



Republic of the Philippines  
NATIONAL PRIVACY COMMISSION

**KGR,**

*Complainant,*

-versus-

**CID Case No. 18-E-040**

*For: Violations of Sections 27, 28,  
31, and 32 of the Data  
Privacy Act of 2012*

**BB, JA, AA**

*Respondents.*

x-----x

**DECISION**

**AGUIRRE, D.P.C.**

Before this Commission is a complaint by KGR (“Complainant”) against BB, JA, and AA (“Respondents”) for violation of several provisions of the Data Privacy Act.

**The Facts**

Complainant was at Rans C Computer Repair Services (“Ran C”) sometime in the morning of 07 March 2018 to print a copy of her resume. She was assisted by Respondent BB, a staff member of Ran C. After several attempts of printing her resume, she was given one copy for which she paid P8.00. Upon checking her resume, she noticed a straight white line on her picture. She called the attention of Respondent BB, who told her that it was fine and that is how the machine prints. Complainant stated that she will not pay for that kind of printing.

Thereafter, on 11 March 2018, Complainant and her mother went to Ran C and she saw copy of her resume posted on one of the CPUs in the shop.<sup>1</sup> Complainant and her mother called the attention of the present staff member, Respondent JA. Respondent JA asked Respondent BB about the resume over the phone and the latter replied,

---

<sup>1</sup> Records, p. 2.

*“Sorry po talaga Ma’am nainis po kasi ako.”*<sup>2</sup> Respondent AA, the owner of Ran C, claims she was not aware of the incident as she was not in the shop for the past few days. Complainant filed an Incident Report, Blotter, and sent two (2) Memoranda to Respondents requesting for a letter of apology and damages under the Data Privacy Act of 2012,<sup>3</sup> which Respondents never replied to.

On 22 May, Complainant filed a Complaint-Affidavit with the National Privacy Commission (“Commission”). The case was called for Discovery Conference on 19 July 2018 and was reset to 11 September 2018 due to work suspension on the original schedule.

During the Discovery Conference, the parties manifested that they were not willing to enter into a settlement. Complainant was given ten (10) days to submit additional evidence to substantiate her allegations. Respondent was given ten (10) days from receipt of such additional evidence to file their Responsive Comment. Complainant was given ten (10) days after her receipt of this to file her Reply.<sup>4</sup>

On 24 September 2018, Complainant sent an email to the Commission stating thus:

As I want to practice and fight for my rights, I feel and am already very exhausted mentally and emotionally. I and my uncle have been trying to have a reasonable and fair settlement with them out of court witnessed by the Circle C Mall admin staff and security officers but they still won’t cooperate. I have decided to stop and not pursue this anymore. Again, thank you to you all. I do appreciate your noble servitude in protecting the privacy rights of your fellow Filipino/s. May God bless you always!<sup>5</sup>

Respondents later filed a Motion to Waive Presentation of Additional Evidence (with attached Joint Counter Affidavit) dated 26 September 2018, stating that the Complainant failed to provide additional evidence and must be deemed to have waived her right to submit the same.<sup>6</sup>

---

<sup>2</sup> *Ibid.*

<sup>3</sup> *Id.*, pp. 9-10; 17.

<sup>4</sup> *Id.*, p. 38.

<sup>5</sup> *Id.*, p. 48.

<sup>6</sup> *Id.*, p. 39.

