Mauritius

Gayrel, Claire

Published in:
Privacy laws & business international report

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

Mauritius: Data protection in an evolving island economy

Claire Gayrel explains the Mauritian Data Protection Act of 2004 which has been amended twice as the island nation looks towards making information technology and telecommunications a pillar of the economy.

The Republic of Mauritius, with its 1.2 million of inhabitants and surface area of about 2,000 square km, developed its first national information and communications technology (ICT) policy in 2007, with the aim of the ICT sector becoming the fifth pillar of the economy – after agriculture, textile manufacturing, tourism, and financial services[1]. In this context, the Ministry of Information Technology and Telecommunications identified, among other objectives, a need to modify the Mauritian Data Protection Act in order to be potentially recognised by the European Union as a third country with an adequate level of protection[2]. The Act, originally enacted on 1 June 2004, was consequently amended twice in 2009 (Act 01/2209 of 16 February, and Act 14/2009 of 30 July).

While the Act draws its inspiration from the European Directive 95/46 and the OECD Guidelines, the Minister of Information Technology and Telecommunications mentions that it has been inspired by the data protection legislation of the United Kingdom, Australia, New Zealand, Canada and Hong-Kong. It shows close affiliation with the UK Act, notably with respect to the organisation of the exemptions regimes.

The Act applies both to the public and the private sectors. The data controller is identified as being the one who decides upon the purposes and means of the processing[3]. It affords protection to living individuals only as data subjects.[4] Both manual and automatic processing operations of data are covered.[5]

Principles

The Act lays down the principle of express consent of the data subject as the main ground for lawfulness of processing.[6] According to the Data Protection Office of Mauritius, the consent must include the "knowledge of the matter agreed to, and voluntary agreement"[7]. Thereby, an express consent can be given orally or in writing. Other grounds for lawful processing are foreseen for specific cases listed in the Act (s24(2)).

The "First Schedule on Data Protection Principles" details the content of all main data protection principles: purpose limitation principle[8], data quality and proportionality principle[9], principle of transparency[10], security principle[11], rights to access[12], rectify, block, erase or destroy personal data[13], restrictions to international transfers[14], specific guarantees with respect of sensitive data[15], a right to object to direct marketing processing[16] and specific guarantees in the matter of data matching[17].

Exemptions to data subjects' right of access

The Act provides a subject access right upon written request and on payment of a fee but includes six categories of exemptions[18].

One provision surprisingly leads to the denial of the data subject's right to request access to the personal data relating to him and processed in the framework of education, training or employment. It provides that the data controller shall not comply with an access request "where he is being requested to disclose information given or to be given in confidence for the purposes of the education, training or employment, or prospective education, training or employment, of the data subject." (S41(5)(a)(i)). This leads to exclusion from the right of access regime in a range of processing operations carried out by schools, universities and employers. The rationale behind such exemptions is not discussed in the preparatory works, and raise, in our view, serious questions about its appropriateness.

Another exemption to the right of access of individuals is provided in section 47 of the Act relating to the specific regime applicable to "health and social work". It is provided that a data controller is exempted from the right of access "where the personal data to which access is being sought relates to the physical or mental health of the data subject and the application of that section is likely to cause serious harm to the physical or mental health of the data subject or of any other person".[19] Often referred to as the "therapeutic exception", this last has however undergone in continental law major evolution under the influence of the autonomy principle of patients[20], coming to restrict considerably the conditions of application of this exception. The European Directive 95/46 recognises the possibility for Member States to provide only an indirect access that would "specify that access to medical data may be obtained only through a health professional"[21]. Full denial of access is however not allowed, and the decisional power of practitioners over the "therapeutic exception" has been limited to a considerable extent in European Union Member States.

A restrictive international transfers regime

Restrictions to international transfers of personal data appear to be inspired partially by the European regime. International transfers of personal data are subject to two cumulative conditions:

i) that personal data can only be transferred with the written consent of the Data Protection Commissioner; and
ii) that the country of destination

ensures an adequate level of protection (adopting the European wording).

