Fair Information Practice Principles (FIPPs)

History of FIPPs

The Fair Information Practice Principles (FIPPs) are a set of eight internationally accepted privacy principles which have provided the foundation for all privacy regulation during the last 50 years. First gaining momentum in the 1970s, these principles remain the core of privacy regulation today, exemplified by the passage of two new state privacy laws passed in 2021 (i.e., Virginia's Consumer Data Protection Act (CDPA) and the Colorado Privacy Act).

In 1973, the U.S. Department of Health, Education, and Welfare (HEW) published a report on *Records, Computer, and the Rights of Citizens* that discussed the importance of privacy safeguards and introduced the concepts of transparency, accessibility, accountability, and use limitation. Soon after, the Privacy Act of 1974 was built on those same four principles and enacted as one of the earliest federal privacy laws. The FIPPs continue to been heavily referenced, including influencing some of the most impactful contemporary privacy laws, the European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

The Eight Principles

According to the International Association of Privacy Professionals, OECD's FIPPs are the most widely used, yet considered minimum standards. Many federal agencies and private sector companies use these principles as a starting point to build their own organization-specific codes, such as VA's Privacy Principles.

These eight principles drive the core aspects of dozens of privacy laws, both domestically and worldwide.

Number	Principle	Description
1	**Collection Limitation**	There should be limits to the collection of personal data - data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2	**Data Quality**	Personal data should be relevant to the purposes for which it is to be used, and should be accurate, complete and kept up-to-date.
3	**Purpose Specification**	The purposes for which personal data are collected should be specified at the time of data collection and the subsequent use limited to the fulfilment of those purposes.
4	**Use Limitation**	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification principle except: A. with the consent of the data subject; or B. by the authority of law.

The Eight Principles (cont'd)

Number	Principle	Description
5	**Security Safeguards**	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6	**Openness**	There should be a general policy of openness about developments, practices and policies with respect to personal data, such as main purposes of their use and identity of the data controller.
7	**Individual Participation**	An individual should have the right: A. to obtain from a data controller the data the controller has about them. B. to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
8	**Accountability**	A data controller should be accountable for complying with measures which give effect to the principles stated above.