



Republic of the Philippines  
NATIONAL PRIVACY COMMISSION

---

**PRIVACY POLICY OFFICE  
ADVISORY OPINION NO. 2022-011<sup>1</sup>**

19 August 2022

[REDACTED]

**RE: PERSONAL DATA RETENTION AND DELETION**

Dear [REDACTED],

We respond to your inquiry regarding the request of a client of Flexi Finance Asia Inc. (FFAI) to delete his personal data from its system.

We understand that FFAI is a financing company that processes basic credit information of its clients, including their personal data as defined in the Data Privacy Act of 2012 (DPA).<sup>3</sup> Under the Credit Information System Act (CISA),<sup>4</sup> FFAI is required to retain the data of its clients for reporting to the Credit Information Corporation (CIC).

You also cite relevant provisions of FFAI's Loan Contract with the client that allows it to retain personal data, *to wit*:

b. Retain my personal information within the period as may be allowed for by law from the date of the termination of my loan contract subject to the discretion of the company. The company may use such information for any legitimate purpose but always in compliance with prevailing and to be enacted laws and regulations.

c. Retain my information in the database of the company with the latter having the right to share the same to all its affiliates and necessary third parties for any legitimate business purpose subject to the assurance by the company that proper security systems are in place to protect my information.

---

<sup>1</sup> Tags: data subject's rights; right to erasure; data retention.

<sup>3</sup> 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 (2012).

<sup>4</sup> An Act Establishing The Credit Information System And For Other Purposes [Credit Information System Act] Republic Act No. 9510 (2008).

Ref No.: PRD-22-00280

NPC\_DIT\_AOT-V1.0, R0.0,05 May 2021

However, the client did not substantiate his/her deletion request with any of the circumstances mentioned in Section 16 (e) of the DPA.

You thus seek guidance on the following:

1. Whether FFAI can compel the client to provide proof of the circumstances provided in Section 16 (e) of the DPA;
2. The number of years that the FFAI can retain its clients' data; and
3. If there is any violation if FFAI does not delete the client's data as requested.

Considering that your questions are interrelated, we shall discuss them jointly.

*Personal Data; Basic Credit Information; Data subject rights; Right to Erasure; Limitations.*

At the outset, we note that your query is silent as to the type of data involved in the client's request. Thus, we deem it prudent to discuss the difference between personal information and sensitive personal information (collectively, personal data) for proper perspective.

The DPA defines Personal Information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.<sup>6</sup>

On the other hand, Sensitive Personal Information refers to personal information:

- (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- (4) Specifically established by an executive order or an act of Congress to be kept classified.<sup>7</sup>

The bases for permissible processing of the two types of personal data differs. Section 12 of the DPA provides for the criteria for lawful processing of Personal Information:

SEC. 12. *Criteria for Lawful Processing of Personal Information.* - The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

- (a) The data subject has given his or her consent;
- (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject

---

<sup>6</sup> Data Privacy Act, § 3 (g)

<sup>7</sup> Id., § 3 (l)

- prior to entering into a contract;
- (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
  - (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
  - (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
  - (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

On the other hand, Section 13 of the DPA enumerates the circumstances when Sensitive Personal Information may be processed:

SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

- (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- (b) The processing of the same is provided for by existing laws and regulations: *Provided*, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further*, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
- (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
- (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided*, That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further*, That the sensitive personal information are not transferred to third parties: *Provided, finally*, That consent of the data subject was obtained prior to processing;
- (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
- (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or

public authority.

In relation to Section 12 (c) and 13 (b) of the DPA, FFAI must additionally comply with the provisions of the CISA in processing the Sensitive Personal Information of its clients since processing based on a legal obligation requires that all conditions imposed by the legal obligation have been complied with as discussed in NPC Resolution 18-010, *viz*:

“Processing based on a legal obligation requires that all conditions imposed by the legal obligation have been complied with. Section 12 (c) of the DPA requires not only that the processing is “necessary” but also that it be in “compliance with a legal obligation”. Compliance with everything required by the claimed legal obligation as a condition for the processing is an essential element for any claim of valid processing under this criterion.”<sup>8</sup>

Under the CISA, entities providing credit facilities are required to submit credit information of its borrowers and thereafter update the same on a regular basis to the CIC.

