IN RE: DEPARTMENT OF FOREIGN AFFAIRS - PASSPORT BREACH

NPC SS 19-001

INITIATED AS A *SUA SPONTE*
NPC INVESTIGATION INTO
THE POSSIBLE DATA PRIVACY
VIOLATIONS COMMITTED BY
THE DEPARTMENT OF FOREIGN
AFFAIRS
x----------x

ORDER

This refers to a *sua sponte* investigation of the possible data breach arising from the alleged mishandling of personal information in relation to the issuance and printing of passports by third parties on behalf of the Department of Foreign Affairs (DFA).

Facts

In January 2019, the media reported the alleged mishandling of personal data in the issuance and printing of passports.[1] Based on the reports, the DFA, through Secretary TLL., announced that individuals renewing their passports were required to bring their birth certificates with them since the FOF DFA's previous third-party passport maker, "took away" passport applicants' data.[2]

Contrary to Secretary TLL's statement, former DFA Secretary PY maintained that there was neither a data breach nor a leak in the DFA.[3] He explained that FOF's contract had ended, and that APO Production Unit, Inc. (APUI) and United Graphic Expression Corporation (UGEC), through a joint venture, now operate and manage the DFA passport system.[4] APUI Chairman, Mr. MD, maintained that passport

[1] Fact-Finding Report, 14 July 2019, at 1, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[2] *Id.*
[3] *Id.*
[4] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

data are with APUI and that the DFA has access to such data.[5] Secretary TLL, shortly thereafter, retracted his earlier statement that FOF did not run away with the data, but it only made the data inaccessible.[6]

As a result, the Commission, through its Complaints and Investigation Division (CID), conducted a *sua sponte* investigation on the alleged data breach that arose from the alleged mishandling of personal data of passport applicants.

On 14 January 2021, the Commission sent to Secretary TLL formal correspondence informing him that the Commission received reports of alleged mishandling of data being processed by third parties for the issuance and printing of passports on behalf of the DFA.[7] The Commission invited the DFA's Data Protection Officer and other authorized representatives to a Fact-Finding Conference on 16 January 2019.[8]

The DFA, through its Data Protection Officer, requested that the meeting be rescheduled to 25 January 2019.[9] It explained that there was no data breach because DFA and APUI remain in custody and control of the data, and the data has not been shared with or accessed by unauthorized third parties.[10]

On 21 January 2021, the Commission and the DFA held the Fact-Finding Conference where the DFA invited the Commission to conduct an on-site investigation of the APUI Printing Facility at Lima Technology Center in Batangas.[11]

On 30 January 2019, the Commission's on-site team did not proceed with the on-site investigation since it was denied access to the APUI Printing Facility.[12] Representatives from APUI and the DFA required the Commission's on-site team to execute a Non-Disclosure Agreement (NDA) before allowing access to the APUI Printing Facility.[13]

---

[5] *Id.*
[6] *Id.*
[7] Letter *from* Atty. GVS, Director IV, Legal and Enforcement Office, National Privacy Commission, *to* TLL, Secretary of Foreign Affairs, Department of Foreign Affairs (14 January 2019).
[8] *Id.*
[9] Letter *from* MGM, Data Privacy Officer, Department of Foreign Affairs, *to* Atty. GVS, Director IV, Legal and Enforcement Office, National Privacy Commission (14 January 2019).
[10] *Id.*
[11] Notice of On-Site Examination, 24 January 2019, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[12] Memorandum *from* Complaints and Investigation Division, National Privacy Commission (30 January 2019).
[13] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

On 23 February 2021, the Commission, through the CID, issued an Order requiring the DFA to submit within fifteen (15) days from receipt thereof, an updated report detailing the facts surrounding the incident, a copy of the DFA's contract with the involved third-party provider, and proof or certification that passport applicant's data remains within the DFA's custody and control.[14]

On 18 March 2021, the DFA submitted its compliance with the Order dated 23 February 2021.[15] It submitted an updated report denying the alleged mishandling of the personal data of passport applicants, a certification stating that the server containing passport applicants' data is currently stored in a vault in the APUI Printing Facility, and is within the DFA's custody and control, and the Memorandum of Agreement and Supplemental Agreement between the DFA and the Bangko Sentral ng Pilipinas (BSP) on the implementation of a Machine-Readable Passport and Visa Project.[16] The DFA seeks the termination or dismissal of the *sua sponte* investigation for lack of sufficient basis.

