International Data Privacy Law Advance Access published January 25, 2013

Mauritius Data Protection Commission: an analysis of its early decisions

Alex Boniface Makulilo*

Abstract

- One of the functions of most data protection authorities is to decide complaints filed to them by individuals and institutions.
- In the course of passing their decisions, data protection authorities interpret data protection legislation. This article analyses the early decisions of the Mauritius Data Protection Commission from the onset of its establishment.
- The point of departure for discussion is the Mauritian Data Protection Act 2004 as well as regulations, codes of conduct, and guidelines made under such Act.
- The conclusion drawn from this analysis is that while these decisions reflect the basic data protection principles laid down in the law, they are not consistent to some extent. Similarly such decisions have at times taken into account factors beyond the provisions of the law.

Introduction

On 1 June 2004 Mauritius passed its data protection legislation, the Data Protection Act 2004 (DPA). The Act was assented to by Sir Enerood Jugnauth, the President of Mauritius on 17 June 2004. However, it did not immediately come into force. The first set of the DPA's provisions, sections 1, 2, 4, 5(b),(c),(e),(g),(h),(i),(j), and 6 came into force on 27 December 2004.[1] These provisions are about the short title of the Act, interpretation, establishment of the office of Data Protection Commission (DPC), vesting it with limited functions, confidentiality and the oath of the Commissioner and other DPC staff. The second set of provisions of the DPA—the rest of the Act—came into force on 16 February 2009.[2] However, the second implementation did not include section 17. The latter, which constitutes the third phase in proclamation, did not come into force until it was amended on 15 April 2009.[3] The amended section 17 came into force on 22 May 2009.[4]

Patterned on the European data protection system, the DPA incorporates the basic principles of data processing as well as a supervisory authority. The latter is the central authority set up to implement the DPA. This article analyses the complaint resolution role of the Mauritius Data Protection Commission. Excluded from the purview of this article are other functions of the DPC, though admittedly, some of them may have ramifications for the complaint resolution role.

The analysis presented here is significant for three reasons. First, it gives a broad overview of the practice of data protection law in Mauritius. In turn, if the DPC's interpretation of the law has any sensible results, this broad picture of how the DPA functions in practice may compliment the EU accreditation process, a recent assessment of which indicates that Mauritius has failed to pass the 'adequacy' requirement set out in the EU Data Protection Directive 95/46/EC.[5] Yet, if such an interpretation by the DPC is still wanting, this article will illuminate the areas which require improvements in order to strengthen the data protection practices. Second, since Mauritius is the only country in sub-Saharan Africa making many decisions, its interpretation of the DPA may somewhat influence the practice of other supervisory authorities on the sub-continent.

* Lecturer, Faculty of Law, Open University of Tanzania. E-mail: alex.makulilo@gmail.com.

1 Proclamation No. 45 of 2004.

2 Proclamation No. 5 of 2009.

3 The amendment was made through the Additional Stimulus Package (Miscellaneous Provisions) Act 2009, Act No. 1 of 2009.

4 Proclamation No. 11 of 2009.

5 CRID (Research Center on IT and Law), University of Namur (Belgium), 'Analysis of the Adequacy of the Protection of Personal Data provided in Mauritius, Final Report, 2010'. (Note that the opinions contained in this report are not of the European Union itself but of a commissioned consultant and hence do not necessarily reflect the position of the European Union).

Thus, it is imperative to examine how the basic data protection principles are implemented in practice in an African jurisdiction. The matter is more significant as the African Union (AU) as well as Southern African Development Community (SADC) are considering the adoption of regional and sub-regional data protection regimes respectively. At the same time, it is important to hint that the Economic Community of West African States (ECOWAS) had already adopted a sub-regional data protection framework. Similarly, the East African Community (EAC) had adopted recommendations which provide guidance to its member countries in legislating national data protection legislation. Third, as is the case in many other jurisdictions where the role of the courts is invariably minimal in providing interpretation of data protection legislation,[6] commentaries and analyses like this are important as an aid to commissioners in their roles.

The Data Protection Act

Scope and application

The Data Protection Act applies to both public and private bodies. It also regulates both automatic and manual processing of personal data. Yet such processing of personal data is limited to individual natural/physical persons only, called the 'data subject'. Legal/juristic persons are outside the purview of the Act.