### Arguments of the Parties

Complainant alleges that the resume contained her sensitive personal information. In her Complaint, she states that “everyone who entered the shop can easily see her resume.”<sup>7</sup> She filed a criminal complaint for violation of Sections 27, 28, 31, and 32 of the Data Privacy Act arising from Improper Disposal, Unauthorized Purposes, Malicious and Unauthorized Disclosure of her sensitive personal information without her prior consent and knowledge.<sup>8</sup>

In their Joint Affidavit, Respondents admit that BB cut the portion of Complainant’s resume where her photo, address, contact nos. and e-mail were printed. They state that he pasted this on the side of the CPU inside the cashier’s counter for purpose of identifying the Complainant in case she returns. He did it because he does not want to transact anymore with Complainant.<sup>9</sup>

They dispute the Complainant’s allegations, thus:

It must be emphasized that the size of the CPU where the resume portion was posted is not fronting a customer or the customer area. Ergo, a customer cannot see what was pasted on the CPU side unless the customer will get [sic] inside the counter or overreach the desk. To conclude, Complainant noticed her photo on the side of the CPU because she is the very person in the photo. She is familiar with herself and her own resume. Be it noted that Complainant’s personal information are not readable from the customer area because the font is too small. In short, there is no public accessibility of the information which R.A. 10173 intends to penalize.

### Issue

The issue to be resolved in this case is whether Respondents committed acts in violation of Complainant’s privacy rights under the Data Privacy Act.

---

<sup>7</sup> Ibid.

<sup>8</sup> *Id.*, p. 1.

<sup>9</sup> *Id.*, at p. 42.

## Discussion

At the outset, it should be noted that the email sent by Complainant on 24 September 2018 to the Commission expressing her intention not to pursue the case cannot be considered an affidavit of desistance for purposes of terminating the case. The Commission thus resolves this Complaint on the basis of the evidence on record.

*Respondents misunderstand the concept of personal information controllers, processing, and disposal.*

In their Joint Affidavit, Respondents argue:

None of the Respondents is a personal information controller nor a personal information processor. Respondents are not engaged to (sic) any of those acts that would define them as personal information controller or processor. Respondents are engaged in the lease of computer units and printing of paper works. They are not engaged in the act of “processing” as defined in R.A. 10173.<sup>10</sup>

There is nothing in the law that requires entities to be engaged in the primary business of processing information before they are considered personal information controllers. By having the control of and discretion in the use of personal information of individuals, they are already considered the controller. They are thus accountable for the protection of the information and for the observation of the obligations under the law. These persons and entities must be able to justify their processing of personal data under any of the lawful criteria provided in the law.<sup>11</sup> They have an obligation to provide mechanisms for the access, correction, and removal of personal data upon request, as well as the filing of a complaint. They are further required to secure the processing of any personal data by documenting and implementing organizational, technical, and physical measures to respect the abovementioned rights.<sup>12</sup> At the core of these obligations are the general data privacy principles<sup>13</sup> of transparency, legitimate purpose, and proportionality. Following this, any person or entity that

---

<sup>10</sup> Records, p. 45.

<sup>11</sup> R.A. 10173, §§ 12-13.

<sup>12</sup> *Id.*, at § 20.

<sup>13</sup> *Id.*, at § 11.

processes information should process information only for legitimate purposes that have been made known to the data subject. They should only process as much information as is needed to achieve their clearly defined and stated business purposes or to comply with the provisions of law or regulation.

Respondents also argue that:

The act prohibits (sic) by Sec. 28 is “processing.” Sec. 3 (j) of R.A. 10173 defined processing as “any operation any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

Respondents did not conduct any kind of operation or any set of operation. The personal information in the resume portion was not collected, recorded, organized, stored nor updated. Neither was there modification, retrieval, consultation, use, consolidation, blocking, erasure nor destruction of data. The personal information in the resume portion remained as is.<sup>14</sup>

It must be clarified that “processing” under the Data Privacy Act is *any* use of personal and sensitive personal information for the duration of its entire data life cycle – from its collection, processing, and retention, up to the disposal or erasure of personal data. A data life cycle begins and ends taking into consideration the purpose for processing that information in the first place.

Despite Respondents’ assertion that they are engaged in the lease of units and printing of paper works,<sup>15</sup> they nevertheless still handle personal information in the course of their operations. Respondents must bear in mind that their processing of such personal information should only be for the purpose of delivering the services they provide.

