Inspection Report

(Published under Section 48(1) of the Personal Data (Privacy) Ordinance)

Personal Data System of the Registration and Electoral Office

Report Number: R23 – 1738

Date of Issue: 20 September 2023

Personal Data System of the
Registration and Electoral Office

Section 36 of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that:

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of –*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations –

(i) to –

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "personal data system" is defined in section 2(1) of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system*".

Section 48 of the Ordinance provides that:

"*(1) ... the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report –*

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection

principles, by the class of data users to which the relevant data user belongs; and

(b) in such manner as he thinks fit."

This inspection report is hereby published in the exercise of the powers conferred under section 48(1) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
20 September 2023

Inspection Report

(Published under Section 48(1) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong)

Personal Data System of the Registration and Electoral Office

Background

1. Since 2017, there have been repeated data breach incidents relating to the personal data held by the Registration and Electoral Office (the REO), and the Office of the Privacy Commissioner for Personal Data (the PCPD) has conducted four investigations[1] in relation to the security of the personal data kept by the REO. The data breach incidents involved, among others, the loss or inadvertent disclosure of the personal data of over 3 million electors and a number of Election Committee members. Each of the incidents attracted considerable media attention and criticism from the public.

2. Against this background, and given that the REO possesses and handles a huge amount of personal data of sensitive nature, the Privacy Commissioner for Personal Data (the Privacy Commissioner) considers that it is in the public interest to carry out an inspection of the personal data system used by the REO under section 36(a) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) (the Inspection) with an aim to strengthen the protection of personal data in the possession of the REO and to prevent the recurrence of data breach incidents in the future.

[1] The relevant investigation reports are as follows:

Registration and Electoral Office – Two Personal Data Breach Incidents
https://www.pcpd.org.hk/english/enforcement/commissioners_findings/files/r22_4116_e.pdf
Registration and Electoral Office – Loss of a Marked Final Register of Electors
https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R19_5120_Eng.pdf
Registration and Electoral Office – Loss of Notebook Computers Containing Personal Data of Election Committee Members and Electors
https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R17-6429_Eng.pdf

Objectives and Scope of the Inspection

3. The purposes of the Inspection were to identify any deficiencies or vulnerabilities in the personal data system of the REO which may expose, or potentially expose, the personal data held by the REO to cyberattacks, system misconfigurations, losses of physical documents or portable devices, inadvertent disclosure by email or by post, etc., to identify possible areas in which to strengthen the protection of personal data, to raise and promote awareness of data security among the REO's staff, and to assist the REO in better complying with the requirements of the Ordinance with regard to the security of personal data to prevent the reoccurrence of data breach incidents.

4. Following the data breach incident of the REO in March 2022, a working group was formed by the Constitutional and Mainland Affairs Bureau, the Office of the Government Chief Information Officer (OGCIO) and the REO to conduct a comprehensive review of the information security of the REO from April to June 2022. Upon completion of the review, the OGCIO provided the REO with a review report setting out its recommendations on ways to enhance the levels of cyber security and the REO's resilience to cyber risks (the Review Report). To avoid duplication of effort, the areas covered in the Review Report were excluded from the Inspection.

5. The Inspection covered the following areas:

(i) The REO's Privacy Management Programme Manual (the PMP Manual);
(ii) Relevant policies and measures (other than IT security measures covered by the Review Report) in place regarding the security of personal data;
(iii) Relevant policies and procedures for handling personal data under the REO's information systems;
(iv) The practices for handling data breaches, including incident response mechanisms; and
(v) Staff awareness of and training on the protection of personal data.

Requirements under the Ordinance

6. The Ordinance governs the collection, processing, holding and use of personal data. The REO, being a data user under the Ordinance, is obliged to comply with the requirements under the Ordinance, including the six Data Protection Principles (DPP) of Schedule 1 to the Ordinance. Regarding the security of personal data, DPP 4(1) requires that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use, having particular regard to –

   (i) The kind of data and the harm that could result if any of those things should occur;
   (ii) The physical location where the data is stored;
   (iii) Any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
   (iv) Any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
   (v) Any measures taken for ensuring the secure transmission of the data.