Territorially, the DPA has a broad scope. It applies to a data controller who is established in Mauritius.[7] In addition such a controller must process personal data in the context of that establishment.[8] However in case a controller is not established in Mauritius but uses equipment in Mauritius for processing data, such a controller is subject to the DPA.[9]

The DPA has an extensive exemption regime. The latter is either partial or whole. The list of matters wholly exempted are national security (sect. 45); crime and taxation (sect. 46); health and social work (sect. 47); regulatory activities (sect. 48); journalism, literature, and art (sect. 49); research, history and statistics (sect. 50); information available to the public under an enactment (sect. 51); disclosure required by law or in connection with legal proceedings (sect. 52); legal professional privilege (sect. 53); and domestic purposes (sect. 54). Partial exemption usually takes the form of relieving the controller from the obligations of notification and the application of certain data protection principles.

The eight data protection principles

The basic principles of data processing in the Data Protection Act 2004 are provided in the *First Schedule*, entitled 'Data Protection Principles'. This schedule contains eight data protection principles inspired by European Directive 95/46/EC and to some extent by the OECD Guidelines. These principles are complimented by various codes of practice and guidelines developed by the Commissioner. Together they provide some insights into the understanding and interpretation of the eight principles. Three of the main codes and guidelines are: 'A Practical Guide for Data Controllers & Data Processors Volume 1' ('Practical Guide') and 'Data Protection—Your Rights—Volume 3' and 'Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems—Volume 5'.

The first principle provides that personal data shall be processed fairly and lawfully. The criteria of 'fairness' and 'lawfulness' are extensively covered in Rule 1 of the Practical Guide. 'Fair collection' means that the data subject has been fully made aware of the fact that his or her data are being collected. On the other hand 'fair processing' entails fulfilment of the conditions stipulated in sections 24 and 25 of the DPA. Section 24(1) states, 'no personal data shall be processed, unless the data controller has obtained the express consent of the data subject'. Yet, the Practical Guide does not explain what is meant by 'lawfully'. However in its wider sense 'lawfully' may mean processing that is in compliance with the provisions of the DPA. This may include elements of authorization (eg consent) as legal justification for processing personal data.

The second principle states that personal data shall be obtained only for a specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose. This principle is partly reflected in sections 22(1), 26(a),(b), and 29 of the DPA. Rule 2 of the Practical Guide, which interprets the second principle, prohibits the collection of information about people routinely and indiscriminately, without having a sound, clear, and legitimate purpose for so doing. Data controllers can only process personal information against the purpose for which it was registered in the entry of the public register.

6 See eg, LA Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law', (2000) 7/1 Privacy Law & Policy Reporter 11–14 & (2000) 7/2 33–6.

7 Data Protection Act 2004, s.3 (3), (a).

8 Ibid.

9 Ibid, s.3 (3), (b).

The third principle is the purpose specification. It requires that personal data shall be adequate, relevant, and not excessive in relation to the purpose for which they are processed. Rule 7 of the Practical Guide elaborates the third principle to require that the data controller should only collect and keep enough information that enables him or her to achieve the purpose for which information is collected and no more. The controller is prohibited to collect and keep information 'just in case' a use can be found for the data in the future. Likewise, controllers are prohibited from asking intrusive or personal questions, if the information obtained in this way has no bearing on the specified purpose for which he or she holds the personal data.

The fourth principle is that personal data shall be accurate and, where necessary, kept up to date. This principle also appears as an obligation in section 23 of the DPA. Rule 6 of the Practical Guide provides that a data controller, after being informed as to the inaccurateness of personal data by a data subject, must rectify, block, erase, or destroy the data as appropriate. This obligation extends to third parties. If the data controller fails to rectify, block, erase, or destroy inaccurate personal data, a data subject may apply to the Commissioner to have such data rectified, blocked, erased, or destroyed. Rule 6 provides further that this requirement (ie keeping data accurate and up-to-date) has additional importance in that it may result in the liability of a data controller to an individual for damages if the former fails to observe the duty of care provision in the Act applying to the handling of personal data.