The Implementing Rules and Regulation (IRR) of the CISA also require submitting entities to submit current, objective, factual, and basic credit data, both positive and negative, on all their data subjects.<sup>11</sup> Basic Credit Data comprises the following:

**4.4. Basic Credit Data.** Every participating entity shall submit to the Corporation the following basic credit data on all data subjects:

- a) Individual
  - i. Personal circumstances such as name (last, first, middle), date of birth, sex, civil status, present residence, employer and position or business, as the case may be;
  - ii. Number of children depending for support;
  - iii. TIN, SSS or GSIS No.;
  - iv. Net income;
  - v. Residence for the last 2 years;
  - vi. Employer/s or business/es for the last 5 years;
  - vii. Owners/lessee of house occupied;
  - viii. Car/s owned;
  - ix. Bank/s where accounts are maintained, including types of bank accounts; and
  - x. Other assets, real or personal.<sup>12</sup>

The IRR of the CISA also provides the data that comprises Negative Information of data subjects. The IRR provides:

#### **4.5. Negative Information**

The Corporation’s credit information database shall likewise contain negative information which shall include, among others, the following:

- a) Past due;
- b) Default/s on loan/s;
- c) Details of the settlement of loans that defaulted;
- d) Foreclosures;
- e) Adverse court judgments relating to debts;

---

<sup>8</sup> National Privacy Commission, NPC Resolution 18-010

<sup>11</sup> Implementing Rules and Regulation of the Credit Information System Act (CISA) Republic Act No. 9510, § 4 (1) (2009)

<sup>12</sup> *Id.*, § 4 (4)(a) (2009)

- f) Report on bankruptcy or insolvency;
- g) Petition or order on suspension of payments;
- h) Corporate rehabilitation;
- i) Other pending court cases (either as plaintiff or defendant) related to credit transactions or cases that will affect the financial capacity of the borrower;
- j) Inclusion in a bouncing check checklist;
- k) Cancelled credit cards; and
- l) Such other information that may be determined by the Corporation.<sup>13</sup>

In view of the foregoing, aside from Personal Information, some of the personal data required to be submitted and/or retained by submitting entities pursuant to the CISA qualifies as Sensitive Personal Information. This can serve as guide on the type and the limits of the processing that FFAI may perform on the personal data of its clients.

Be that as it may, please note that regardless of the nature of the personal data involved, the DPA recognizes certain rights in favor of the data subject. Relevant to your query are the rights to suspend, withdraw, or order the blocking, removal, or destruction of his or her data from the personal information controller's (PIC) filing system, subject to specified conditions as stated in Section 16 (e) of the DPA.

The NPC provided further guidance on the matter through NPC Advisory No. 2021 - 01 on Data Subject Rights.<sup>15</sup> Section 10 thereof provides:

SECTION 10. *Right to Erasure or Blocking.* – A data subject has the right to request for the suspension, withdrawal, blocking, removal, or destruction of his or her personal data from the PIC's filing system, in both live and back-up systems.

- A. This right may be exercised upon discovery and substantial proof of any of the following:
  - 1. The personal data is:
    - a) incomplete, outdated, false, or unlawfully obtained;
    - b) used for an unauthorized purpose;
    - c) no longer necessary for the purpose/s for which they were collected; or
    - d) concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press, or otherwise authorized;
  - 2. The data subject objects to the processing, and there are no other applicable lawful criteria for processing;
  - 3. The processing is unlawful; or
  - 4. The PIC or PIP violated the rights of the data subject.

