Republic of the Philippines
NATIONAL PRIVACY COMMISSION

In Re: DATA BREACH INVOLVING THE COMELEC DATA PROCESSING SYSTEM IN WAO, LANAO DEL SUR
x----------x

NPC CID Case No.: 17-002
For: Violation of the Data Privacy Act f 2012

DECISION

PATDU, D.P.C.

Before this Commission is a reported Personal Data Breach involving the Commission on Elections ("**COMELEC**") data processing system in Wao, docketed as NPC Case No. 17-002.

COMELEC reported that on 11 January 2017, a desktop computer of the Office of the Election Officer ("**OEO**") of Wao, was stolen by unidentified persons. The desktop computer contained, among other applications, the Voter Registration System ("**VRS**") and the Voter Search ("**VS**") program that utilize the data stored in the National List of Registered Voters ("**NLRV**").

COMELEC notified this Commission about the possible personal data breach through electronic mail on 28 January 2017. The notice to this Commission, included the following statement:

> *"At the outset, the undersigned respectfully informs the NPC that, as a security feature, all data encoded in the computers of all OEOs are already encrypted in AES 256, and that the portable hard disk containing said data are likewise encrypted. Upon completion of the on-going investigation being conducted to determine the scope, including the measures undertaken and still to be undertaken to address and reduce the consequences of such breach, if any, the COMELEC shall be providing the NPC with a detailed report on the matter once all data relative*

> *thereto shall have become available. For the meantime, the COMELEC respectfully requests an extension of time to comply with such notifications.*

The initial notification was followed by another report dated 03 February 2017. From the submissions, this Commission found out that the VRS contained a total of 58,364 registration records for the Municipality of Wao. 40,991 of said records (as of 19 October 2016) are intended for the Barangay elections, and 17,373 (as of 13 September 2016) are for the Sangguniang Kabataan ("**SK**") elections. 35, 491 of the Barangay elections data are active voters, while 5,500 are deactivated voters. 17,336 of the SK elections data are active voters, while 37 are deactivated voters.

The NLRV, on the other hand, contains approximately 75,898,336 records as of 17 October 2016. 55,195,674 of which are active voters and 20,703,662 are deactivated voters.

COMELEC also reported on actions they have taken, and other measures for implementation following the incident.[1] For instance,

---

[1] According to COMELEC, part of the measures that have been implemented and/or still for implementation are the following:
Measures already taken:

1. Memorandum dated 23 January 2017 called for installation of CCTV cameras in all field offices, including the hiring of a consultant for the Data Privacy Act compliance.
2. Memorandum dated 01 February 2017 prescribed the interim security measures and controls that will secure and prevent loss, destruction, unauthorized access and misuse of data pending issuance of the key policies related to data security, use, processing, storage and disposal.
3. Conduct of training-seminar on the Data Privacy Act.

Measures to be undertaken:

1. Use of biometrics by the accountable officers to gain access to the VRS and NLRV. The COMELEC Information Technology Department ("**ITD**") has been directed to develop an application on the matter.
2. Limit the number of personal data in the NLRV deployed in the local field offices and overseas posts. Also under development is the patch that will delete and wipe-out the NLRV storage devices in the offices of the election officer.
3. Drafting of the rules and guidelines on limiting the use of the VS and NLRV in the local field offices to eighty-one (81) Provincial Election Supervisors only, instead of one thousand, six hundred fifty-six (1,656) election officers.
4. Streamline registration forms to cover only personal data required by law (R.A. No. 8189).

COMELEC reports that the security feature, encryption in AES 256, of the fields containing personal information has already been implemented since 17 October 2016.

Considering the seriousness of the possible data breach, involving personal data of millions of Filipinos, and the delay in notification, this Commission conducted further investigations on the circumstances surrounding the personal data breach.[2]

Specifically, an Order for On-Site Examination of Systems and Procedures, dated 07 February 2017, was issued to assess risks to data subjects in a selected field office of COMELEC. The observation and inspection of the personal data processing procedures were carried out at the COMELEC facilities in Taguig City on 08 February 2017.