The fifth principle concerns data retention. It requires that personal data processed for any purpose shall not be kept longer than is necessary for the purpose or those purposes. This principle is otherwise known as retention of personal data. Rule 8 of the Practical Guide provides that this requirement places a responsibility on data controllers to be clear about the length of time for which the data will be kept and the reason why the information is being retained. If there is no good reason for retaining personal information, then that information should be routinely deleted. Moreover, if the data controller wishes to retain information about customers to help provide better service to them in future, he or she must obtain the customers' consent in advance.

The sixth principle is that personal data shall be processed in accordance with the rights of the data subjects under the DPA. This principle has to be read in conjunction with Part VI of the DPA which deals with the rights of data subjects. The right of access to personal data under section 41 is the most important to the exercise of other rights of rectification, blockage, erasure, or destruction in section 44 of the DPA. Rule 10 of the Practical Guide essentially repeats the requirements and exceptions provided in Part VI of the DPA. Moreover it places an obligation on the data controller to explain to the data subject the logic used in any automated decision-making process where the decision significantly affects the individual and the decision is solely based on the automated process.

The seventh principle is a security principle. It states that appropriate security 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. This principle is broadly covered in section 27 of the DPA as part of the obligation of the data controller.

The eighth principle is about the international transfer of personal data. It states that personal data shall not be transferred to another country, unless that country ensures an adequate level of protection of the rights of data subjects in relation to the processing of personal data. This principle has to be read together with section 31 of the DPA. The latter section deals with the international transfer of personal data similar to Articles 25 and 26 of Directive 95/46/EC. Rule 9 of the Practical Guide interprets the eighth principle together with section 31 as setting out two criteria for the transfer of personal data to a foreign country, namely (i) that the foreign country in question ensures an adequate level of data protection and also (ii) the transfer is authorized in writing by the Commissioner.

Other rules of data processing

Apart from the eight data protection principles, the DPA contains special rules for the processing of personal data. These include sensitivity; direct marketing; and data matching.

The Commissioner's decisions

An overview

Since the DPA has come into force, the Commissioner has handed down a total of ten decisions. Before analysing these decisions, it is important to highlight their main general features. To start with, all the Commissioner's decisions have been posted on the Commission's website. Postings appear to be made immediately after a decision is made. However, it is difficult to establish exactly the date of publication, as the website does not contain this information. Pending complaints are unknown since the Commissioner neither posts this information on the website nor in annual reports.

However, the Commissioner had reported in her annual reports the number of complaints received in a particular year and the areas where such complaints fall. For example, in the second annual report of 2010, the Commissioner received two complaints.[10] In 2011, the Commissioner received eleven complaints and decided six of them.[11]

A party lodging a complaint is called the 'complainant' while the party against which a complaint is lodged is called the 'respondent'. The identities of the complainant and respondent are always anonymized. The Commissioner has done this on the basis of a duty of confidentiality imposed upon her and every officer in the Commission under section 6 of the DPA. However, some non-direct parties to a complaint are fully named by their identities. This is the case, for example, in the third and fifth decisions considered below.

Citation of these decisions is by reference number, followed by 'In the matter of', then the names of the parties. The first and second decisions are referenced as PMO/DPO/DEC while in the third to tenth they are DPO/DEC. In each case a serial number of a decision is added at the end. In these references PMO stands for 'Prime Minister's Office', DPO is the 'Data Protection Office' and DEC stands for 'decision'. It is not clear why the Commissioner dropped PMO in the subsequent reporting of her decisions. One may argue, though with some risk of a lack of certainty, that the Commissioner wanted to demonstrate a sense of the independence of her office in determining the complaints.

The other basic feature of the Commissioner's decisions is that they are relatively short, usually ranging between two to three A4 pages with only a few decisions exceeding this range. Yet, they are sufficient to convey information about the nature of a complaint, the legal issues involved, the essential steps taken by the Commissioner in investigation, a summary of the evidence, her findings, and verdicts.

Time is also of essence in complaint resolution. The Commissioner has taken an average of six months to one year to resolve one complaint. A number of reasons may be assigned. First, in some instances complainants had lodged their complaints with the wrong authority. When a situation like this occurs, it takes some time to reroute the complaint to the Commissioner. Second, some complaints are laid by anonymous complainants. These types of complaints usually require long investigations.