7. In addition, DPP 4(2) requires that if a data user engages a data processor (whether within or outside Hong Kong) to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

8. With regard to the retention of personal data, DPP 2(2) requires that all practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used. Section 26(1) of the Ordinance further provides that a data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless (a) any such erasure is prohibited under any law or (b) it is in the public interest (including historical interest) for the data not to be erased.

Methodology

9. To inspect the personal data system of the REO and examine how staff members effectively comply with the PMP Manual, data security policies and practices, the Inspection Team[2] carried out the Inspection which lasted from August 2022 to April 2023, during which the Inspection Team obtained six batches of written submissions which contained over 4,800 pages of documents from the REO, including copies of its relevant policies, manuals, guidelines, training materials and copies of service contracts between the REO and data processors.

10. The Privacy Commissioner exercised her power of entry on premises under the Ordinance to conduct on-site visits. With the agreement of the REO, the Inspection Team conducted five visits to various divisions and teams of the REO between January and February 2023 to:

    (i) carry out face-to-face interviews with the personnel responsible for overseeing the implementation of the PMP Manual and management of the REO's personal data system;
    (ii) interview staff members ranking from directorate officers to operational staff to obtain details of the actual operation of personal data handling and to understand staff members' knowledge of the PMP Manual, internal policies and guidelines and data protection training;
    (iii) inspect the REO's demonstration of the operation of its personal data system, including the REO's information systems, the procedure for accessing personal data and the management procedures concerning access control of the REO's information systems by members of staff; and
    (iv) inspect the locations for the storage of personal data and the security measures adopted for the storage of personal data.

[2] The Inspection Team consisted of one Chief Personal Data Officer, one Senior Personal Data Officer, two Personal Data Officers and one Assistant Personal Data Officer.

Key Findings

11. This report is based on the information provided by the REO and the matters that came to the Inspection Team's attention during the on-site visits. The legal obligation to comply with the requirements under the Ordinance rests with the REO. The findings and recommendations made in this report do not in any way affect or prejudice the Privacy Commissioner in exercising any powers or performing any functions under the Ordinance.

(I) The PMP Manual

12. The Privacy Commissioner is pleased to note that the REO has embraced the protection of personal data as a part of its data governance by adopting the personal data privacy management programme (the PMP) and has developed the PMP Manual based on its organisational structure and operations. The Privacy Commissioner considers that the PMP Manual has included all components as recommended by the PCPD in the "Privacy Management Programme: A Best Practice Guide"[3] in terms of organisational commitment, programme controls, ongoing assessment and revision.

13. In terms of organisational commitment, the REO has established clear reporting mechanisms and designated a Personal Data Controlling Officer at the rank of Deputy Chief Electoral Officer to manage the implementation of the PMP and facilitate compliance with the Ordinance. Further, the REO has designated another Deputy Chief Electoral Officer to take up the role of Departmental Secretary to review the effectiveness of the PMP on an annual basis and assist the Personal Data Controlling Officer in conducting ongoing assessment and revision of the PMP Manual. The Privacy Commissioner is pleased to note that top management of the REO is committed to protecting personal data privacy in the implementation and review of its personal data policy.

14. The PMP Manual has also clearly set out the roles and responsibilities of the Personal Data Controlling Officer and other relevant officers for the

[3] https://www.pcpd.org.hk/english/publications/files/PMP_guide_e.pdf

implementation and management of the PMP. A data protection officer has been assigned to each division and/or unit to assist the Personal Data Controlling Officer and Departmental Secretary in reviewing the personal data protection measures in their respective divisions and/or units to ensure compliance with the Ordinance. The Privacy Commissioner notes that relevant staff members were familiar with their roles and responsibilities and the reporting mechanism as stipulated in the PMP Manual.

