DATA PROTECTION PRINCIPLES

OECD Guidelines

First released in 1980, and then updated in 2013, these guidelines represent perhaps the most widely accepted and circulated set of internationally agreed upon privacy principles along with guidance for countries as they develop regulations surrounding cross-border data flows and law-enforcement access to personal data. (Although the OECD guidelines are not legally binding, **the principles are widely emulated in national privacy laws)**.

PRINCIPLES

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

CONVENTION 108

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108)

The Convention opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field. Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.

PRINCIPLES

Personal data undergoing automatic processing shall be:

- obtained and processed fairly and lawfully;
- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date;
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR replaced the Data Protection Directive in 2018. The aim of the GDPR is to provide one set of data protection rules for all EU member states and the European Economic Area (EEA)

PRINCIPLES

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

DATA PROTECTION PRINCIPLES

Fair Information Practice Principles

The United States Federal Trade Commission's fair information practice principles (FIPPs) are guidelines that represent widely accepted concepts concerning fair information practice in an electronic marketplace.

(1) The Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
(2) The Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
(3) The Purpose Specification Principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
(4) The Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except a) with the consent of the data subject, or b) by the authority of law.
(5) The Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. 71
(6) The Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
(7) The Individual Participation Principle. An individual should have the right:
    a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b) to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him;
    c) to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;
(8) The Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Generally Accepted Privacy Principles (GAPP)

A framework promulgated by the American Institute of Certified Public Accountants (AICPA) in conjunction with the Canadian Institute of Chartered Accountants (CICA).

PRINCIPLES

The ten principles are management, notice, choice and consent, collection, use and retention, access, disclosure to third parties, security for privacy, quality, monitoring and enforcement.

APEC Privacy Principles

A set of non-binding principles adopted by the Asia-Pacific Economic Cooperative (APEC) that mirror the OECD Fair Information Privacy Practices. Though based on OECD Guidelines, they seek to promote electronic commerce throughout the Asia-Pacific region by balancing information privacy with business needs.