As alluded to, so far the Commissioner has decided ten complaints. It is imperative to survey these decisions in order to uncover: how the basic data protection principles have been applied in practice; how the Commissioner has engaged other provisions of the DPA, codes of practice and guidelines; how relevant such decisions are in the development of a data protection system in Mauritius; in whose interest the decisions are made; etc.

Analysis of the ten decisions

In *Complainant v Respondents 1, 2, and 3*,[12] the complaint was about unauthorized use of the complainant's curriculum vitae (CV) by respondents 1, 2, and 3. The complainant alleged that he originally communicated electronically his CV to respondent 1. The CV was to be used to support his contract with respondent 1 for the implementation of a food security project at respondent 2 who was a beneficiary of respondent 3.

In her decision, the Commissioner found that there was no evidence to support the complaint of unauthorized or unlawful use of personal data in the complainant's CV by respondents 1, 2, and 3 in carrying out the project. The reason given by the Commissioner was that the complainant was not any longer hired as consultant for the project after the cancellation of the contract with respondent 1. She set aside the complaint under sections 26(a) and (b) and 28 of the Data Protection Act as the offence had not been proved beyond reasonable doubt.

The Commissioner's decision in this instance is based on the second principle of data protection, that is purpose specification. It is also important to note that the Commissioner's decision is based on the duty to destroy personal data under section 28 of the DPA once its purpose has lapsed. Both of these requirements were fulfilled by the respondents. Yet, a close examination of the above decision leaves a lot to be desired. For example, it was not until the complainant had brought the matter to the attention of the Commissioner who had officially written to respondent 3, that the latter was able to return the complainant's CV. Arguably, the extended retention of the complainant's

10 Mauritius Data Protection Office, Third Annual Report 2011, p.9, <http://www.gov.mu/portal/goc/dpo/files/annrep2010.pdf>, accessed 11 August 2012.

11 Mauritius Data Protection Office, Third Annual Report 2011, pp. 5 &8, <http://www.gov.mu/portal/goc/dpo/files/Jan_Dec2011AnnRep.pdf>, accessed 11 August 2012.

12 Ref.No: PMO/DPO/DEC/1 (lodged on 21 July 2010, decided on 23 March 2011).

CV by respondent 3 after notification from the complainant did not comply with section 28 of the DPA.

In *Complainant v Respondent*[13] the complaint was about the use of CCTV cameras in residential areas. The complainant alleged that his neighbour, who is the respondent, had placed CCTV cameras in his yard, the visual angle of which was directed towards him. As a result, it had caused and was continuing to cause heavy prejudice to him by violating his privacy. The complainant further alleged that because of the acts of the respondent, he was not able to open his kitchen room and his family was suffering from intense heat during the summertime.

The Commissioner's site visit revealed that the images which were recorded by the respondent's camera did not capture anything outside the respondent's site. She decided that there was no incriminating evidence against the respondent. Nonetheless, she required the respondent to place, within two months of the date of receipt of the decision, a small but visible and legible sign near his entrance gate or any other appropriate area within his premises to inform all visitors that CCTV cameras were in operation for security purposes. The rationale for this was to prevent any potential infringement of the privacy rights of individuals and violations of the provisions of the DPA. The Commissioner set aside the complaint under section 11 of the DPA as no offence under the DPA had been proved beyond reasonable doubt.

This decision shows that the Commissioner did not specifically refer to the 'Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems—Volume 5', although she applied some of the rules laid down. Moreover, in contrast to the first decision, she set it aside under section 11 of the DPA. Admittedly, this is the correct enabling provision for the Commissioner's decision.

A similar decision involving claims of privacy as a result of the use of CCTV is *Complainant v Respondent.*[14] In this complaint, the complainant alleged that the respondent (a college) placed CCTV cameras in such a position as to affect his private life through the monitoring of his movements from and to his dwelling house. He provided the schema of the alleged positioning of the camera systems where he resided.

The Commissioner's site visit to the respondent's premise revealed that the respondent installed the CCTV cameras to deter vandalism from students, trespassing by her pupils on neighbouring houses and littering on the school compound. Despite the sound justification, the investigation revealed that two cameras slightly focused beyond the boundary walls because they were long range surveillance. As a result, passers-by and vehicles could be viewed outside the college premises.