15. However, the Privacy Commissioner notes that although the PMP Manual was updated in June 2022, the REO did not make corresponding amendments or updates to the PMP Manual in relation to the amendment provisions of the Ordinance relating to doxxing, which came into effect in October 2021. The Privacy Commissioner recommends that the REO should ensure that the content of the PMP Manual is up to date to reflect any amendments to the Ordinance.

16. According to the PMP Manual, the REO reviews and updates its personal data inventory annually. Although the REO has specified the storage location of most of the personal data (e.g. the designated shared drive of a specific unit/team, the address of the office or warehouse, etc.), it was observed that the electronic storage locations of certain types of personal data marked in the inventory were vague. For example, the term "IT Systems" was used by some teams to describe the storage location of personal data. These vague descriptions could possibly cause confusion and improper storage. The Privacy Commissioner therefore recommends that the REO should state the specific electronic storage location of the personal data in the personal data inventory to facilitate good data governance and enhance transparency.

17. It is noted that the PMP Manual has briefly introduced the criteria for triggering a Privacy Impact Assessment (PIA), albeit without specifying the personnel responsible for deciding whether a PIA is to be conducted. This may lead to lapses in performing a PIA when it is warranted. The Privacy Commissioner recommends that the REO clearly set out the criteria and mechanism, including the ranking of the personnel responsible for making the decision, for conducting

a PIA in the PMP Manual to ensure that all relevant data processing activities are subject to appropriate assessment and scrutiny.

Recommendations:

(i) Ensure that the content of the PMP Manual is up to date to reflect any amendments to the Ordinance;

(ii) State the specific electronic storage location of the personal data in the personal data inventory;

(iii) Clearly set out the criteria and mechanism, including the ranking of the personnel responsible for making the decision, for conducting a PIA in the PMP Manual.

(II) Policies and guidelines which are in place governing the overall security of personal data

18. The Privacy Commissioner notes that the REO has put in place policies and guidelines which govern personal data protection and security, details of which are not set out in this report in order to maintain the confidentiality of the security measures adopted by the REO.

19. Having examined the relevant policies and guidelines, the Privacy Commissioner is pleased to note that the REO has embedded the protection of data privacy into its operations. The policies and guidelines have integrated data privacy protection and security measures into procedures relating to all the major activities of the REO from voter registration, election-related activities to the safekeeping of electoral documents.

20. To facilitate access to the policies and guidelines, the REO has stored all the policies and guidelines in a central portal accessible to all staff members. The REO circulates the policies and guidelines to all staff members through emails biannually. Regular training and seminars on data protection also have been provided to staff members to deliver training on the REO's data protection policies.

These actions demonstrate the REO's continuous efforts to ensure that its staff members are familiar with the requirements under the Ordinance and the REO's data security policies and procedures.

21. In addition to the promulgation of policies and guidelines, the REO has made efforts to facilitate staff members in better understanding the requirements of the relevant policies and guidelines regarding the security of personal data. For example, the REO devised the "End User Instructions on IT Security" to serve as a quick reference on the REO's policy on information technology security (IT Policy) and to provide practical security tips in a simple "dos and don'ts" format.

22. The Privacy Commissioner also notes that some divisions and teams of the REO have developed concise operational procedures and manuals to reflect their respective functions and responsibilities and have set out data protection requirements or tips relevant to their operations. The Privacy Commissioner is of the view that these are good practices which could facilitate staff members in understanding the policies and procedures relevant to the security of personal data.

23. During the examination of the policies and guidelines, the Privacy Commissioner noted that the REO's IT Policy has set out the requirements for asset management, which include drawing up an inventory of assets and conducting periodic reviews of the inventory to ensure that the IT equipment is properly kept and maintained. While it is noted that the REO has set up internal mechanism for conducting inventory stocktaking, the Privacy Commissioner recommends that the REO should review and update the IT policies and guidelines to specifically set out the interval and personnel responsible for conducting the inventory stocktaking of the IT equipment.