In addition, Respondents’ appreciation of the term “disposal” is also misplaced. In their Joint Affidavit, they state:

Disposal means “throwing away.” To set the record straight, Respondents did not dispose the resume portion bearing the photo, contact number, address and e-mail of Complainant.

---

<sup>14</sup> Records, p. 44.

<sup>15</sup> *Supra at note 10.*

Respondent BB pasted the resume portion on the CPU and not “disposed.”<sup>16</sup>

Contrary to what Respondents assert, “disposal” is not limited to the physical act of throwing away. Simply recycling the backside of a document containing personal or sensitive personal information can be considered “improper disposal” since it allows the further processing of the personal data despite its purpose having already been fulfilled. As stated above, personal data should only be processed for as long as necessary to achieve the stated purpose. Once that purpose is achieved, the personal data should be disposed of in a way that makes further processing no longer possible.

Respondent and all other personal information controllers should be aware of the obligations imposed by the Data Privacy Act. These misconceptions, though not enough to merit a recommendation for prosecution in this case, nevertheless pose very real risks to data subjects.

*The Complaint must be dismissed for lack of merit.*

It is a disputed fact whether the posted resume is indeed viewable by the general public. While the Complainant alleges that “it can be easily seen by anyone who will enter their shop,” the Respondents claim that “the side of the CPU where the resume portion was posted is not fronting a customer or customer area... a customer cannot see what was pasted on the CPU side unless the customer will get (sic) inside the counter or overreach the desk.”<sup>17</sup>

Such fact is crucial in determining whether such posting was pursuant to a legitimate business interest – that is, choosing whom to transact with – and whether such was done in a manner that is mindful of the general privacy principle of proportionality.

In administrative proceedings such as this case, it is the complainant who carries the burden of proving their allegations with substantial

---

<sup>16</sup> Records., p. 43.

<sup>17</sup> Records, p. 43.

evidence or such “relevant evidence that a reasonable mind might accept as adequate to support a conclusion.”<sup>18</sup>

Instead of providing the additional evidence as directed during the Discovery Conference,<sup>19</sup> Complainant sent an email to the Commission stating that she will no longer pursue the case.<sup>20</sup>

The Commission is bound to adjudicate complaints following its Rules of Procedure, which provides:

**Section 22. Rendition of decision.** – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.<sup>21</sup>

As such, on the basis of all the evidence presented, the Commission finds that there is insufficient evidence to support the claims of Complainant for Respondents’ violation of the Data Privacy Act.

The Commission therefore resolves to dismiss the complaint for lack of substantial evidence required in establishing cases before quasi-judicial bodies.

**WHEREFORE**, on the basis of this Complaint, the Commission hereby resolves to **DISMISS** the Complaint of KGR against Respondents BB, JA, and AA.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

**SO ORDERED.**  
Pasay City, 12 May 2020.

---

<sup>18</sup> Ombudsman v. Fetalvero, G.R. No. 211450, 23 July 2018.

<sup>19</sup> Records, p. 38.

<sup>20</sup> *Supra* at note 5.

<sup>21</sup> NPC Circular No. 16-04 dated 15 December 2016 (“NPC Rules of Procedure”), Sec. 22, Emphasis supplied.

(sgd)  
**LEANDRO ANGELO Y. AGUIRRE**  
*Deputy Privacy Commissioner*

WE CONCUR:

(sgd)  
**RAYMUND ENRIQUEZ LIBORO**  
*Privacy Commissioner*

(sgd)  
**JOHN HENRY DU NAGA**  
*Deputy Privacy Commissioner*

**COPY FURNISHED**

**KGR**  
*Complainant*

**BB,**  
**JA,**  
**AA**  
*Respondents*

**AMM**  
*Counsel for Respondents*

**COMPLAINTS AND INVESTIGATIONS  
DIVISION;  
ENFORCEMENT DIVISION;  
GENERAL RECORDS UNIT  
National Privacy Commission**