Prudent Participant Data Usage Principles

The Government Accountability Office (GAO) was asked by Congress to review retirement plan data privacy, including how retirement plans use and share 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

Best Practices

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.

- **Purpose specification**
- **Collection limitation**
- **Data quality**
- **Use limitation**
- **Security safeguards**
- **Openness**
- **Individual participation**
- **Accountability**

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.