Recommendation:
(iv) Review and update the IT policies and guidelines to specifically set out the interval and personnel responsible for conducting the inventory stocktaking of the IT equipment.

(III) Physical security measures (other than IT security measures covered by the Review Report) for the protection of personal data

24. During the Inspection, the Privacy Commissioner was satisfied that the REO has generally adopted appropriate levels of security measures for physical documents and/or devices containing personal data. Details of the security measures taken are not set out in this report in order to maintain the confidentiality of these measures.

25. In addition to the responsibility for safeguarding the personal data in its possession, the REO, being the data user, should also take all practicable steps to ensure that personal data entrusted to data processors are well protected. DPP 4(2) of the Ordinance requires that if a data user engages a data processor to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. It is noted that the REO generally has adopted contractual (e.g. entering into contracts with clauses specifying the data processors' obligations to ensure data security and report any data breaches) and other means (e.g. conducting on-site inspections and supervision of the work of its data processors) to protect personal data entrusted to its data processors. The REO has also conducted annual reviews of the performance of its data processors by completing the Data Processor Review Checklists, which are reviewed by the Personal Data Controlling Officer as required in the PMP Manual. However, the Privacy Commissioner notes that in a few contracts with data processors, the REO has not specified its rights to audit and inspect the data processors on the handling and storage of the personal data entrusted to the data processors. It is also noted that the REO did not conduct site inspections in some cases. In this regard, the Privacy Commissioner recommends that the REO review all the service contracts with the data processors to include contractual terms on the REO's rights to audit and inspect how the data processors handle and store personal data and exercise its rights to conduct audits and inspections periodically.

Recommendation:

(v) Review all of the service contracts with the data processors to set out the REO's rights to audit and inspect how the data processors handle and store personal data and the REO's rights to conduct audits and inspections periodically.

(IV) Technical security measures (other than IT security measures covered by the Review Report) to protect personal data in the REO's information systems

26. The Privacy Commissioner is pleased to note that the REO has leveraged appropriate technical measures to protect personal data in the information systems of the REO. These include measures implemented to achieve secure transmission of the data (e.g. encryption of data transmitted via a secured network) and disabling the function of exporting personal data from one of the information systems. The REO has also enforced the least privilege principle when assigning the resources and privileges of information systems to users. Data access rights are granted to users based on "need-to-know" and "need-to-use" principles, and the access rights are reviewed periodically.

27. The REO's IT Policy sets out the IT security requirements for protecting all information systems and data in the REO. Having read all of the relevant documents submitted by the REO and conducted interviews with members of the REO, the Privacy Commissioner considers that the REO has established clear policy and procedures on data governance and data security, which cover the roles and responsibilities of staff as regards the maintenance of information systems and the handling of data security incidents. The REO has also provided a comprehensive guide to staff members that defines their respective roles and responsibilities in complying with the requirements stipulated in the IT Policy.

28. During the on-site visits, the Inspection Team noted that users of the REO's information systems, have separate accounts and passwords to access the functions in their respective systems. The accounts and access rights to the functions are granted to the users by the respective divisions or teams based on

operational need. Only authorised staff are allowed to retrieve or access relevant personal data in the REO's information systems. The user accounts and access rights are revoked when they are no longer required. In addition to adopting technical measures to prevent unauthorised access to information systems, the REO regularly reminds staff members of their obligations to handle personal data in accordance with the departmental circulars and not to download classified information from the REO's information systems without prior approval.

29. The REO rolled out an Electronic Poll Register (EPR) System for issuing ballot papers at polling stations in September 2021. Under the EPR System, an elector's identity card is scanned with an EPR tablet to verify that the person is a registered elector and to ascertain the types of ballot papers to be issued. Audit trails are available to log all system activities, any abnormal activities are reported. The Privacy Commissioner is pleased to note that the REO conducted a PIA with satisfactory results before launching the system. In addition, it was noted during on-site visits that the devices used to show electors' data for identity verification purposes were secured with proper security devices or measures. These measures reflect that the REO has adopted "Privacy by Design" for the EPR System.

