

Data Protection, Privacy & Freedom Of Information

Table Of Contents

- Data Protection, Privacy & Freedom Of Information
 - Table Of Contents
 - Privacy
 - Criticism Of Facebook (Privacy Concerns)
 - Cooperation With Government
 - What is the Data Protection Act?
 - * Data Protection Act, 1998
 - How Can The Data Protection Act Help Us?
 - Main Principles Of The 1998 Act
 - Data Protection Principle
 - * First
 - * Second
 - * Third
 - * Fourth
 - * Fifth
 - * Sixth
 - * Seventh
 - * Eight
 - Rights Of Data Subjects
 - Data Protection Act, Pakistan
 - * Freedom Of Information
 - * Freedom Of Information Ordinance
 - References

Privacy

- Fear about large amount of information about individuals being held on computer files
- Individuals could be harmed by the existence of computerized data that could be transferred to an unauthorized third party at high speed and very little cost

The data could be,

- **Healthcare** records: records
- **Criminal Justice**: investigations & proceedings
- **Financial**: Financial institutions & transactions
- **Biological**: Traits, genetic material
- **Residence**: Geographical records
- **Ethnicity**
- **Privacy Breach**
- **Geo-location**: Location-based service and geo-location

Criticism Of Facebook (Privacy Concerns)

- Facebook Beacon 2007,
 - “Beacon was a part of Facebook’s advertisement system that sent data from external websites to Facebook, for the purpose of allowing targeted advertisements and allowing users to share their activities with their friends.”

Cooperation With Government

- Data Mining

What is the Data Protection Act?

- Freedom to process data vs privacy of individuals
- 1984 act was repealed by the 1998 act
- Anyone who processes personal information must comply with the eight principles

Data Protection Act, 1998

- To protect individuals from,
 - The use of inaccurate personal information or information that is incomplete or irrelevant
 - The use of personal information by unauthorized persons
 - Use of personal information other than the intended purpose
- Terms of the act,
 - Personal Act
 - Data Users
 - Data Subject
 - Data Controller
- Rules Of Data Processing,
 - Processing means obtaining, recording or holding the information or data or carrying out any operations on it, including,
 - * Organization, adaption or alteration of the information or data
 - * Retrieval, consultation or use of the info or data
 - * Disclosure of the info or data by transmission, dissemination or otherwise making available
 - * Alignment, combination, blocking, erasure or destruction of the information or data

How Can The Data Protection Act Help Us?

- It gives u the right to see our files
- It says those who record and use personal information must be open about how the information is used
- It must follow the 8 principles of good information handling

Main Principles Of The 1998 Act

- Personal data must be,
 1. Fairly and lawfully processed
 2. Processed for limited purposes
 3. Adequate, relevant and not excessive
 4. Accurate not kept for longer than is necessary
 5. Processed in line with your rights
 6. Held securely
 7. Measures shall be taken against unauthorized or unlawful processing of personal data & against accidental loss or damage
 8. Transferred to countries with adequate data protection

(FPAAPHMT)

Data Protection Principle

First

Personal Data shall be processed fairly and lawfully and in particular shall not be processed unless,

1. At least one of the conditions in Schedule 2 is met
2. In case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

Second

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purposes or those purposes.”

Data controllers must notify the Information Commissioner of the personal data that they are collecting and the purposes for which it is being collected.

Third

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.”

Many violations of this principle are due to ignorance rather than to intent to behave in a way contrary to the Act.

Local government has a bad record of compliance with this principle, for example shops that demand to know customers’ addresses when goods are not being delivered are also likely to be in breach of this principle.

Fourth

“Personal data shall be accurate and, where necessary, kept up to date.”

While this principle is admirable, it can be extremely difficult to comply with.

Fifth

“Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.”

This principle raises more difficulties than might be expected.

Sixth

“Personal data shall be processed in accordance with the rights of data subjects under this Act.”

Right to know whether a data controller held data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

Seventh

“Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

Eight

“Personal data shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”

Rights Of Data Subjects

The 1998 Act extends this right of access so that data subjects have the right to receive,

1. A description of the personal data being held
2. An explanation of the purpose for which it is being held and processed
3. A description of the people or organizations to which it may be disclosed
4. An intelligible statement of the specific data held about them
5. A description of the source of the data

Data Protection Act, Pakistan

- Organizations that provide computer/telephone services can monitor and record communications without the consent of the users of the service, provided this is done for one of the following purposes,
 - To establish facts, for example, on what date a specific order was placed

- To ensure that the organization’s regulations and procedures are being complied with
- To ascertain or demonstrate standards which are or ought to be achieved
- To prevent or detect crime (whether computer-related or not)
- To investigate or detect unauthorized use of telecom systems
- To ensure the effective operation of the system, for example, by detecting viruses or denial of service attacks
- To find out whether a communication is a business communication or a private one
- To monitor (but not record) calls to confidential, counselling helplines run free of charge by the business

Freedom Of Information

- Under the terms of the Act, any member of the public can apply for access to such information
- The Act also provides an enforcement mechanism if the information is not made available

Freedom Of Information Ordinance

The Right to Information Act (RTI) is an Act of the Parliament of India “to provide for setting out the practical regime of right to information for citizens” and replaces the erstwhile Freedom of information Act, 2002.

References

- Chap 14 Data Protection