IN RE: DEPARTMENT OF FOREIGN AFFAIRS (DFA) 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

RESOLUTION

AGUIRRE*, D.P.C.;*

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

Facts

In January 2019, several newspaper outlets reported that the DFA is requiring some applicants for passport renewal to bring their birth certificates because its previous outsourced passport maker "took away" all its applicants' data.[1]

[1] Helen Flores, *DFA Passport Maker Runs Off with All Data*, THE PHILIPPINE STAR, 12 January 2019, *available at* https://www.philstar.com/headlines/2019/01/12/1884444/dfa-passport-maker-runs-all-data (19 July 2022); John Nieves, *Its Like The Government Doesn't Care About Protecting Our Data,* UNBOX, 13 January 2019, *available at* https://unbox.ph/editorials/its-like-the-government-doesnt-care-about-protecting-our-data/; Catalina Ricci S. Madarang, *Making Sense of DFA's Passport Data Theft Controversy, INTERAKSYON,* 14 January 2019, *available at* https://interaksyon.philstar.com/special-features/2019/01/14/142166/making-sense-dfas-passport-data-theft-controversy-teddyboy-locsin/.

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 14 January 2019, National Privacy Commission (NPC), through its Complaints and Investigation Division (CID), sent a formal correspondence to DFA Secretary Teodoro L. Locsin, Jr. informing him of reports of alleged mishandling of data for the issuance and printing of passports.[2]

On 23 February 2021, the Commission, through the CID, issued an Order for DFA to submit the following:

1. Updated Report detailing the facts surrounding the incident;
2. Copy of DFA's contract with the involved third-party provider; and
3. Proof or Certification that the applicant's data is within DFA's custody and control.[3]

On 18 March 2021, DFA submitted proof of its compliance with the Order dated 23 February 2021 and provided the Commission with the following:

1. Updated Report denying the alleged mishandling of the personal data of passport applicants that were processed by the Bangko Sentral ng Pilipinas (BSP) when it was handling passport printing for DFA;
2. Copies of the Memorandum of Agreement between the DFA and BSP in 2006; and
3. A certification stating that the server, with passport applicants' data contained therein, is under the DFA's custody and control.[4]

On 07 September 2021, the CID submitted its Technical Report to the Commission on the results of the Vulnerability Assessment Penetration Testing (VAPT) conducted on DFA's online passport appointment system "www.passport.gov.ph", and its search of the dark web for evidence of database exfiltration.[5] On the possible data breach reported in the newspaper article, the CID determined that

---

[2] Letter from National Privacy Commission to DFA Secretary Teodoro L. Locsin, 14 January 2019, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NPC 2019).
[3] CID Order, 23 February 2021, at 1, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NPC 2019).
[4] Letter from Undersecretary Brigido J. Dulay, 18 March 2018, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NPC 2019).
[5] CID Technical Report, 07 September 2021, at 4, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).

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

there was no personal data exfiltration that had occurred despite the alleged "taking away" of passport data.[6] The CID, however, discovered that several pieces of personal information remain publicly available and may be downloaded using a web browser and a specific search criterion.[7] The CID assessed that the website "www.passport.gov.ph" is vulnerable to an Insecure Direct Object Reference (IDOR) attack.[8] The CID's investigation also revealed that attackers could bypass security controls and use the website as a platform for attacks against its users.[9]

Based on the CID's Technical Report,[10] the Commission issued an Order on 11 November 2021 directing DFA to comply with the following within thirty (30) days from its receipt:

> **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 of 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.**[11]

Since DFA did not comply with the Order, on 31 May 2022, the Commission, through the Enforcement Division (EnD), issued its

---

[6] *Id.*
[7] *Id.* at 1.
[8] *Id.* at 3.
[9] *Id.* at 3.
[10] Order, 11 November 2021, *in* In re: DFA – Passport Breach, NPC SS 19-001 (NPC 2019).
[11] *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

Enforcement Letter, reiterating the directives in the Order dated 11 November 2021.[12]

On 09 June 2022, the DFA sent a letter to the NPC in compliance with the Enforcement Letter dated 31 May 2022.[13] It provided the results of the VAPT conducted by the its hosting and application service provider for the passport system, APO Production Unit Inc. (APO), as well as the measures taken after the assessment.[14] Further, it included APO's report on the implementation of a "noindex" parameter to the http header to prevent any indexing of saved information by any search engine.[15]

On 21 June 2022, the DFA sent another letter reiterating the results of the VAPT conducted by APO and emphasizing that "links to specific passport application forms when "site:passport.gov.ph" is typed in the browser's search box no longer generate the questionable result."[16]

Issue

Whether the DFA implemented sufficient measures to manage security incidents.