30. The Privacy Commissioner notes that although the REO has maintained log records, and there is a policy specifies that the REO's information systems will be monitored by means of audit logging, there was insufficient evidence that the relevant units of the REO had conducted an adequate review of the log records to ensure proper usage of the systems. It is also noted that some teams did not have knowledge of whether the log records of the modules they used contained personal data. Reviewing the log records of a system containing personal data is crucial for detecting security incidents and unauthorised activities, so as to identify the root cause and prevent future incidents. The Privacy Commissioner recommends that the REO take appropriate measures to ensure that the log records are properly reviewed regularly in accordance with its own policy.

31. In addition, the Privacy Commissioner notes that some log records that contained personal data did not have defined retention periods. The Privacy Commissioner recommends that the REO should review all categories of log records to ensure

that the personal data contained in the records are retained for no longer than is necessary, thereby reducing the risk of unauthorised or accidental access, processing, erasure, loss or use.

32. The Privacy Commissioner also notes that different modules of one of the REO's information systems were owned by respective divisions that devised their own operational manuals for the system without consulting the Information Technology Management Unit (ITMU), a team that is responsible for maintaining updates of the system. The Privacy Commissioner recommends that the REO should strengthen the coordination between the ITMU and individual divisions concerning the use of the REO's information systems that contain personal data to ensure proper usage of the relevant systems.

Recommendations:

(vi) Take appropriate measures to ensure that the log records are properly reviewed regularly;

(vii) Review all categories of log records to ensure that the personal data contained in the records are properly retained for no longer than is necessary to reduce the risk of unauthorised or accidental access, processing, erasure, loss or use;

(viii) Strengthen the coordination between the ITMU and individual divisions concerning the use of the REO's information systems that contain personal data to ensure proper usage of the relevant systems.

(V) <u>The practices for handling data breaches</u>

33. The PMP Manual covers the elements of the data breach response plan and outlines its practices for handling a data breach, which encompass a set of steps and mechanisms for managing a data breach, including reporting, notification, containment, investigation and evaluation. The PMP Manual also specifies that the requirements of security incident management in another administrative circular should be followed if the incident is related to information security. The

Privacy Commissioner notes that the REO duly followed the required steps in handling the two data breaches in 2022, such as by reporting the matter to the PCPD and relevant regulatory bodies, notifying the affected individuals, investigating the data breaches and conducting post-incident reviews and adopting immediate improvement measures.

34. The Privacy Commissioner is pleased to note that the REO has committed to conducting incident response drills on information security at regular intervals after considering the relevant recommendations provided in the Review Report provided by the OGCIO.

35. As the digital age unfolds, online data breaches occur periodically. However, it is important to note that data breaches can also occur offline. In fact, of the four data breach incidents that have occurred within the REO since 2017, two were the result of the physical loss of devices or documents containing personal data.

36. In this regard, the REO is recommended to conduct data breach simulations to assess staff resilience in following the required steps when they are faced with data breaches of different natures, including the loss of physical records and/or equipment. This exercise will help identify areas for improvement and assist in fine-tuning the REO's data breach response plan.

Recommendation:
(ix) Conduct data breach drills for both information security incidents and the loss of physical records and/or equipment on a regular basis.

(VI) <u>Staff awareness of and training on the protection of personal data</u>

37. Regarding staff training, the Privacy Commissioner appreciates that the REO has put in considerable efforts to enhance staff awareness of personal data protection and security. It is noted that on top of induction trainings and regular briefings and trainings by individual divisions, the policies and guidelines related to the protection of personal data have been recirculated regularly, and posters have been

put up around the offices of the REO to raise staff awareness of the importance of data protection.

38. In relation to data security, the ITMU has issued monthly alert emails and forwards data security alert emails from the OGCIO to staff members. The Inspection Team noted that to provide prominent reminders, the REO has configured the computer workstations to show practical data protection tips on the screensavers to remind staff members about the proper handling of personal data.

