



**IN RE: KGJS FLEET MANAGEMENT
 MANILA, INC.**

NPC BN 18-135

X-----X

RESOLUTION

AGUIRRE, D.P.C.:

Before the Commission is KGJS Fleet Management Manila, Inc.’s (KGJS) breach notification involving the reposting of the contents of its website to another website resulting in the disclosure of personal information of its employees.

Facts

On 20 July 2018, a KGJS employee reported that it received a text message on his company-issued mobile phone about an inquiry for a job opening.¹ According to the job applicant, he/she obtained the information on the job opening, which includes the employees’ personal information, from *www.Indeed.com* (Indeed), a website for job listings.²

KGJS narrated that the personal information of its employees can be accessed on Indeed using the keyword “kgjs” on the website’s search feature.³ KGJS deduced that the personal information came from its own website and other possible website sources such as Philippine Overseas Employment’s (POEA) website.⁴

KGJS clarified that there was no agreement between KGJS and Indeed about the re-posting of its website content.⁵ Further, its employees

¹ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 2, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ *Id.*

have no knowledge of authorizing Indeed to post information related to job openings.⁶

On 23 July 2018, the employee received another call from the same mobile number inquiring about a sea-based job opening posted on Indeed.⁷ The employee reported this matter to his manager and to KGJS' Data Protection Officer (DPO).⁸ The DPO then conveyed the same information to the Data Breach Response Team.⁹

On 24 July 2018, KGJS notified the National Privacy Commission (NPC) of the incident involving the personal information of its employees.¹⁰

KGJS explained that a total of four (4) of its employees were affected by the re-posting on Indeed's website.¹¹ Two (2) of the employees' information such as their full name, designation, company direct line, and company mobile number were listed directly on its company website.¹² Two (2) other employees' information such as company mobile numbers, a "wrong" email address of an employee, and their full names as official representatives of KGJS, according to KGJS, were possibly obtained from the POEA website.¹³

KGJS indicated that this information was publicly posted on its website to serve as contact persons for inquiries on crew requirements or sea-based job openings.¹⁴

KGJS averred that the posting of its employees' personal information on Indeed may "result to identity theft and unauthorized transfer and re-posting of web content/article."¹⁵ KGJS also stated that there might be "possible misinterpretation" of the its job posting or "possible misinformation" between the employee and the applicants.¹⁶ Lastly,

⁶ *Id.*

⁷ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 3, in In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.* at 1.

¹¹ *Id.* at 2.

¹² *Id.*

¹³ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 3, in In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

KGJS reasoned that “applicants who are web visitors and users of Indeed may presume that the job posting is legitimate and may result to unauthorized collection of personal information and resume.”¹⁷

On 27 July 2018, KGJS updated the NPC on its breach notification.¹⁸ KGJS explained that it removed the affected employees’ personal information from its company website on 24 July 2018.¹⁹ It also sent an email notification to the affected employees about the incident.²⁰ Indeed also removed the job posting as confirmed through an email sent on 26 July 2018.²¹

On 30 July 2018, KGJS submitted a Full Report²² where it claimed that there was “no database breach”²³ and no sensitive personal information was involved.²⁴

KGJS reported that its employees’ personal data posted in the POEA website has already been corrected and updated.²⁵ KGJS also reported that it also submitted a letter of information to POEA regarding the incident.²⁶

KGJS also “de-indexed” and removed the personal data on its website to reduce the risk of “indexed searching” and to prevent the recurrence of the incident,²⁷ It also conducted a Privacy Impact Assessment (PIA) of its website.²⁸

Issue

¹⁷ *Id.*

¹⁸ Update as of 27 Jul 18 – Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 27 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² Full Report as of 30 Jul 18: Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 30 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

²³ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 2, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

²⁴ *Id.* at 5.

²⁵ *Id.* at 3.

²⁶ Update as of 27 Jul 18 – Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 27 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

²⁷ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

²⁸ *Id.* at 6.

Whether KJGS sufficiently addressed the incident and implemented security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. KGJS implemented reasonable and appropriate security measures to address the incident. Nonetheless, the incident does not amount to a personal data breach.

Section 3 (F) of NPC Circular 16-03 (Personal Data Breach Management) defines a personal data breach:

Section 3. *Definition of Terms.* For the purpose of this Circular, the following terms are defined, as follows:

...

F. **“Personal Data Breach”** refers to 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. It may be in the nature of:

1. An availability breach resulting from loss, accidental, or unlawful destruction of personal data;
2. Integrity breach resulting from alteration of personal data; and/or
3. A confidentiality breach resulting from the unauthorized disclose of or access to personal data.²⁹

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access to personal data transmitted, stored, or otherwise processed.³⁰

In this case, the website Indeed is a metasearch engine that consolidates job listings from websites and recruiting companies.³¹

²⁹ National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], § 3 (F) (15 December 2016).

