LAW ENFORCEMENT ACCESS TO DATA IN MAURITIUS

By Drudeisha Madhub
Data Protection Commissioner
Date: 12.08.14

DATA PROTECTION PRINCIPLES

Individuals have the right to

- find out whether their personal data are being processed
- get access to the data ("subject access")
- have inaccurate data corrected and unlawfully processed data blocked or erased
- Individuals do not have to give reasons for seeking access

The right of subject access is one of the main pillars of data protection

Interference with right to private life *Leander v Sweden:1987*

- Applicant sought employment in a museum on a naval base. After a security check, he was refused employment but not told why or allowed to comment.
- The ECtHR found that storing and release by security police of information about applicant's private life was an interference with his right to private life of subject access is one of the main pillars of data protection

Subject access: independent supervision *Gaskin v UK:1989*

- Applicant had been in care as a child. As an adult, he sought access to his care records. He was given some, but refused others where the authors objected. There was no opportunity to seek an independent review.
- The Court found that the applicant had a vital interest in receiving the information about his early development. Refusal by the authors could be compatible with Article 8, but the principle of proportionality required that an independent authority be able to arbitrate.
- Subject access is one of the main pillars of data protection

Private life at work *Niemitz v Germany :1992*

- The applicant's office was searched, under warrant, for incriminating documents in a criminal case.
- The court found that the search of the applicant's workplace involved interference with his rights under Article 8. The derogations might be more far-reaching in such cases.

Fundamental importance of data protection: Particular sensitivity of HIV information *Z v Finland: 1997*

- The case involved a criminal trial in which both the defendant and his wife were HIV positive. During the trial, doctors were compelled to disclose both the husband's and the wife's medical records.
- The ECtHR found that there had been interference with the wife's right to private life. In considering whether it was proportionate, it took into account that data protection was of fundamental importance to the right to private life. The need to protect confidentiality was of particular importance where HIV was involved. Interference could be justified only by an overriding requirement in the public interest.

The need for safeguards *Rotaru v Romania: 2000*

- The applicant complained that the Romanian Intelligence Service held information on his private life, some of it 50 years old, and he could not refute the untrue information.
- The ECtHR found that there was an interference with the applicant's private life, and that there was a basis in domestic law. However, the law provided insufficient limits on the powers available: for example, the kind of information collected; the period for which it was kept; the people able to consult it; the purposes for which it may be used.

The need to inform data subjects *Perry v UK: 2003*

- The police made a covert video-recording of a suspect who refused to take part in an identity parade. They showed the video, along with others, to witnesses in place of an identity parade.
- The ECtHR found that there had been an unjustified interference with the applicant's right to private life. The police had not obtained his consent to the recording, informed him that it was being made, or informed him of his rights.

Disclosure of personal data in court *L.L. V France: 2006*

- The applicant had been involved in divorce proceedings. His wife produced a medical report about him which he said she had obtained fraudulently. The case went to appeal and the appeal court quoted from the report.
- The ECtHR found that the appeal court had disclosed personal data about the applicant. The appeal court could have based its decision on other evidence, the report being only of subsidiary use. The interference with the applicant's right to private life, in view of the fundamental importance of the protection of personal data, was not proportionate.

Protection of private life on internet *KU v Finland: 2008*

- **A message on an on-line dating site about the alleged availability of the applicant, a 12 year old boy, was posted anonymously. The ISP would not reveal the identity of the originator of the message, to allow charges to be brought, because of the law on confidentiality of communications. The Finnish courts agreed.**
- **The ECtHR found that there had been a violation of the boy's right to private life. Freedom of expression and confidentiality of communications were primary considerations. Users of internet services must have a guarantee that their own privacy and freedom of expression will be respected. But such guarantee cannot be absolute and must sometimes give way to other legitimate concerns, including the protection of the rights and freedoms of others.**

Unrestricted retention of DNA *S.and Marper v UK: 2008*

- DNA profiles, cellular samples and fingerprints of the applicants, one a minor, were retained indefinitely after their criminal trials had resulted in no finding of guilt.
- The ECtHR found that retaining all three categories of information was an interference with the right to private life. There was a risk of stigmatisation in treating the information of convicted and unconvicted people in the same way. This could be especially harmful in the case of minors. The retention of the data did not strike a fair balance between public and private interests.

DATA PROTECTION: BALANCE

- **It is not the aim of data protection to prevent personal data being used**
- **It seeks to balance organisations' need to use personal information with individuals' right to respect for their privacy**

  "Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other."