39. Although the REO has the aforementioned measures in place to raise staff awareness of personal data protection and security, the effectiveness of the measures is not evident. During the interviews, the Inspection Team noted that some staff members demonstrated a lack of awareness of data protection or were unfamiliar with the contents of the PMP Manual. The Privacy Commissioner recommends that the REO take a top-down approach to establish mechanisms to ensure and evaluate the effectiveness of training and education on data protection and to identify knowledge gaps and areas where additional training or education may be warranted.

40. In compliance with the enforcement notices issued by the Privacy Commissioner in December 2022, the REO has developed a departmental Education and Training Plan to strengthen training on data security and protection. In particular, the REO will organise talks/seminars/workshops on data security and protection at least twice a year and assess the participation and effectiveness of the relevant training plan annually.

41. The Privacy Commissioner also notes that the REO has formed a training and awareness workgroup in response to the recommendation provided by OGCIO in the Review Report. The workgroup consists of senior and junior staff members of different teams and collects staff's opinions to understand their needs before making a training plan.

Recommendation:

(x) Take a top-down approach to establish mechanisms to ensure and evaluate the effectiveness of training and education on data protection and identify knowledge gaps and areas where additional training or education may be warranted.

The REO's Follow-up Actions on the Review Report

42. The REO has been implementing the recommendations made in the Review Report in phases to enhance the governance of information security management, raise information security awareness, strengthen the protection of its major system and provide additional protection for departmental IT infrastructure, details of which are not set out in this report in order to maintain the confidentiality of the security measures adopted by the REO.

Conclusion

43. Based on the Inspection results, it is evident that the REO has made significant efforts to implement a PMP and has built a robust infrastructure to protect personal data privacy, which is supported by an ongoing review and monitoring process to facilitate compliance with the requirements under the Ordinance. The compliance standard of the REO in terms of data protection is expected to be further stepped up, considering its implementation of the recommendations in the Review Report and its continuous compliance with the PCPD's enforcement notices relating to the two data breach incidents in 2022.

44. The Privacy Commissioner is pleased to note that the REO has adopted the good practices outlined in this report, such as appointing designated officers to review the effectiveness of the implementation of the PMP, providing comprehensive guidance and training to staff members and adopting "Privacy by Design" in its information system. However, the Privacy Commissioner strongly encourages the REO to consider the recommendations provided in this report (see the Annex) and

continuously strive to instil and maintain a strong culture of data protection among all staff members to better protect the privacy and security of the personal data of its stakeholders and demonstrate its commitment to good data governance and building trust with members of the public.

Annex: Recommendations made by the Privacy Commissioner

(i) Ensure that the content of the PMP Manual is up to date to reflect any amendments to the Ordinance;

(ii) State the specific electronic storage location of the personal data in the personal data inventory;

(iii) Clearly set out the criteria and mechanism, including the ranking of the personnel responsible for making the decision, for conducting a PIA in the PMP Manual;

(iv) Review and update the IT policies and guidelines to specifically set out the interval and personnel responsible for conducting the inventory stocktaking of the IT equipment;

(v) Review all of the service contracts with the data processors to set out the REO's rights to audit and inspect how the data processors handle and store personal data and the REO's rights to conduct audits and inspections periodically;

(vi) Take appropriate measures to ensure that the log records are properly reviewed regularly;

(vii) Review all categories of log records to ensure that the personal data contained in the records are properly retained for no longer than is necessary to reduce the risk of unauthorised or accidental access, processing, erasure, loss or use;

(viii) Strengthen the coordination between the ITMU and individual divisions concerning the use of the REO's information systems that contain personal data to ensure proper usage of the relevant systems;

(ix) Conduct data breach drills for both information security incidents and the loss of physical records and/or equipment on a regular basis; and

(x) Take a top-down approach to establish mechanisms to ensure and evaluate the effectiveness of training and education on data protection and identify knowledge gaps and areas where additional training or education may be warranted.