The Commissioner decided that the respondent had implemented corrective measures to safeguard privacy rights, namely posting the proper signage to inform all the college's users of the presence of CCTV cameras. That was in compliance with sections 22, 23, 24, 25, 26, 27, 28, and 29 and Part VI of the Data Protection Act. Moreover, the enforcement notice served to the respondent had been observed by her.

Like the previous decision, the Commissioner properly applied some of the rules in the 'Guidelines to regulate the Processing of Personal Data by Video Surveillance Systems–Volume 5' although without express reference to it. However, in this particular complaint the Commissioner found sufficient evidence to incriminate the respondent. Yet she avoided reaching such a conclusion. Although not specifically stated, this may be partly due to the Commissioner's acceptance of the respondent's defence of 'no malicious intention to invade the privacy rights of the complainant and/or neighbours'. Instead, she decided that the respondent had implemented corrective measures and complied with the enforcement notice. It is also important to note that this is the only complaint in which the Commissioner had used the enforcement notice to make the respondent compliant with the provisions of DPA.

In *Complainant v Respondents 1 and 2*[15] the complaint was about unauthorized marketing by short service message (SMS). In this matter it was alleged that the complainant received an SMS on his private mobile phone number reading as follows: 'INVEST IN LAND. Buy land on the heights of Les Marianes. Show day 19 December from 14h30 onwards. Phone [respondent 1] for more info: . . . '. The SMS was sent to the complainant, an officer working with the Office of Data Protection Commissioner, without his consent. The complainant's number was private and registered on his name at Orange Mauritius Telecom. He requested an enquiry by the Commissioner as to how the leaking of his private mobile number had taken place.

13 Ref.No: PMO/DPO/DEC/2 (lodged on 8 November 2010, decided on 25 April 2011).

14 Ref.No: DPO/DEC/4 (lodged on 13 April 2011, decided on 5 August 2011).

15 Ref.No: DPO/DEC/3 (lodged on 17 December 2010, decided on 26 June 2011).

The Commissioner found that it was proved beyond reasonable doubt that the SMS complained about was sent through a genuine error to the complainant on his mobile and was not meant to cause any prejudice to him. Nevertheless, she required both respondents to carry out direct marketing activities in compliance with the requirements of the DPA, particularly Part IV. She also required respondent 1 to provide a more user friendly and efficient marketing system where the option to deregister or opt-out was incorporated in the SMS (containing the advert) itself before sending. The Commissioner required respondent 1 to envisage opt-in consent to confirm express consent of the customers electronically together with the signing of the appropriate consent forms as already catered for by him. Respondent 1 was similarly required to comply with the principle of purpose specification and security. Moreover, respondent 2 was required under section 27 of the DPA to enter into a contract with the data processor, that is, respondent 1, which stipulates that the latter would only act on instructions received from the data controller, that is, respondent 2, and was bound by the obligations devolving on the data controller. The complaint was thus set aside for the above legal conditions to be fulfilled.

The Commissioner's findings in this instance do not refer or in any case take into account the provisions of 'A Practical Guide for Data Controllers & Data Processor—Volume 1' regarding direct marketing. As a result, her decision is fundamentally inconsistent with her own guidelines. It is particularly significant to note that the Commissioner has complicated the data subject's requirement of consent in the context of direct marketing. Whereas in the Practical Guide she was prepared to accept 'passive consent', that is failure by the data subject to 'tick a box' marked 'opt-out' in compliance with the provisions of the DPA, in the present decision she insisted on express consent. Moreover, the Commissioner's view, that the express consent already obtained by respondent 1 in duly written forms was to be complimented by electronically 'opt-in' consent to confirm the previously obtained consent, raised the standard too high. It can be argued that the two-stage consent approach may not be in compliance with section 24(1) of the DPA which imposes a duty on data controllers and processors to obtain 'express consent' before processing personal data. This provision or section 30 of the DPA does not impose an extra duty to 'confirm consent' by obtaining another 'express consent' in respect of the same personal data and for the same purpose. However, a direction to include an option to deregister in the marketing SMS itself is plausible and user friendly.

It is interesting to note that in the present complaint the Commissioner found sufficient evidence that respondent 1 had used the complainant's private mobile phone number without his consent. Surprisingly, in her decision, she avoided expressly ruling so. Instead, she applied the standard of proof of 'beyond reasonable doubt' to the respondents' defence. Accordingly she was prepared to accept 'genuine error' as a defence to mitigate the effect of the unlawful use of someone's private mobile phone number.

