



SAMPLE DATA COLLECTION POLICY AND WHY YOU NEED ONE

It's not a secret that we participate in a surveillance economy, but it may be worse than you think. An FTC [staff report](#) examined large social media and video streaming services' data collection and use practices and concluded these businesses engage in vast surveillance of consumers to monetize their personal information while failing to adequately protect them online.

Why would anyone be surprised? Payroll collects a vast amount of data from employees and is being asked to do a lot more with it. Maybe it's time for a data-collection policy.

QUESTIONS YOUR POLICY MUST ANSWER

Before writing your policy, consider these questions.

- **What personal information do you collect?** List the categories of personal information you collect from employees: their names, Social Security numbers, addresses, email addresses, dates of birth, marital status, salary, retirement and health contributions, bank account numbers, biometric information, etc.
- **Why is the information collected?** Specify the purpose for collecting employees' personal information: to pay them accurately; to comply with wage-and-hour laws and quarterly and annual reporting mandates; to facilitate staffing, salary levels and other decisions made by the C-suite; and to protect against fraud and manipulation of the company's financial accounts.
- **Who has access to the information?** Identify the offices with which you will share payroll data. Internally, these offices include HR, or course, the CFO, the CEO and the CIO. External third parties include the group health plan administrator, FSA administrators, the 401(k) administrator, state child support agencies, the IRS and state tax authorities and attorneys.



- What security measures do you use to protect data collected?** Describe the security measures the payroll department uses to keep employees' personal information safe. Be sure to cover security safeguards the company requires its business partners and vendors to use.

SAMPLE POLICY

Policy Type: Data

Title: Data Collection, Access and Use Policy

Effective Date: [Fill in date]

Responsible Parties for Policy Compliance: [Fill in individuals' titles]

Authority: The payroll department will review its data-collection, access and use policy annually or as needed; when there is a change to a data collection, access or use activity; and upon request by executive committee.

Collection and Use of Information: Personal information used to determine employees' salaries, benefits and privileges must be collected and used only for the purpose for which it is intended. If information comes from a third party, employees' written permission is required.

Information Accuracy: Personal information provided by employees must be accurate and complete. The information in the system must be relevant, necessary and timely.

Standards of Conduct Regarding Personal Information: Payroll has a duty to protect the security of employees' personal information by:

- Ensuring the accuracy, relevance, timeliness and completeness of records.
- Avoiding any unauthorized disclosure, verbal or written, of records.
- Collecting only the information needed to perform an authorized function.



- Collecting information directly from employees, whenever possible.
- Maintaining and using records with care to prevent the inadvertent disclosure of information.
- Safeguarding Information: Paper records are to be placed in secured locations. Electronic systems must use passwords, identity verification, detection of break-in attempts, firewalls, encryption and/or other security measures determined to be appropriate.

Retention and Destruction of Data: Employees' data will be retained for as long as the statute of limitations remains open on any tax or labor issue. Data will be then retained for 10 additional years and will be removed, destroyed or deleted appropriately when the data are no longer relevant.

Disaster, Health or Safety Emergency: [Name of company] may, on a case-by-case basis, disclose, without employees' consent, information to appropriate parties in the event of a disaster or other health or safety emergency.