On 17 September 2021, the CID submitted its report after a thorough assessment of the documents that the DFA submitted and the online passport appointment system available on the website, "passport.gov.ph".[17] As a result of its technical investigation, the CID determined that there was no exfiltration of passport applicants' personal data.[18] The CID also monitored the dark web for any signs of the purported data breach and found no traces of the exfiltration of data.[19]

The CID, however, discovered vulnerabilities in the website, "passport.gov.ph".[20] It learned that several pieces of personal information remain publicly available data and may be downloaded using a web browser and a specific search criterion.[21] It also determined that the appointment code is made of a pattern composed of the DFA Branch ID, Year, Month, Date, and Appointment Number.[22] With the use of a random appointment code, the CID was

[14] Order, 23 February 2021, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[15] Letter *from* The Undersecretary for Civilian and Security and Consular Affairs *to* National Privacy Commission (18 March 2021).
[16] *Id.*
[17] Supplemental Fact-Finding Report, 17 September 2021, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[18] Technical Report, 07 September 2021, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019), at 4.
[19] *Id.* at 3.
[20] *Id.* at 4.
[21] Supplemental Fact-Finding Report, 17 September 2021, at 3, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NTC 2019).
[22] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

able to access other application forms.[23] The CID thus, concluded that the website, "passport.gov.ph" is vulnerable to an Insecure Direct Object References (IDOR) attack.[24]

The CID further assessed the website, "passport.gov.ph" and determined that attackers could bypass security controls, and use the website as a platform for attacks against its users.[25]

Discussion

A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."[26] In this case, the Commission conducted a *sua sponte* investigation on the DFA passport system, including the website, "passport.gov.ph" to determine the circumstances of the incident and whether it meets the definition of a personal data breach.

The Commission, through the CID, conducted a technical investigation and discovered several vulnerabilities in the website, "passport.gov.ph" which put the security of the DFA passport system into question. Section 20 of the Data Privacy Act of 2012 (DPA) requires the implementation of appropriate measures on systems and computer network to protect the personal information in its custody:

> Section 20. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[27]

It is incumbent upon the personal information controller to implement the following security measures to its system:

> Section. 20. *Security of Personal Information.*

[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (k).
[27] *Id.* § 20.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

x x x

(c) The determination of the appropriate level of security under this section must take into account 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 practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

x x x

(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

Section 28 of the Implementing Rules and Regulations of the DPA further provides:

Section 28. *Guidelines for Technical Security Measures*. Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

x x x

b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> mitigating action against security incidents that can lead to a personal data breach;[28]

The Commission emphasizes the paramount duty of personal information controllers such as the DFA to implement adequate organizational, physical, and technical measures in order to secure the personal information of its data subjects and to prevent possible data breach incidents. For this reason, it is incumbent upon the DFA to address the vulnerabilities that the Commission identified in the DFA passport system.

WHEREFORE, premises considered, the Commission **ORDERS** the Department of Foreign Affairs (DFA) within thirty (30) days from receipt of this Order to:

(1) **ADDRESS** the vulnerabilities on the DFA passport system available on the website, "passport.gov.ph" by performing Vulnerability Assessment Penetration Testing on passport.gov.ph and adding a "noindex" parameter to the HTTP header to prevent any indexing of saved information by any search engine; and

(2) **SUBMIT** proof that it has addressed the vulnerabilities on the DFA passport system.

The Commission shall furnish the DFA with its Technical Report dated 07 September 2021 to guide the DFA in addressing the technical vulnerabilities identified in the DFA passport system.

SO ORDERED.

City of Pasay, Philippines.
11 November 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

[28] National Privacy Commission, Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, rule I, § 28.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

DEPARTMENT OF FOREIGN AFFAIRS
2330 Roxas Boulevard, Pasay City

MGM
Data Protection Officer
Department of Foreign Affairs

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228