This complaint also demonstrates the possibilities of conflicts of interest surrounding the functions and powers of the Commissioner. As alluded to, the complainant in the present complaint was an officer working in the Data Protection Office. To partly resolve the conflict of interest, the Commissioner delegated her powers to investigate to another person. While this is a commendable approach, it has to be noted that the same Commissioner proceeded to decide the complaint. It is not clear how she dealt with the issues of conflict of interest at the decision stage. It is submitted that merely working together with the Commissioner may not necessarily prevent the latter from deciding a complaint involving a co-employee.

A similar dispute involving unlawful disclosure of personal data by unauthorised marketing by SMS is *Complainant v Respondent.*[16] The complainant alleged that he received an unsolicited SMS on his mobile phone number. The SMS was sent to him after the mobile phone service provider had disclosed his personal information to an unauthorized third party.

The Commissioner decided that there was evidence on record to suggest that an offence of unlawfully disclosing the mobile number of a subscriber to a third party under section 29 of the DPA may have been committed. Such an offence is punishable by a fine not exceeding RS200,000 and a term of imprisonment not exceeding 5 years. Accordingly, the Commissioner referred the matter to the police under section 20 for further investigation and possible prosecution. This decision is a landmark one in the sense that the Commissioner was direct in the exercise of her powers.

Somewhat similar to the preceding two decisions is *Complainant v Respondent.*[17] The complaint concerned unauthorized marketing by phone. The complainant

16 Ref.No: DPO/DEC/8 (lodged on 28 June 2011, decided on 12 June 2012).

17 Ref.No: DPO/DEC/5 (lodged on 17 December 2010, decided on 17 August 2011).

alleged that he received a call from someone claiming to be calling on behalf of the respondent from telephone number [...]. The person calling said to the complainant that he got the complainant's number from Orange (a telecom company in Mauritius). He also claimed that the complainant was very lucky to have won a 50 per cent discount on the training courses the respondent was offering. The complainant stated in his complaint that he had never played any game to receive that discount nor had he granted written authorization to Orange to disclose his private phone number to any third party. On the base of that, the complainant requested the Commissioner to investigate how the leaking of his private mobile number had taken place.

The Commissioner decided that it was proved beyond reasonable doubt that the call was made to the complainant on his mobile by the respondent. She required the respondent to carry out his marketing activities in compliance with the relevant provisions of the Data Protection Act particularly Part IV. Similarly the Commissioner required the respondent to provide a more user friendly and efficient marketing system whereby the option to deregister or opt-out is given whilst securing the written consent of the customers for marketing. Moreover, she directed that consent collected should not be used for any purpose incompatible with the original purpose. The respondent was also required to ensure that appropriate security and organizational measures are taken to protect the personal data of customers.

It can be noted from this decision that the Commissioner required only 'express consent' as opposed to both 'express consent' and confirmation of the previous consent by an 'opt-in' option as in the third decision. Therefore while the two complaints are similar, the level of consent required has not been consistent. Moreover, contrary to the Practical Guide, where it is provided by the Commissioner that express consent may be oral or written, in the present decision she insisted that written consent must always be given. It is also important to note that, although the Commissioner found the respondent incriminated by evidence, she did not say so expressly. Instead, she proceeded to direct corrective measures. Lack of awareness or rather ignorance of the law pleaded by the respondent might have influenced the Commissioner not to deal strictly with the respondent. However such a defence raised by the respondent had not been expressly considered.

In *Complainant v Respondent*[18] the complaint alleged unauthorized use of private e-mails. It was lodged by anonymous data subjects. The allegations were that the respondent had emailed symbolic pictures of a religious nature to several persons. For that, he had used complainants' e-mail addresses without their authorization. The complainants alleged further that the respondent used their e-mail addresses allocated to them by the organizations they were working for and as such he divulged their private addresses and infringed their right of privacy.

The Commissioner decided that it was proved beyond reasonable doubt that the respondent was not aware of the implications of sending the e-mail addresses of third parties to unauthorized recipients and there was no mala fides involved in his action. The enquiring officers informed him of such implications.