Discussion

A security incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data.[17] It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.[18]

---

[12] Final Enforcement Assessment Report, 28 June 2022, at 3, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).
[13] Letter *from* Medardo G. Macaraig, Assistant Secretary and Data Protection Officer, Department of Foreign Affairs, *to* Rodolfo S. Cabatu, Jr. and Maria Theresita E. Patula, National Privacy Commission, Enforcement Division (09 June 2022)
[14] Final Enforcement Assessment Report, 28 June 2022, at 3, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).
[15] *Id.* at 3.
[16] Letter *from* Medardo G. Macaraig, Assistant Secretary and Data Protection Officer, Department of Foreign Affairs, *to* Rodolfo S. Cabatu, Jr. and Maria Theresita E. Patula, National Privacy Commission, Enforcement Division (21 June 2022)
[17] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], Rule I § 3 (J) (15 December 2016).
[18] *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

When the Commission, through the CID, discovered that several pieces of personal information remain publicly available and may be downloaded using a web browser and a specific search criterion,[19] there is no question that a security incident occurred in this case.

Section 4 of Rule II of NPC Circular 16-03 (Personal Data Breach Management) states that Personal Information Controllers (PICs) should implement policies and procedures to manage security incidents:

> Section 4. *Security Incident Management Policy*. A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:
>
> A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
> B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
> C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
> D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
> **E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.**[20]

The Commission issued an Order dated 11 November 2021 directing the DFA to address the security incidents that the Commission found while conducting its investigation. The DFA submitted its report

[19] Final Enforcement Assessment Report, 28 June 2022, at 3, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).
[20] NPC Circ. No. 16-03, § 4. (Emphasis Supplied).

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

addressing the vulnerabilities of the DFA passport system and adding the "noindex" parameter to the HTTP header that resulted to the vulnerability assessment "Risk Level: High" scoring zero (0) when the CID conducted its own vulnerability check.[21] The score zero (0) means that the updated website is less likely to be breached by potential digital attack.[22] The EnD determined:

> On 16 June 2022, the former performed the vulnerability assessment using the OWASP ZAP vulnerability assessment tool. As such, the vulnerability assessment "Risk Level: High" scored 0, which means the updated website is less likely to be breached by potential digital attacks. Moreso, the EnD further conducted a test to verify previously publicly available data that could be downloaded from the passport appointment system using Google and Firefox web browsers which specifies a certain search criterion example "site:passport.gov.ph" as the keyword.
>
> Furthermore, the OWASP ZAP scanned zero (0) high-risk vulnerability, which means no critical threat or high potential breach may occur that needs urgent fixing or concerns. The OWASP ZAP gives an overview of the improvement on the website compared to the previous result of twenty-nine (29) high-risk vulnerabilities on the technical report dated 07 September 2021. Therefore, the passport appointment system website has now addressed the two (2) recommendations and is able to improve its security against potential attackers or hackers.[23]

Following DFA's compliance with the Order dated 11 November 2021 the Commission finds that DFA has sufficiently addressed the vulnerabilities on the DFA passport system available on the website "www.passport.gov.ph".

Although the DFA already addressed the vulnerabilities identified by the Commission, it is still obliged to periodically conduct vulnerability assessments as a preventive or minimization measure for possible personal data breach.[24] Section 6 of Rule III of NPC

---

[21] Final Enforcement Assessment Report, 28 June 2022, at 5, *in* In the Matter of Department of Foreign Affairs (DFA) Office of Consular Affairs Passport Appointment System (passport.gov.ph) Vulnerability, NPC SS 19-001 (NPC 2019).
[22] *Id.*
[23] *Id.*
[24] NPC Circ. No. 16-03, § 6 (D).

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

Circular 16-03 provides for preventive measures to minimize the occurrence of a security incident:

> Section 6. *Preventive or Minimization Measures*. A security incident management policy shall include measures intended to prevent or minimize the occurrence of a personal data breach. Such safeguards may include:
>
> . . .
>
> D. Regular monitoring for security breaches and vulnerability scanning of computer networks[.][25]

The Commission emphasizes the duty of PICs to implement adequate safeguards to prevent or minimize occurrences of personal data breach or security incidents. Considering that the monitoring and implementation of security measures remains a continuing responsibility of PICs, the DFA, as a PIC, shall regularly monitor for security breaches and conduct vulnerability scans of its computer network and the DFA passport system.

WHEREFORE, premises considered, this Commission finds the submission of the Department of Foreign Affairs in response to the Order dated 11 November 2021 **SUFFICIENT**. This Commission resolves that the matter is hereby **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
14 July 2022.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

---

[25] *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

JOHN HENRY D. NAGA
Privacy Commissioner

DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

DEPARTMENT OF FOREIGN AFFAIRS
2330 Roxas Boulevard, Pasay City

MGM
Data Protection Officer

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