UNIT 10 OECD PRINCIPLES

Structure

10.1 INTRODUCTION

The Organization for Economic Co-operation and Development (OECD) was originally established as the inter-governmental Organization for European Economic Co-operation (OEEC) with support from the United States and Canada to co-ordinate the economic reconstruction of Europe after World War II. The OECD formally took over from the OEEC in 1961 and has its headquarter in Paris.

As an economic alliance, the mission of the OECD has been to help member country governments achieve sustainable economic growth in the form of creation of employment opportunities and higher standards of living while maintaining financial stability and thereby contributing to the overall development of the world economy. The OECD purports to assist sound economic expansion in member countries and other countries in the process of economic development and thereby contributes to growth in world trade on a multilateral and non-discriminatory basis.

The OECD produces internationally agreed instruments, decisions and recommendations with the constituent elements of dialogue, consensus and peer review in order to promote directives in areas where multilateral agreements may be required for the economic progress of individual countries in an increasingly global and competitive economy.

The OECD currently consists of about 30 member countries including the United States, the United Kingdom, Germany, France, Japan and Korea. The governing body of the OECD (Council) comprises of representatives from its member countries. In addition to the member countries, the OECD maintains active relationships with about 70 other non-member countries including India and with various non-governmental organizations, offering its analytical expertise and accumulated experience to such countries and organizations.

10.2 OBJECTIVES

After studying this unit, you should be able to:

- explain the background of the OECD;
- describe the basis for the OECD Guidelines;
- describe the scope of the OECD Guidelines;
- explain the principles for national application; and
- explain the principles for international application.

10.3 OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANS BORDER FLOWS OF PERSONAL DATA

The OECD Guidelines on the protection of privacy and transborder flows of personal data have been framed to address issues pertaining to requirement of protecting personal data privacy in the light of the widespread dissemination of cross-border personal data.

10.3.1 Basis for the OECD Guidelines

There has been an increasingly widespread trans-jurisdictional flow of personal data across international frontiers in the past few decades owing to the rapid advancement in data transmission technology and technological processes and leading to emerging issues in the areas of unlawful storage of personal data, storage of inaccurate personal data and the unauthorized disclosure or onward transmission of such data leading to the abuse of personal data privacy.

A need to protect personal data privacy has been recognised by various countries in the form of legislations, regulations and policy guidelines formulated by them in this regard. However there has also been a parallel recognition that any disparities in such sometimes diverging legislations, regulations and policy guidelines across countries could disrupt the free trans border flow of necessary personal data and further that such disruptions could impart serious damage to critical sectors of the economy such as banking and insurance.

Recognising the above issues, the OECD member countries decided that it would be imperative to formulate comprehensive guidelines to harmonise the various national privacy legislations, regulations and policy guidelines in order to develop a dual framework of upholding privacy protection of personal data as well preventing interruptions in the trans border flow of such data. The OECD Guidelines on the Protection of Privacy and Trans Border Flows of Personal Data (Guidelines) were framed as a result of the above recognition in the form of recommendations made by the Council. The Guidelines were formally adopted with effect from September 23, 1980 and represent a consensus on basic principles that can either be built into existing national legislations, regulations and policy guidelines of member countries or alternatively, serve as a basis for legislations in member countries that do not have the same in the form and manner set out as follows:

- Member countries take into account in their domestic legislations the principles concerning the protection of privacy and individual liberties set forth in the Guidelines;

- Member countries endeavour to remove (if created) or avoid creating unjustified obstacles to trans border flows of personal data in the name of privacy protection;
- Member countries co-operate with one another towards the comprehensive implementation of the Guidelines; and
- Member countries agree at the earliest on specific procedures of consultation and co-operation for the application of the Guidelines.

10.3.2 Scope of the OECD Guidelines

The Guidelines have general application to the personal form of data i.e. information that can be related to identified or identifiable individuals, whether in the public or private sectors. Such form of data poses a critical danger to issues in respect of privacy and individual liberties owing to its inherent nature cum context and the manner in which it is processed.

The Guidelines however do not purport to constitute a set of general privacy protection principles — for instance, the invasion of privacy by candid photography, physical maltreatment or defamation are outside the scope of the Guidelines unless such acts are in any way associated with the handling of personal data.

The broad scope of the Guidelines is as follows:

1. The Guidelines permit the application of different measures of data protection to different categories of personal data on the basis of the nature and the context in which such categories of data are collected, stored, processed or disseminated;
2. The Guidelines cover personal data that does not purportedly contain any risk to privacy or individual liberties i.e. simple and factual data if used in a context where the same may become offensive to the subject of such data shall be included in the scope. However, data collections of an obviously innocent nature such as personal notebooks are excluded;
3. The Guidelines in their application extend to both forms of processing of personal data i.e. the automated form of processing personal data and the non-automated form;
4. The Guidelines permit the exceptions contained therein including those relating to national sovereignty, national security and public policy subject to such exceptions being restricted to as few as possible and further subject to the same being made known to the public at large;
5. The Guidelines permit their comprehensive observance in the particular context of federal country jurisdictions to be affected by the division of powers in such jurisdictions; and
6. The Guidelines purport to be construed as minimum standards that are flexible to and capable of being supplemented by any additional measures adopted for the protection of privacy and individual liberties.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 4 Min.*

What are the various ways in which OECD Guidelines can serve as a basis for legislation?