  Police Data Protection Recommendation: Preamble

ICT LAWS IN MAURITIUS

- Data Protection Act (DPA) 2004
- Computer Misuse and Cyber-Crime Act 2003
- Postal Services Act 2002
- The Information and Communication Technologies Act 2001
- The Electronic Transaction Act 2000
- Independent Broadcasting Authority Act 2000
- Copyright Act 1997
- Child Protection Act

The Data Protection Act in Mauritius

- Under the Data Protection Act 2004, the Data Protection Office as a law enforcement body has certain powers on access to data namely sections 7, 8, 13 and 17. Section 46 of the DPA provide for exceptions from the application of sections 23 to 26, second third, fourth and eight principles and part VI only in respect of blocking and not access to personal data. Section 52 caters for disclosure required by law or court order or legal proceedings.

Section 8 - Powers to obtain information

Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act and section 30 of the Financial Intelligence and Anti-Money Laundering Act –

(a) the Commissioner may, by notice in writing served on any person, request from that person, such information as is necessary or expedient for the performance of his functions and exercise of his powers and duties under this Act; and

Section 8 - Powers to obtain information

(b) where the information requested by the Commissioner is stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the person named in the notice shall produce or give access to the information in a form in which it can be taken away and in which it is visible and legible.

Section 13- Preservation Order

- The Commissioner may apply to a Judge in Chambers for an order for the expeditious preservation of data, including traffic data, where he has reasonable grounds to believe that such data is vulnerable to loss or modification.

Section 17- Powers of entry and search

- An authorised officer may enter and search any premises for the purpose of discharging any functions or exercising any powers under this Act.
- No authorised officer shall enter or search any premises unless he shows to the owner or occupier a warrant issued by a Magistrate for the purpose referred to above.

Section 17- Powers of entry and search

- A Magistrate may, on being satisfied on an information upon oath that entry and search into any premises are necessary to enable the authorised officer to discharge any of his functions or exercise any of his powers under this Act, issue a warrant authorising the authorised officer to enter and search the premises.

Section 17- Powers of entry and search

Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act and section 30 of the Financial Intelligence and Anti-Money Laundering Act, an authorised officer may, on entering any premises –

(a) request the owner or occupier to produce any document, record or data;

(b) examine any such document, record or data and take copies or extracts from them;

(c) request the owner of the premises entered into, or any person employed by him, or any other person on the premises, to give to the authorised officer all reasonable assistance and to answer all reasonable questions either orally or in writing.

Obligations of data controllers under DPA

- Under the Data Protection Act 2004, data controllers (i.e the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing personal data) have responsibilities and obligations related to the processing they undertake.

- The data controller is thus required to implement organisational measures to protect personal data against unauthorised disclosure or access.
- The data controller should ensure that the data is necessary for an investigation and at the very least that he discloses it on an need to know basis.

- **For transfer of personal data abroad, the data controller is also required to seek the written authorisation of the Data Protection Commissioner.**

Transborder Access to data

- ***Article 32 of the Budapest Convention on Cybercrime***
- ***Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction***

Current Article 32 of the Budapest Convention on Cybercrime

Relating to Transborder access to stored computer data with consent or where publicly available:

A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

- **The implementation of the said article therefore depends on what is the "lawful and voluntary consent of the person who has the lawful authority to disclose the data" according to the national law of the requested Party**

- Current practice in international agreements and treaties in the field of law enforcement where mutual legal assistance is granted on the basis of national legal requirements of the requested party

The issue of direct access to data and the applicable law - Article 29 Working Party's comments

- The issue of consent

  According to our DPA, consent can only be given by data subjects. Therefore, companies acting as data controllers usually do not have the "lawful authority to disclose the data" which they process for e.g. commercial purposes.

- They can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required.

- Data controllers cannot lawfully provide access or disclose the data to foreign law enforcement authorities that operate under a different legal and procedural framework from both a data protection and a criminal procedural point of view.

- **It is imperative that data transfers have a specific and legitimate legal basis in the law of the requested Party (e.g. judicial authorisation/warrant), that the principles of necessity and proportionality are respected and that no large-scale access to personal data is permitted. An additional protocol to an international Convention that would appear to provide for access to data stored on computers abroad by applying the law (or the definitions of consent) of the searching party would be in violation of the Data Protection Act.**

Thank You

Questions
&
Answers