



Prudent Participant Data Usage Principles

Historically, according to a few courts, participant data may not be a plan asset under the Employee Retirement Income Security Act (ERISA), but it is undeniably an asset.^[i] And increasingly, it's being used like one. Plan fiduciaries are held to a duty of loyalty and prudence to ensure that every decision and every service provider engagement is undertaken in the best interests of participants and beneficiaries. Today, that duty includes the securing and preservation of participant data.

The Government Accountability Office (GAO) was recently asked to review retirement plan data privacy, including how selected retirement plans use and share participant data and how selected service provider policies incorporate leading privacy practices.^[ii] This update explores those findings and how they apply to plan fiduciaries.

Here's What You Really Need to Know:

- GAO recommended that the Department of Labor (DOL) provide additional guidance about participant data privacy for retirement plan sponsors and service providers.
- GAO was asked by members of Congress to examine how data on retirement plan participants is used and shared by service providers, including whether such data is used beyond purposes of plan administration and potentially shared with third parties.^[iii]
- Participants have filed several lawsuits alleging that service providers used their data for targeted marketing and cross-selling other services by the service provider (beyond recordkeeping services).^[iv]
- Some privacy disclosures that GAO reviewed did not consistently incorporate leading privacy practices.

Let's Dive In...

Retirement plans rely on participant data to ensure accurate and efficient plan administration. This includes the personally identifiable information (PII) and financial information that plan sponsors share with service providers including, but not limited to, full legal name, date of birth, address, contribution rate, investment election, hire date, and salary. Plans necessarily share this participant PII with service providers to properly administer benefits. But GAO found that the same data is often used, or permitted to be used, for marketing financial products, and in some cases, sold outright.

The GAO report notes that as of November 24, 2025, 19 states have enacted comprehensive data privacy laws that have already taken effect or that will do so in 2026. In 2018, California was the first state to enact

such legislation, which took effect in January 2020, followed by legislation enacted in Virginia and Colorado in 2021 and which took effect in January 2023 and July 2023, respectively.

Typically, state law wouldn’t matter because ERISA preempts state laws that “relate to” an employee benefit plan. The Supreme Court’s formulation is that a state law relates to an ERISA plan if it has a connection with or reference to such a plan.[v] However, when it comes to the application of state privacy laws, it is a gray area and depends on the specific requirements of the law, such as security breach notices versus retention of data and the ability to opt out of the notice. Service providers must carefully review and understand each of these requirements for states in which they operate.

Going Beyond State Privacy Issues

While ERISA does not include explicit provisions addressing data privacy in retirement plans, it does, however, require that plan fiduciaries use plan assets exclusively to provide plan benefits or to defray certain administrative costs. While some plan participants have argued that participant data should be considered a plan asset under ERISA and that plan service providers that exercise authority and control over the management and disposition of participant data should be subject to ERISA’s fiduciary responsibilities, courts that have ruled on this question have to date rejected this argument.

While some disclosures stated that participants could opt out of having their data shared for marketing (which is required under some state privacy laws), GAO noted that opt-out provisions sometimes varied in what they covered or were not provided at all.

Plan sponsors can, of course, contractually limit service providers from collecting certain types of information or using participant data for marketing. However, research from the Society of Professional Asset Managers and Recordkeepers (SPARK) Institute found that participant data privacy was of greater concern to the larger plan sponsors than the small or mid-sized plan sponsors that participated in the study. [vi] Further, many small or mid-sized plan sponsors, even if concerned about data privacy, often lack the bargaining power to change contractual arrangements with service providers related to the use of participant data and privacy.

Best Practices

The GAO noted that the selected service provider privacy participant disclosures it reviewed did not consistently incorporate leading privacy practices, as reflected in the Fair Information Practice Principles (FIPP). FIPP provides a framework for responsible data handling, emphasizing key privacy protection principles such as transparency in data practices, purpose specification to define intended uses, and restrictions to prevent unauthorized use of personal data.

These FIPP best practices should be considered in disclosures; plan sponsors should use this as a checklist for consideration, and may want to ask for samples during the RFP process:

Principle	Description
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Collection limitation	The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.

Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Why it Matters

This is not just a privacy issue (or cybersecurity issue), but it is a governance issue. Clearer limits on how participant data can be used, along with greater transparency and participant consent, could reduce risks ranging from identity theft to unwanted commercialization of personal information. Absent more definitive guidance, fiduciaries may increasingly need to make their own judgments about where to draw the line when the use of participant data supports participants and when it begins to work against them. Of course, given that there is no federal privacy framework today, nor is privacy part of ERISA, the GAO report notes that frameworks like FIPP could assist service providers in ensuring transparent privacy policies and proper safeguarding of participant information.

The GAO Recommendation

The GAO recognizes that the DOL previously issued cybersecurity guidance in 2021 and 2024.[vii] The GAO report comments that DOL's cybersecurity guidance does not provide examples of acceptable uses of participant data, define what information it considers to be private, or describe the types of situations in which service providers should obtain permission to use or disclose information about participants. It also notes that the guidance does not refer to leading privacy practices as benchmarks for plan sponsors' or service providers' management of participant data.

GAO recommends that DOL issue additional guidance clarifying:

- What participant information should be considered private
- When service providers should obtain permission to use or share that information
- What best practices — including participant choice — should look like in practice

The DOL has not committed to doing so, stating only that it will consider the recommendation as resources permit.

That said, the report referenced the DOL's 2021 cybersecurity guidance states that a prudent fiduciary should make sure that contracts contain "clear provisions on the use and sharing of information" and that the contract "should spell out the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse." [viii]

Action Items for Plan Sponsors:

- Understand applicable state and local data privacy requirements, including where state requirements are preempted by ERISA.
- Review service provider agreements for provisions governing data use and sharing.
- Consider whether non-administrative uses of participant data should be limited or require explicit consent by plan fiduciaries and participants.
- Incorporate recognized privacy frameworks into plan governance and oversight practices, and continue to monitor over time.

[i] *Harmon v. Shell Oil*, No. 3:20-cv-00021 (S.D. Tex. 2020).

[ii] U.S. Government Accountability Office, *Retirement Plans: Department of Labor Guidance Could Mitigate Privacy Risks for Participants*, GAO-26-107271 (Washington, DC: GAO, February 26, 2026), <https://www.gao.gov/products/gao-26-107271>.

[iii] Senator Bernie Sanders (I-VT), Representative Robert Scott (D-VA), Senator Patty Murray (D-WA).

[iv] The GAO report notes that retirement plan participants have filed at least 11 lawsuits from 2009 through 2024 in federal courts that allege that plan sponsors breached their fiduciary duty under ERISA by failing to prevent contracted service providers from using participant data for their own purposes, and subjected participants to unwanted marketing. As of December 2024, seven of these cases had been settled, and five included agreements by the plan sponsor to add contractual language preventing service providers from using participant data for marketing.

[v] *Shaw v. Delta Air Lines, Inc.*, 463 U.S. 85 (1983).

[vi] SPARK Institute and Defined Contribution Institutional Investment Association Retirement Research Center, *SPARK Study: Understanding Data Privacy Sensitivities Across the Defined Contribution Industry* (Simsbury, CT: SPARK Institute, April 2023), https://cdn.ymaws.com/dciia.org/resource/resmgr/rrc_media/projects_2022/DCIIA-RRC-SPARKDataPrivacy_0.pdf.

[vii] U.S. Department of Labor, Employee Benefits Security Administration, "Compliance Assistance Release No. 2024-01: Cybersecurity Guidance Update," September 2024, <https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/compliance-assistance-releases/2024-01>

[viii] U.S. Department of Labor, Employee Benefits Security Administration, *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* (Washington, DC: DOL, April 2021), <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf>.



Christopher D. Cervantes, C(k)P®, CFP®, CIMA®, NQPA®
Founder & Managing Partner
5700 Tennyson Parkway, Suite 250
Plano Texas 75024
214.800.4451
Christopher.Cervantes@valorousadvisors.com
www.valorousadvisors.com