Where the country cannot be considered to provide an adequate level of protection, it is nevertheless possible to obtain the authorisation of the Commissioner when the data controller proves reliance on adequate safeguards. A transfer is also possible in specific cases (exemptions), which however do not exempt the data controller from obtaining the approval of the Data Protection Commissioner. The Mauritian regime therefore appears to be quite restrictive with respect to transborder data flows. It requires the controller to obtain the approval of the Data Protection Commissioner in all cases, whether the transfer is intended toward a country ensuring an adequate level of protection or not. This appears to be burdensome both for controllers and the Commissioner.

Exemption regimes

The Act excludes, or partially excludes, some activities from its scope, with specific exemption regimes for some activities. Part VII of the act specifically regulates the following matters: "national security", "crime and taxation", health and social work", "regulatory activities", "journalism, literature and art", "research, history and statistics", "information available to the public under an enactment", "disclosure required by law or in connection with legal proceedings", "legal professional privilege" and "domestic purposes". With the exception of the health and social work exemption regime to the right of access (discussed above), most other exemptions regimes can be justified and do not raise many issues. Two points however deserve discussion.

First, several activities are exempted from the proportionality principle according to which personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.[22] The Act exempts the processing of personal data for the prevention and detection of crime, or for the assessment or collection of any tax, duty or any imposition of a similar nature, or processing for a wide range of regulatory activities listed in s48. Although these exemptions are only allowed "to the extent that such an application would be likely to prejudice" these matters, they are questionable, particular because of the wide range of regulatory activities concerned.

Second, "crime and taxation" matters (S46), notably the processing of personal data "for the prevention and detection of crime" and "apprehension or prosecution of offenders" are exempted from various principles of the Act, but surprisingly are not exempted from the obligation of information imposed on controllers according to section 22 of the Act. This may be an unintended loophole of the Act, otherwise the Mauritian police would have to inform suspected people about fraudulent activities under investigation. This omission nevertheless raises the issue as to whether exemptions to data protection principles for police activities have duly been assessed.

Enforcement mechanisms

The Act provides for several enforcement mechanisms, including the establishment of a Data Protection Office ('the DPO')[23], headed by a Data Protection Commissioner. The DPO is a public office, and the Commissioner, who must be an experienced barrister, enjoys a permanent status of public officer.

Concerning independence, a former section 21 of the Act of 2004 provided that "the Prime minister may give in writing such directions of a general character to the Commissioner, not inconsistent with this Act, which he considers to be necessary in the public interest, and [that] the Commissioner shall comply with those directions". The section has been repealed by the Amending Act 1/2009 showing the will of the legislature to provide an unambiguous independence to the Commissioner.

The Commissioner has normative functions (see below), control functions and enforcement powers that are typical of any regulatory authority, from Part III of the Act. Among its normative functions, the Commissioner is notably entitled to issue or approve codes of practice or guidelines, authorise data matching processing, co-operate with supervisory authorities of third countries (s5). Among its extensive control powers, the Commissioner has the "power to obtain information" (s8); to issue an "enforcement of notice" (s12) or "preservation order" (s13); the "power to carry out prior security check" (s14); the "power to request assistance" from other authorities

REFERENCES

1. Ministry of Information Technology and Telecommunications National ICT Policy 2007-11
2. *Idem*, p. 7
3. See the definition of "data controller", section 2 of the Act
4. See the definition of "data subject", section 2 of the Act
5. See the definition of "processing", section 2 of the Act
6. Section 24, subsection 1 of the Act
7. "A Practical Guide for Data Controllers", Volume 1, Data Protection Office, available on www.gov.mu/portal/site/dataprotection
8. Section 26, a) and b) of the Act, second principle of the Data Protection Schedule
9. Section 22, subsection 1 and section 23 of the Act, third and fourth principle of the Data Protection Schedule
10. Section 22 of the Act
11. Section 27 of the Act, seventh principle of the Data Protection Schedule
12. Section 41 of the Act
13. Section 44 of the Act
14. Section 31 of the Act, eighth principle of the Data Protection Schedule
15. Section 25 of the Act
16. Section 30 of the Act
17. Section 32 of the Act
18. Section 43 and 47 of the Act
19. Section 47, subsection 1 of the Data Protection Act
20. HERVEG, J., VERHAEGEN, M-N., POULLET, Y., 'Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé', *Revue de droit de la santé*, 2002, pp. 56-85
21. Recital 42 of the European Directive 95/46
22. Third principle of the Data Protection Schedule and Section 26, c) of the Data Protection Act
23. Section 4 of the Act
24. www.gov.mu/portal/site/dataprotection
25. Section 63 of the Act