This Commission, through its investigating officer, also completed a preliminary investigation, where a recommendation for criminal prosecution was made against CTL. On 9 February 2018, this Commission directed CTL to submit his Responsive Comment on the Preliminary Fact-Finding Report charging possible *Concealment of Security Breaches Involving Sensitive Personal Information*, and *Accessing Personal Information and Sensitive Personal Information Due to Negligence*.

On 13 February 2017, proceeding from the records of the Case, including the onsite examination, this Commission issued a Compliance Order mandating the COMELEC to:

---

5. Execution of Non-Disclosure Agreements ("**NDA**") with the Job Orders/Contract of Services personnel authorized by the Commission En Banc to be hired. Said NDA shall likewise apply to regular employees of departments and offices that have personal data in their custody.
6. Execution of Data Sharing Agreements with Law Enforcement Agencies.
7. Submission to the Commission En Banc, for its approval, of a Notice to be incorporated in documents containing data requested by data sharing agencies.
8. Drafting of the key policies on the compliance requirements of the Data Privacy Act, for approval by the Commission En Banc.
9. Nationwide training of all the field officials on Data Privacy Act compliance, including the integration of such compliance requirements during the orientation of newly hired employees.
10. Finalization of the Privacy Impact Assessment, for submission to the Commission on or before 27 February 2017.

[2] Rule IX, Sec. 38(c) of the IRR of the DPA

1. Erase all National List of Registered Voters in the computer system in the different municipalities and cities, if it cannot be secured using appropriate organizational, physical and technical security measures;

2. Notify data subjects affected by the personal data breach as soon as possible, but not to exceed two weeks;

    a. Notification by publication in two newspapers of general circulation will be allowed for individuals with records in the National List of Registered Voters (NLRV);
    b. Individual notification for the individuals with records in the Voters Registration System (VRS) in the Municipality of Wao, in accordance with NPC Circular 16-03 on Personal Data Breach Management;

3. Submit to the National Privacy Commission proposed and implemented revisions in the voter registration process, taking into account the Data Privacy Act, its Implementing Rules and Regulations, and related Issuances of the Commission in two weeks;

4. Include in the submission the status of implementation of part III "Measures Taken to Address the Breach" of the Report on this personal data breach dated February 3, 2017 submitted by the Commission on Elections;

5. Submit a Compliance Report within 15 days from receipt of this Order.

In compliance to the above Order of this Commission, COMELEC submitted its Compliance Report on 28 February 2017.[3] COMELEC

[3] In response to the order to submit proposed and implemented revisions in the voter registration process in view of the DPA, COMELEC submitted a draft of the Policy on Field Office Systems outlining the policy on data privacy, security and protection; and a draft of the Resolution to align changes in the VRS and the VS with the General Instruction on the conduct of the system of continuing registration of voters.

COMELEC also reported the following: approval on the budget for the installation of CCTV cameras; delay in hiring a consultant due to low budget allocation; dissemination of Memorandum on interim security measures and controls on data processing; addition of a 1-day seminar on data privacy in their Strategic Planning Seminar attended by directors and division

reported that the COMELEC en Banc approved the modifications in both local and overseas Voter Registration Systems with the issuance of Minute Resolution No. 17-0092, dated 14 February 2017, entitled "In the Matter of the Proposed Changes on the Voter Registration System (VRS) and Voter Search Systems and Database-Updated".

As to the order to notify affected data subjects of the personal data breach, COMELEC reported the publishing of notifications for individuals whose records are included in the NLRV in two newspapers on 24 February 2017. COMELEC also reported shipping individual notifications to those individuals included in the VRS of Wao and the completion of personal delivery to affected voters on 27 February 2017.

On 15 March 2018, this Commission received CTL Responsive Comment on the Preliminary Fact-Finding Report, presenting his defenses to the issues raised before this Commission.

Issues

What remains for Resolution before this Commission are:

1. Whether there was negligence in the safekeeping of the desktop that contained the personal data of registered voters

2. Whether there was concealment of the personal data breach by failing to notify the Commission and the data subjects affected.