This decision is the first in which the Commissioner expressly accepted a lack of awareness of the provisions of the Data Protection Act (ie ignorance of law) as a defence for the unlawful processing of personal data. Yet, in the first annual report of 2009, the Commissioner maintains that ignorance of the obligations under the DPA is not a legitimate excuse, especially given the fact that data protection obligations are more often simply just a question of adopting good civilian manners.[19] She similarly accepted a lack of malicious intention to harm anybody as a defence. It is also interesting to note that, as in the third decision, the Commissioner directed herself on the respondent's defence rather than focusing on the merit or otherwise of the complaint.

In *Complaint v Respondents 1 and 2*,[20] the complaint concerned the use of personal data in the context of a debit/credit card. The complainant alleged that respondents 1 and 2 stored his debit/credit card details during a purchase transaction at the Point of Sale (POS).

The Commissioner decided that it was proved beyond reasonable doubt that respondents 1 and 2 displayed the required effort to remedy the potential dangers of the personal information of customers being used for illegal transactions by adopting appropriate security and organizational measures. However, she required the respondents to show compliance with international and local standards by ensuring that per-

18 Ref.No: DPO/DEC/6 (lodged on 18 February 2011, decided on 26 August 2011).

19 Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009–February 2010, p. 42.

20 Ref.No: DPO/DEC/7 (lodged on 7 June 2011, decided on 14 May 2012).

sonal information as identified above are not kept illegally.

In *Complainant v Respondent*[21] the complainant alleged unauthorized use of a password. The facts of the complaint were as follows. The complainant was an employee of the respondent. Originally the complainant wrote an anonymous letter to the Commissioner alleging receiving unsolicited e-mails to her office e-mail address. Those e-mails contained symbolic pictures of a religious nature and were similarly sent to several persons using their e-mails without their authorization. The complainant alleged that the respondent divulged the private e-mails allocated to employees including her, to unauthorized third parties copied in the same e-mail. On this account, she was suspended from her post by the respondent alleging that the letter of complaint sent to the Commissioner was not authorized by the respondent. Hence it was prejudicial to the respondent.

The Commissioner decided that first, there is no legal requirement in the Data Protection Act which obligates all complainants wishing to lodge a complaint with the Commissioner to inform and obtain the permission of management. Second, the Commissioner decided that a password given to an employee is her personal data. The complainant could not be responsible for unauthorized use of her password which was at the same time known to the IT department. Finally, the Commissioner made a number of orders to the respondent to comply with security measures under section 27 of the DPA. In the above decision, the Commissioner did not only confine herself to the interpretation of the DPA, but also the Constitution of Mauritius and the Employment Rights Act.

The tenth complaint is *Complainant v Respondent.*[22] This was about the unauthorized disclosure of personal data. Similar to the previous decision, the present decision arose in the context of employer–employee relations. The complainant, the employer, alleged that the respondent, an employee, forwarded personal data from her office e-mail to her personal e-mail address. The forwarded files contained pay roll details, employees' names, salaries, salary amount, car allowances, overtimes, loans, and transport.

An investigation by the Commissioner revealed that the respondent was required to handover her duties to the complainant as her employment with the complainant was ending. She forwarded the files to her personal e-mail address as the office e-mail was inaccessible outside the office. Yet, she had to complete her duties at home.

The Commissioner decided that an employee should seek the authorization of her employer before transferring confidential information from her office e-mail address to her personal e-mail address. However, in this particular matter the Commissioner found that since the respondent had not used the information for illegal purposes but only for work purposes and in the benefit of the employer (ie complainant) in accordance with the section of 'required confidentiality' in the contractual agreement, and has already resigned from the company, she has not committed any offence under the Data Protection Act. The Commissioner also took in account the fact that no mala fide or criminal intent was detected from the respondent during the enquiry.

It is interesting to note that the Commissioner's decision in this complaint was not directly based on the Data Protection Act and its regulations. Her decision was based on the interpretation of the confidentiality clause in the respondent's employment contract.