³⁰ *Id.*

³¹ See Adam Hayes, Indeed v. Linked-in: What is the Difference, *available at* <https://www.investopedia.com/articles/personal-finance/020215/indeed-vs-linkedin.asp> (last accessed November 2023).

Indeed provides job seekers access to job listings and allows them to post resumes and research companies.³²

When a user searches for job listings on Indeed, one can see job listings that Indeed scans from the internet and collates into a user's search results.³³

When a user clicks the "Apply on company site" button, Indeed will send the user's job application to the employer's applicant tracking system (ATS).³⁴ The ATS is a software that employers use during the recruitment and hiring process to streamline the hiring process.³⁵

Indeed explained that if a user applies directly on the company's website, the user will not receive any communication from Indeed about his or her application status.³⁶ The employer may communicate with the applicant through its own hiring platform, or through email.³⁷

Considering that the purpose of posting job openings on Indeed is to maximize visibility and attract as many potential candidates as possible, the information of the KGJS employees or recruiters that were posted on Indeed would have been used in a way that was still consistent with the original purpose for posting it on KGJS's website.

KGJS' reasoning that the posting on Indeed may result to "identity theft and unauthorized transfer" and "unauthorized collection of personal information and resume"³⁸ is speculative. Through the ATS, it is the recruiting company itself that handles the collection of any applicant information and not Indeed.

³² See About Indeed, available at <https://ph.indeed.com/about> (last accessed January 2023).

³³ See About Jobs on Indeed: What You Need to Know, available at <https://support.indeed.com/hc/en-us/articles/115002786323-About-Jobs-on-Indeed-What-You-Need-to-Know> (last accessed 31 January 2024).

³⁴ *Id.*

³⁵ See What are Applicant Tracking Systems, available at <https://www.indeed.com/career-advice/career-development/what-are-applicant-tracking-systems> (last accessed 31 January 2024).

³⁶ *Id.*

³⁷ See About Jobs on Indeed: What You Need to Know, available at <https://support.indeed.com/hc/en-us/articles/115002786323-About-Jobs-on-Indeed-What-You-Need-to-Know> (last accessed 31 January 2024).

³⁸ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 3, in In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

As stated by KGJS, Indeed possibly obtained the information of the employees from the KGJS and POEA website.³⁹ These websites are accessible to the public particularly for the purpose of recruitment and placement through a manning agency.⁴⁰

Given these reasons, the incident cannot be considered a confidentiality breach resulting from the unauthorized disclosure of or access to personal data. There is no unauthorized access to the systems maintained and managed by KGJS nor was there any breach of security protecting the personal data processing system of KGJS.

Additionally, the details of the personal data of the recruitment officers of KGJS, such as names and designation, are publicly and readily available.⁴¹ In addition, the contact numbers for inquiries on job openings are their company contact numbers and not their personal phone numbers.⁴²

NPC Circular 16-03 only pertains to personal data of an individual or natural person.⁴³ Since the contact number involved is the contact number of KGJS, a juridical person, this incident does not amount to a personal data breach as contemplated by NPC Circular 16-03.

Even though the matter is not considered a reportable breach, KGJS implemented reasonable and appropriate security measures to address the incident. KGJS implemented measures to minimize any potential risks associated with the incident, therefore minimizing any adverse effects on the individuals whose data were impacted.

KGJS immediately requested the removal of its employees' information on Indeed.⁴⁴ Indeed confirmed the removal through

³⁹ *Id.* at 2.

⁴⁰ Final Breach Notification Evaluation Report, 21 March 2023, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2023).

⁴¹ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 2, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

⁴² *Id.*

⁴³ *See* NPC Circ. No. 16-03.

⁴⁴ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

email.⁴⁵ KGJS also conducted the removal of its employees' personal information from its own website.⁴⁶

KGJS also notified the four (4) employees through email whose data may have been acquired from the security incident.⁴⁷ KGJS provided them with an update on the initiatives undertaken to address the matter.⁴⁸

Lastly, KGJS modified its website to ensure that it does not appear in search results on any third-party websites.⁴⁹

Based on the foregoing, the actions taken by KGJS following the incident allowed it to enhance its security measures and are sufficient to close the case in accordance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) and NPC Circular 16-03.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-135 In re: KGJS Fleet Management Manila, Inc. is considered **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

⁴⁵ Full Report as of 30 Jul 18: Security Incident dated 20 Jul 18 of Article/Web Content in Company Website, 30 July 2018, at 1, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

⁴⁶ Security Incident dated 20 July 2018 of Article/Web Content in Company Website, 24 July 2018, at 5, *in* In re: KGJS Fleet Management Manila, Inc., NPC BN 18-135 (NPC 2018).

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *Id.*

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

CG
Data Protection Officer
KGJS Fleet Management Manila, Inc.

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