(sec.16); and the "power of entry and search any premises" (sec. 17). Finally, he is entitled to investigate the complaints brought to him (sec.11).

Appointed in August 2007, the Data Protection Office has proven to be rather active[24]. It has used its powers to issue a code of practice regulating the use of video surveillance systems operated by the police force. It has dealt with its first complaints (six since the beginning of the year 2011), and published five guidelines addressing aspects of the Act. The Commissioner has no direct sanction powers. The judiciary has exclusive jurisdiction over the offences committed under the Act.[25]

Conclusion

Although there are some weaknesses and loopholes in the Act, it is nevertheless fair to insist on the positive direction of the Mauritian initiative in the matter. In particular it is important to highlight the active role of the Data Protection Office and its Commissioner, Drudeisha Madhub, who has also been appointed in 2011 as one of the five members of the Commission for the Control of Files of INTERPOL. The support of the Government and the legislature also shows the political will to associate the policy objective to make Mauritius a Cyber Island with important data protection guarantees.

AUTHORS

Claire Gayrel is a researcher at CRIDS (Centre de Recherche Information, Droit et Société) Faculty of Law of Namur, Belgium.
Email: claire.gayrel@fundp.ac.be

Facebook: Audits for the next 20 years

In a settlement, agreed at the end of November, Facebook has agreed to various measures to rectify its alleged deception in its privacy policy.

The FTC says that Facebook was violating users' privacy by changing privacy settings without first notifying and obtaining consent from users. For example, in 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. The company did not warn users that this change was coming, or get their approval in advance.

It was also said that Facebook led customers to believe that it was not providing data to advertisers. Facebook also claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible – in fact access to the content remained. In addition, it was found that Facebook has not complied with US Safe Harbor requirements.

Facebook has now agreed to independent third-party audits, every two years, for the next 20 years. The audits are to certify that it has a privacy programme in place that meets or exceeds the requirements of the FTC order. Facebook now needs to seek users' consent before overriding privacy settings, and prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account.

Each violation of this consent order may result in a civil penalty of up to $16,000.

• *See www.ftc.gov/opa/2011/11/privacysettlement.shtm*

Ireland's DPA auditing Facebook

A spokesperson at the Irish Data Protection Commission told *PL&B* on 7 November that the office commenced a comprehensive audit of Facebook Ireland at the end of October. "This will assess Facebook's compliance with the requirements of the Irish Data Protection Acts as they apply to its users outside of the US and Canada. This Office [DPA] is in communication with other data protection and privacy authorities which are or have examined Facebook privacy practices."

The investigation stems from 22 complaints by the same individual about Facebook's privacy practices. It focuses initially to establish whether a breach has taken place, and will comprise on-site and off-site elements.

"Facebook is cooperating fully with the audit and we would anticipate that it will implement any necessary changes to comply with any requirements identified without the need for any use of powers by the Commissioner," the spokesperson said.

The audit should be completed by the end of the year, at which point the Commissioner will decide whether he will make some aspects public.

• *The complaints can be seen at www.europe-v-facebook.org/EN/Complaints/complaints.html*

Google settlement : 20 years of audits in US

The US Federal Trade Commission announced in October that it has approved the final settlement with Google on social network Google Buzz. The settlement, first issued in March, requires Google to implement a comprehensive privacy program, and have regular, independent privacy audits for the next 20 years.

• *See www.ftc.gov/opa/2011/10/buzz.shtm*