possess.

Practicing data minimization by collecting and retaining only the minimum amount of data necessary can better prepare organizations for data demands as well as help protect against the risks of hacking or ransomware attacks. For example, it may not be necessary to collect data on an individual's citizenship or immigration status, and even if it is, it may not be necessary to distinguish between subcategories like naturalized and natural-born citizens. Likewise, age, or an age range, may in some circumstances suffice instead of date of birth.

Data retention

Crafting and maintaining a **data retention policy** that specifies how long data is kept before routine deletion is another way to reduce risk. Some types of data, such as medical or legal records, may be subject to legally required minimum retention periods, which can vary from state to state. But communications with individuals receiving services or case files for past recipients, for example, may not need to be retained indefinitely; if they do, they can be specifically flagged to avoid automatic deletion.

Conducting regular audits can catch and fill gaps in a response plan

Data or cybersecurity audits can assess the effectiveness and implementation of these policies as well as other relevant organizational practices. Audits may raise pertinent questions about data governance for organizations, such as: Is sensitive data encrypted, and should it be? Similarly, should an organization store sensitive data separately? Is sensitive data stored solely on organizational devices or do staff use personal devices to handle sensitive data in their professional capacity? What third parties might need or have access to sensitive data (e.g., technology vendors or other suppliers)? What steps has an organization taken to secure data from external breaches?

Audits should also consider risks from third-party data-sharing, storage, or processing agreements. Vendor contracts, for example, may include clauses about how legal demands for data will be handled.

Below are various data security and cyber-audit tools to assist organizations in establishing and maintaining effective data policies:

- For organizations or individuals seeking step-by-step support and resources for a variety of needs ranging from secure communications to anti-phishing, consider AccessNow's Digital Security Helpline, the Ford Foundation's Cybersecurity Academy Courses, and ACT's Simplified Cybersecurity Protection Tools.
- For organizations drafting a cybersecurity policy or assessing their cybersecurity risks, consider the Ford Foundation's Cybersecurity Assessment Tool or NTEN's Tech Accelerate tool.
- For organizations that handle large amounts of data and need help thinking about organizational approaches for handling it responsibly, consider NetHope's Data Governance Toolkit.
- For organizations that have completed an audit of their cybersecurity and data management practices and have an understanding of their remaining needs, Techsoup's Security Products for Nonprofits offers a range of security tools with discounts for nonprofits.

Thinking ahead about communications and escalation

Establishing clear internal and external communications policies will reduce the risk of miscommunication and ensure consistency around an organization's response to a data demand. When crafting this plan, organizations should seek the advice of legal counsel on whether and how to communicate with government actors, the media, and other partners. Key considerations for a communications plan include:

- How will message consistency be maintained?
- Will one person or team manage external correspondence?
- How will other relevant staff, teams, or partners provide input?
- What are the risks and benefits of communicating publicly about the data demand?
- What are the risks and benefits of communicating privately with partners or similar organizations?

Responding to data demands

In the event an organization receives a data demand from the government, there are several factors that may affect how the organization responds, including the type of demand and what data it requests.

A subpoena, for instance, will typically include a list of the demanded material and a date by which the recipient must deliver it—but the exact details of compliance are often a matter of interpretation and negotiation. Organizations should think carefully about what they provide and how. If organizations want to learn more about responding to subpoenas, Protect Democracy has a separate guide here.

If the demand takes the form of an informal request from a government agency, compliance may not be mandatory. Organizations should share such a demand with legal counsel as they weigh the risks of possible responses. Legal counsel should ensure that the government has a legal basis for issuing the demand and has complied with relevant legal obligations. For example, the Privacy Act requires that the federal government must generally publish a system of records notice in the Federal Register before initiating a new collection of data. Data demands that have not complied with this requirement may not be lawfully authorized. Legal counsel can help organizations determine whether sharing the data is permitted under federal or state law and not, for example, restricted by privacy laws such as HIPAA or FERPA.

As with a subpoena, if an organization intends to turn over sensitive data in response to an informal data demand it should work with counsel and other stakeholders to identify areas for negotiation or clarification with the government. Especially for large or onerous demands, there may be ways to simplify compliance or avoid providing some forms of data that are more sensitive.

Protect Democracy is a nonpartisan nonprofit organization dedicated to preventing American democracy from declining into a more authoritarian form of government.

protectdemocracy.org