Summary of the ten decisions

An overview of the Commissioner's ten decisions reveals the following common trends. First, in all the complaints the standard of proof is beyond reasonable doubt. However, it is less clear who primarily bears the burden of proof. Also less obvious is the criterion for the shifting of this burden. Second, the Commissioner has not strictly enforced the provisions of the DPA. In most cases she has resisted making an express finding of infringement of the provisions of the DPA even if that was the case. This is partly because many data controllers and processors in Mauritius are not aware of their obligations, suggesting a reason why the Commissioner has accepted ignorance of the law and/or a lack of awareness of the provisions of the DPA as a defence. Third, there are no formal definitions of complaint outcomes. More often the Commissioner concludes her decision by 'setting aside' a complaint. Yet 'set aside' is not clear as sometimes it appears to mean the complaint is not found, hence it is dismissed or it has been resolved. Therefore, it is difficult to readily ascertain the outcomes of such complaints. It is submitted that consistency in reporting the outcomes of complaints is required. This also needs to be made around formalized definitions which explain the meaning of complaint outcomes (resolved, settled, dismissed,

21 Ref.No: DPO/DEC/9 (lodged on 22 September 2011, decided on 12 July 2012).

22 Ref.No: DPO/DEC/10 (lodged on 3 October 2011, decided on 19 July 2012).

withdrawn, etc.). Fourth, the current way of anonymizing parties to the complaint is somewhat confusing. Parties appear to be the same in most complaints. This may cause difficulties for properly distinguishing these decisions. An alternative way of achieving anonymity while maintaining some degree of identification for distinguishing decisions is to refer to the names of parties by initial capital letters of their first names (eg Z v P). Also important in the citation of decisions is to add the year of the decision. Fifth, in all ten decisions, the Commissioner has not explained to the parties their right of appeal to the ICT Appeal Tribunal, as is required under section 11(b) of the DPA. It is not certain whether the Commissioner has been using a different method to notify the parties of this right. The Commissioner had confirmed that none of her decisions were appealed to the ICT Appeal Tribunal partly because parties were satisfied by the Commissioner's decision.[23] However, one point has to be made clear. None of the above ten decisions ended with settlement. Hence the signed declarations by parties in the Commissioner's decisions that they consented for a site visit, were satisfied with the way the complaint and/or investigation were handled do not qualify as settlement to bar appeals. It is imperative to note that the Commission's website is not linked to the website of the ICT Appeal Tribunal. This makes it difficult to ascertain if there is any appeal in the Tribunal arising from the Commissioner's decision. However, the strategies employed by the Commissioner to require parties to make written declarations as to their satisfaction with the outcomes of the investigation and the decision offer solid grounds to believe that no appeal has ever been referred to the ICT Appeal Tribunal. Such declarations, to say the least, have largely headed-off any possibility of appeal.

It can be submitted that most of the problems enumerated above are largely caused by the absence of regulations on proceedings of the Commission in determining complaints. In connection with this, the Commissioner once observed that section 11 of the DPA simply provides for investigation of the complaint, notification to the complainant in writing of her decision and information about the appeal to the ICT Appeal Tribunal.[24] 'There is no provision in the Data Protection Act on the manner in which a hearing may take place and the evidences to be submitted before the Commissioner . . . '[25]

Future trends

Despite their pitfalls in some places, the decisions of the Commissioner provide a fertile ground for the consolidation of data protection practices. As one may notice, in the last three decisions, the Commissioner has started to unfold her powers. Perhaps this is because a considerable period has passed since the Mauritius Data Protection Act came into force, suggesting that data controllers and processors are somewhat familiar with the requirements imposed upon them by the Act. Perhaps also, this is due to the fact that the Commissioner had made considerable efforts to bring the law to the knowledge of the public (controllers, processors, and data subjects) through presentations, leaflets, seminars, and workshops. Since Mauritius is currently seeking EU accreditation of its data protection system, the Commissioner is likely to continue to tighten her grip in making bold decisions to instil confidence in the European Union that the data protection regime is adequate.

doi:10.1093/idpl/ips038

23 Interview by the author of this article and the Mauritius Data Protection Commissioner, Port Luis, Mauritius, 4 July 2011(note that little is known about decisions which were decided after the date of this interview). However, there are solid grounds to believe that no appeal has ever been referred to the ICT Appeal Tribunal as explained in the article.

24 Mauritius Data Protection Office, First Annual Report of the Data Protection Commissioner February 2009–February 2010, p. 14.

25 Ibid.