.....

.....

.....

.....

.....

.....

10.4 OECD GUIDELINES: BASIC PRINCIPLES OF NATIONAL APPLICATION

The Guidelines are primarily an embodiment of eight comprehensive principles regarding the collection and use of personal data and are termed as the Basic Principles of National Application (Principles). Prior to setting out and for the purpose of understanding the nature and meaning of the Principles, it shall be relevant to understand the following terms in their context:

a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data is collected, stored, processed or disseminated by that party or by an agent on its behalf.

The above definition of a data controller attempts to define a subject who, under applicable domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. Such data controller may be a legal or natural person, public authority, agency or any other body.

The definition excludes at least four categories that may be involved in the processing of data, namely

(i) licensing authorities and similar bodies which exist in some member countries and which authorize the processing of data but are not entitled to decide what activities should be carried out and for what purposes;

(ii) data processing service bureaus which carry out data processing on behalf of others;

(iii) telecommunication authorities and similar bodies which act as mere conduits; and lastly

(iv) "dependent users" who may have access to data but who are not authorized to decide inter alia, what data should be stored and who should be able to use such data.

The above definition of data controller provides a benchmark threshold for the member countries of the OECD to define the roles and responsibilities of a data controller. Further, in the implementation of the Guidelines, member countries may develop more complex schemes of levels and types of responsibilities.

b) "personal data" means any information relating to an identified or identifiable individual (data subject).

The terms "personal data" and "data subject" clarify that the applicability of the Guidelines is confined only to physical persons. The Guidelines therefore do not take into account the misuse of non-identifiable anonymous data.

c) "trans border flows of personal data" means movements of personal data across national borders.

The above definition restricts the application of certain provisions of the Guidelines to international data flows and omits the data flow problems particular to a federal jurisdictional set-up. Further, the Guidelines recognise that though movements of data often take place through electronic transmission, however other means of data communication are not excluded including the transmission of data by satellite.

The Principles are set out herein below as follows:

1. **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.

This principle deals with the basic issue that it is desirable to recognise the categories of data, which could be per se sensitive, and therefore the collection of such sensitive data should be restricted or even prohibited. For example, sensitive data relating to an individual could be regarding an individual's health, race, religion and criminal records the use of which could be detrimental or discriminatory in relation to an individual and hence should not be without the knowledge or consent of the data subject. This forms the basis for the privacy legislation of countries such as the United States. Though it may be difficult to universally specify as to what constitutes "sensitivity", however the following limits have been recognised in the collection and processing of data, which could be considered sensitive:

- data quality aspects i.e. to be able to derive information of sufficiently high quality from the data collected and that the data should be collected in a proper information framework;
- limits associated with the purpose of data processing i.e. only certain categories of data ought to be collected and that data collection should be restricted to the minimum to fulfill the specified purpose;
- "earmarking" of especially sensitive data according to traditions and attitudes in each member country;
- limits to data collection activities of certain data controllers;
- civil rights' concerns.

This principle is further directed against practices that involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is a minimum critical requirement. However, there is an exception in respect of situations where for practical or policy reasons, the knowledge of the data subject is not considered necessary. Criminal investigation activities and the routine up dating of mailing lists are examples in this regard. Further, the principle does not also exclude the possibility of a data subject being represented by another party, for instance in the case of minors and mentally disabled persons.

2. **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.

The principle deals with the accuracy, completeness and up-to-datedness of data, which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives.

3. **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.

The principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle (supra) and the Use Limitation Principle (below). It implies that prior to, and in any case not later than at the time of data collection, it should be possible to identify the purposes for which these data are to be used and that any later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. New purposes should not be introduced arbitrarily and the freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorized copying or the like.

4. **Use Limitation Principle**

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 principle deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorized purposes without being inspected and thus disclosed in the proper sense of the word. Therefore, the initially or subsequently specified purposes should be decisive for the uses to which the concerned data can be put. The two exceptions, as stated above are the consent of the data subject (or his representative) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data, which have been collected for purposes of administrative decision-making, may be made available for research, statistics and social planning.

5. **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.

This principle highlights that while security and privacy issues may not be identical however, security safeguards should reinforce limitations on data use and disclosure. Further, such safeguards shall include physical measures (locked doors and identification cards, for instance), organizational measures (such as authority levels with regard to access to data and obligations for data processing personnel to maintain confidentiality) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them).

Under this principle, "loss" of data purports to encompass such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media while "modified" is construed to cover unauthorized input of data, and "use" to cover unauthorized copying.

6. **Openness Principle**

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means 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 should be readily available.

This principle may be viewed as a prerequisite for the Individual Participation Principle; for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means, which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

7. **Individual Participation Principle**

Under the provisions of this principle, an individual should have the right:

a) to obtain from a data controller (or otherwise) a confirmation of whether or not the data controller has data relating to him; and

b) to have communicated to him, data relating 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.