Decision

---

chiefs; directive to use biometrics to gain access in the VRS and the VS; development of application to limit the number of personal data in the NLRV and the deployment of application to wipe-out the NLRV from storage devices in the offices of the election officer; finalization of rules and guidelines on limiting the use of VS and NLRV in the local field offices; streamlining of the registration forms to cover only personal data required by Republic Act No. 8189; execution of Non-Disclosure Agreements with COMELEC personnel; planned execution of Data Sharing Agreements with Law Enforcement Agencies; incorporation of Notice in all documents requested by data-sharing agencies; drafting of a Data Privacy Manual; nationwide training of all field officials on DPA compliance; submission of Privacy Impact Assessment to NPC; meeting with PNP to discuss security concerns of COMELEC field offices; the publishing of the required notification to affected data subjects in two newspapers of general circulation and the completion of personal delivery of individual notices to affected data subjects in Wao, Lanao del Sur.

1. Negligence in the safekeeping of the desktop computer that contained the personal data of registered voters.

On 15 March 2018, CTL submitted his Responsive Comment to the Preliminary Fact-Finding report denying the allegation of negligence in the safekeeping of the desktop computer containing personal data of voters. He averred to have implemented physical security measures such as causing the installation of padlocks to every point of ingress and egress of the office. To support his defense, he attached to his Comment photographs of the whole office building where the COMELEC office in Wao is located, and of all doors and windows of the office showing that padlocks were properly installed. Moreover, he maintained that he assigned his casual employee, to make sure that all points of entry and exit, including the windows, are locked before the last person leaves the office. A sworn affidavit of the casual employee is also attached to his Comment attesting to this claim. CTL maintains that what took place at the COMELEC office in Wao was a robbery with force upon things, whereby the robber gained entry by destroying the back window. He asserted that said robbery was beyond his control.

Section 20 of the DPA mandates personal information controllers (PICs) to implement reasonable and appropriate organizational, physical and technical security measures to protect personal information against natural and human dangers. What is reasonable and appropriate in a given circumstance is determined, in part, by the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practice, the cost of security implementation and relevant guidelines issued by this Commission. There is negligence if there is failure to implement such reasonable and appropriate security measures.

In this case, CTL cannot be said to have been negligent in implementing reasonable and appropriate security measures to prevent the taking of the desktop computer containing voter personal data. Just like what a reasonable and prudent man would have done to secure the computers inside the office, CTL placed padlocks and gave instructions to make sure that all doors and windows are locked at the end of the working day. He also installed

a strong password to said desktop computer and only he and his casual employee knew the said password. The robbery was committed with force upon things, implying that the perpetrator had to break the locks and force his way through the back window into the office of the Election Officer. Further, COMELEC, in their personal data breach report to this Commission, maintains that technical security measures are in place to limit access to the VRS program in the desktop computer and that the VRS and the NLRV data are encrypted in AES 256.

Considering the submissions of COMELEC to this Commission, and the continuing efforts to strengthen its security measures, this Commission holds that the evidence is insufficient to warrant criminal prosecution for providing access due to negligence.

2. Concealment of the Personal Data Breach.

The reported robbery of the COMELEC field office in Wao, happened on 11 January 2017. COMELEC notified this Commission of the personal data breach only on 28 January 2017.

Section 20 Chapter V on the Security of Personal Information of the Data Privacy Act of 2012 provides:

> ***Section 20. Security of Personal Information.*** –
>
> *xxx*
>
> *(f) The personal information controller shall* ***promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person****, and the personal information controller or the Commission believes (that such unauthorized acquisition is likely to give rise to a real risk of serious harm*

> *to any affected data subject. Xxx (Emphasis supplied.)*

The Implementing Rules and Regulations and NPC Circular 16-03 defined what constitutes prompt notification. That is, notification of personal data breach shall be within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

The IRR allows delay in the notification to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

In the events leading to the loss of the computer, COMELEC narrated in their breach notification that the loss was discovered at around 8:00 am of 12 January 2017 by MTA, a Job Order casual employee of the Local Government Unit detailed at the COMELEC field office. On the same day, CTL informed, in writing, NDY of the robbery incident and the loss of the desktop computer. The incident was also reported to the Wao police, who immediately conducted its initial investigation of the case.

