

# **Organisation for Economic Cooperation and Development guidelines**

## **Annex to the recommendation of the Council of 23 September 1980**

### **Guidelines governing the protection of privacy and transborder flows of personal data**

#### **Part 1: General**

##### **Definitions**

1. For the purposes of these Guidelines:
  - 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 are collected, stored, processed or disseminated by that party or by an agent on its behalf;
  - b) "personal data" means any information relating to an identified or identifiable individual (data subject);
  - c) "transborder flows of personal data" means movements of personal data across national borders.

##### **Scope of Guidelines**

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.
3. These Guidelines should not be interpreted as preventing:
  - a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
  - b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
  - c) the application of the Guidelines only to automatic processing of personal data.
4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:
  - a) as few as possible, and
  - b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.
6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

## **Part 2: Basic principles of national application**

### **Collection Limitation Principle**

7. 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.

### **Data Quality Principle**

8. 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.

### **Purpose Specification Principle**

9. 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 fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

### **Use Limitation Principle**

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
  - a) with the consent of the data subject; or
  - b) by the authority of law.

### **Security Safeguards Principle**

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

### **Openness Principle**

12. 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 identify and usual residence of the data controller.

### **Individual Participation Principle**

13. 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 communicated to him, data relating to him
  - i) within a reasonable time;
  - ii) at a charge, if any, that is not excessive;
  - iii) in a reasonable manner; and
  - iv) 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.

### **Accountability Principle**

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

### **Part 3: Basic principles of international application: free flow and legitimate restrictions**

- 15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
- 16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
- 17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its 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.
- 18. 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 transborder flows of personal data that would exceed requirements for such protection.

### **Part 4: National implementation**

- 19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:
  - a) adopt appropriate domestic legislation;

- b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- c) provide for reasonable means for individuals to exercise their rights;
- d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- e) ensure that there is no unfair discrimination against data subjects.

## **Part 5: International cooperation**

- 20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.
- 21. Member countries should establish procedures to facilitate:
  - i) information exchange related to these Guidelines, and
  - ii) mutual assistance in the procedural and investigative matters involved.
- 22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.