The right of individuals to access and challenge personal data is generally regarded as the most important privacy protection safeguard. The right to access should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or such similar measures.

In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical field, a medical practitioner can serve as a go-between. In

some countries supervisory organs, such as data inspection authorities, may provide similar services. Further, the requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests.

Communication of such data "in a reasonable manner" is construed to mean that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain copies of data relating to them is a matter of implementation, which as per the interpretation of this principle must be left to the decision of each member country.

The right to be given reasons is narrow in the sense that it is limited to situations where requests for information have been refused. The right to challenge in (c) and (d) purports to be broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure. The right to challenge also does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.). Such matters are the subject of domestic law and legal procedures.

8. **Accountability Principle**

A data controller should be accountable for complying with measures that give effect to the principles stated above.

This principle is structured on the premise that since the data controller takes decisions in respect of both data and data processing activities; it is for his benefit that the processing of data is carried out. Accordingly, it becomes essential that accountability for complying with privacy protection rules and decisions should be placed onto the data controller irrespective of the processing of data being carried out by another party such as a service bureau. On the other hand however, the Guidelines do not prevent service bureau personnel, "dependent users" and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information. Accountability refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 4 Min.*

What is the relationship of the purpose specification principles with the data quality principle and the use limitation principle?

.....

.....

.....

.....

.....

.....

10.5 OECD GUIDELINES: BASIC PRINCIPLES OF INTERNATIONAL APPLICATION

The Guidelines also deal with the Basic Principles of International Application (International Principles), i.e. principles that are chiefly concerned with relationships between member countries. The International Principles are:

- Member countries should take into consideration the implications of domestic processing and re-export of personal data for other member countries;
- Member countries should take all reasonable and appropriate steps to ensure that trans border flows of personal data (including transit through a member country) are uninterrupted and secure;
- Member countries should refrain from restricting trans border flows of personal data between themselves and other member countries except where the latter does not yet substantially observe the Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. Member countries may also impose restrictions in respect of certain categories of personal data for which their domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection.
- Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans border flows of personal data that would exceed requirements for such protection. (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data available at http://www.oecd.org).

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

Under what circumstances should countries NOT refrain from restricting transborder flows of data between themselves?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

10.6 SUMMARY

- OECD seeks to assist member countries by providing internationally agreed upon instruments, decisions and recommendations.
- OECD framed Guidelines on protection of privacy and transborder flaws of personal data on recognition that a critical need to protect personal data privacy has arisen due to increasingly widespread trans- jurisdiction flow of personal data.

- The Guidelines permit application of different measures of data protection, extend to both automated and non-automated forms of processing personal data, provide for security and policy based exceptions and seek to be construed as minimum standards capable of adaptation.
- The Guidelines provide 8 basic principles of national application:
  - (i) Collection Limitation
  - (ii) Data Quality
  - (iii) Purpose Specification
  - (iv) Use Limitation
  - (v) Security Safeguards
  - (vi) Openness
  - (vii) Individual Participation
  - (viii) Accountability
- OECD Guidelines lay down principles for international application.
  - (i) Implication of domestic process and re-export
  - (ii) Transborder flows to be uninterrupted and secure
  - (iii) Refrain from restricting transborder flows except under specific exemptions
  - (iv) Avoid developing law and policies that create obstacles to transborder flows.

10.7 TERMINAL QUESTIONS

1. What is the background of the OECD Guidelines?
2. What are the emerging issues with regard to unlawful storage and transmission of personal data?
3. Broadly define the scope of the OECD Guidelines?
4. What are the eight principles set out in the OECD Guidelines?
5. What are the basic international principles of the OECD Guidelines?

10.8 ANSWERS AND HINTS

Self Assessment Question

1. OECD Guidelines may serve as a basis for legislation in countries by such countries
   - (a) taking into account in their domestic legislation, the OECD principles;
   - (b) endeavouring to remove or avoid creation of unjustified obstacles to transborder flows of personal data;
   - (c) co-operating with one another towards the comprehensive implementation of OECD Guidelines;
   - (d) agreeing on specific procedures of consultation and cooperation for application of guidelines.
2. The Purpose Specification Principle (PSP) provides that
   - (a) Specifying of the purposes for personal data is collected not later than at the time of data collection itself; and

(b) Restricting the subsequent use of such collected data to the fulfillment of the said purpose. It is closely associated with Data Quality principle on account of the stress it lays upon the accuracy, completeness and up to datedness of the data collected to be linked to the purpose for which such data is collected. Further, it is closely associated with use limitation principle as it seeks to emphasize that personal data should not be disclosed for purposes other than those clearly specified at the time of collection.

3. Member countries should restrict transborder flows of personal data when other countries to where data transmission is intended, do not substantially deserve the guidelines or where the re-export of such data would circumvent its domestic privacy legislation.

Terminal Questions

1. Refer to section 10.3 of the unit.
2. Refer to section 10.3 of the unit.
3. Refer to section 10.3 of the unit.
4. Refer to section 10.4 of the unit.
5. Refer to section 10.5 of the unit.