Upon ascertaining the possibility of a personal data breach, COMELEC ITD issued a memorandum on 24 January 2017 addressed to Executive Director/ Data Protection Officer JMT, advising him that since the lost computer contained personal information, notice of such loss should be submitted to the NPC and affected data subjects. JMT received the memorandum on 26 January 2017. He then immediately submitted the required notification to this Commission two days later on 28 January 2017. COMELEC communicated that its mindset was on the operational aspect of the registration process, thus immediate action was taken to replace the lost computer to ensure the resumption of the conduct of continuing registration of voters in Wao. They also emphasized the implementation of security measures. COMELEC believes that the unauthorized acquisition of the personal data in the desktop computer would not likely present a real risk of serious harm to those affected because of the existing security measures. The VRS is protected from any unauthorized

person gaining access to the program. Further, the VRS and the NLRV data are encrypted at par with the standard set by this Commission. It would require a certain degree of technical skill and decryption capability in order to extract the VRS and NLRV data from the desktop computer. There is low probability that real risk of serious harm would befall data subjects because of the security measures in place.

From the records of the case, and considering that NPC Circular 16-03 took effect only on January 13, 2017, or two days after the incident in Wao, this Commission finds that the delay in notification for the particular circumstances in this case do not amount to concealment as defined in the Data Privacy Act.

Section 30 of the DPA provides:

> *SEC. 30.* ***Concealment of Security Breaches Involving Sensitive Personal Information. –*** *The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.*

CTL reported the incident to his superiors on the same day that the robbery was discovered. Indeed, the determination of the scope of the breach should have been completed faster, and notification of the Commission should have been immediate based only on available knowledge. While COMELEC claims that the security measures are adequate considering the use of encryption and other safeguards, it should have been more circumspect. Such assertion by itself is inadequate basis to support the assumption that notification is not necessary. We take notice, however, that guidelines such as the factors to consider in determining necessity of notification have been provided only in NPC Circular 16-03.

In sum, this Commission finds that there is insufficient evidence to recommend the prosecution of the responsible officers of COMELEC or CTL for the crimes of Access due to Negligence under Section 26, or Concealment of a Security Breach under Section 30 of the Data Privacy Act of 2012.

This Commission considers, however, the need to ensure that existing policies on data privacy and data security are operationalized not just in the Central Office of COMELEC but also in regional and local field offices as well. It is not sufficient to provide documentation of compliance with the DPA, rather, it must be integrated in daily operations and data processing activities. While the evidence is not sufficient to warrant criminal prosecution, COMELEC must be able to demonstrate compliance with the DPA.

The National Privacy Commission is mandated, under the DPA, to protect personal information. To this effect, NPC Circular 16-03 on Personal Data Breach Management provides guidelines to help PICs prevent and properly manage such breaches when they occur. Further, Section 9 of the same Circular provides for a procedure for post-breach review for the purpose of improving the personal data breach management policies and procedures of the PIC:

> ***SECTION 9. Documentation.*** *All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:*
>
> *A. Description of the personal data breach, its root cause and circumstances regarding its discovery;*
> *B. Actions and decisions of the incident response team;*
> *C. Outcome of the breach management, and difficulties encountered; and*
> *D. Compliance with notification requirements and assistance provided to affected data subjects.*
>
> *A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of*

> *the personal information controller or personal information processor.*

In order to ensure that existing breach management policies and procedure are being implemented, this Commission finds it necessary to further require COMELEC to submit its post-breach review report.

WHEREFORE, premises considered, **the COMMISSION ON ELECTIONS** is **ORDERED** to SUBMIT to this Commission, within thirty (30) days from receipt of this Decision:

1. The Designation of Data Protection Officers/ Compliance Officers for Privacy for every Regional Unit and the names and contact information thereof;

2. A copy of its Security Incident Management Policy, pursuant to Sections 4 and 5 of NPC Circular 16-04, including documents demonstrating:

    a. Creation of its Breach Response Team, and the composition thereof;

    b. Dissemination of this Security Policy to all election field offices;

3. Complete Post-Breach Report on its management of this Personal Data Breach in compliance with Section 9 of NPC Circular 16-03.

SO ORDERED.

Pasay City,
15 August 2019.

(Sgd.)
IVY D. PATDU
Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

JMT
Commission on Elections

CTL
Wao

(x) LEGAL AND ENFORCEMENT OFFICE

(x) GENERAL RECORDS UNIT