Further, the same advisory provided grounds for denying requests for erasure or blocking by a Data Subject, *viz*:

*2. Denial of Request.* A request for erasure or blocking may be denied, wholly or partly,

---

<sup>13</sup> Id., § 4 (5) (2009)

<sup>15</sup> National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021 – 01] (January 29, 2021).

when personal data is still necessary in any of the following instances:

- a.) Fulfillment of the purpose/s for which data was obtained;
- b) Compliance with a legal obligation which requires personal data processing;
- c) Establishment, exercise or defense of any legal claim;
- d) Legitimate business purposes of the PIC, consistent with the applicable industry standard for personal data retention;
- e) To apprise the public on matters that have an overriding public interest or concern, taking into consideration the following factors:
  - i. Constitutionally guaranteed rights and freedoms of speech, of expression, or of the press;
  - ii. Whether or not the personal data pertains to a data subject who is a public figure; and
  - iii. Other analogous considerations where personal data are processed in circumstances where data subjects can reasonably expect further processing.
- f) **As may be provided by any existing law, rules, and regulations.”**

Additionally, the IRR of CISA also provides for Data Subject rights which necessarily includes the right to dispute and erasure, *viz*:

#### **4.6. Rights of Data Subjects**

- a) A borrower shall have the right to have ready and immediate access to credit information pertinent to him subject to the payment of a prescribed fee;
- b) He shall have the right to dispute erroneous, incomplete or misleading credit information;
- c) He shall be entitled to a simplified dispute resolution process to fast track the settlement/resolution of disputed credit information;
- d) He shall be informed of any correction or removal of any erroneous, incomplete or misleading information within 5 working days from verification or conclusion of an investigation or from deletion of the disputed information, as the case may be;
- e) He shall be entitled to indemnity in case of denial, without justification, of the aforementioned rights;
- f) He shall be notified by a submitting entity of the latter’s obligation to submit and disclose basic credit data to the Corporation; and
- g) He shall have the right to know the causes of refusal of an application for credit facilities or services from a financial institution that uses credit data as basis or

ground for such refusal.<sup>18</sup>

Further, CIC Circular No. 2015-01<sup>19</sup> lays down the obligations of a submitting entity under the CISA, *viz*:

4.6 The Submitting Entity shall regularly submit the Basic Credit Data of all its Borrowers contained in its data base, file or system, to the CIC not later than on the 5<sup>th</sup> day of the month and in the form/format and manner prescribed by the CIC.

4.7 The Submitting Entity shall ensure that the Basic Credit Data of all its borrowers with the CIC is accurate, complete, correct, and current up to the relevant Update Cycle Date.

4.8 The Submitting Entity shall ensure that when receiving Error Reports from the CIC, the Submitting Entity shall rectify errors in the relevant files and send the corrected files to the CIC within a period of three (3) working days. X x x”

In fine, while both the DPA and the CISA and all related issuances recognize the right of a Data Subject to request the deletion of his personal data, the exercise of such right is not absolute. PICs, such as FFAI, may request the data subject to substantiate his/her request. However, FFAI is also obliged to observe the limits imposed by law as to the type of data and the conditions for its processing.

*Data retention period; CISA requirements.*

It must be emphasized that the DPA requires that personal data shall only be retained for as long as necessary for the fulfillment of the purposes for which the data was obtained; for the establishment, exercise or defense of legal claims; for legitimate business purposes; or as provided by law.<sup>20</sup> Other conditions for the retention of data are also provided in Sections 12 and 13 of the DPA.

The DPA further provides that personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined. NPC Advisory Opinion No. 2017-24 is instructive on this point, *viz*:

“From the foregoing, it is clear that the DPA and its IRR does not provide for a specific retention period. Instead, the law sets out the general principles and guidelines for the retention of personal data. As a general rule, records containing personal data should be retained only for as long as may be necessary for the purpose or purposes for which the personal data were collected.”

Further, Section 19(d)(1) and (2) of the IRR of the DPA provides:

“d. Personal Data shall not be retained longer than necessary.

1. Retention of personal data shall only for as long as necessary:

---

<sup>18</sup> Implementing Rules and Regulation of the Credit Information System Act (CISA) Republic Act No. 9510, § 4 (6) (2009)

<sup>19</sup> Credit Information Corporation, Enforcement of the Credit Information System Act Pursuant to Republic Act No. 9510 and its Implementing Rules and Regulations [Circular 2015-01] § 4.2 (15 May 2015)

<sup>20</sup> Data Privacy Act of 2012, § 11 (e).

- a) For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
- b) For the establishment, exercise or defense of legal claims; or
- c) For legitimate business purposes, which must be consistent with standards followed by the applicable industry or appropriate government agency.

Retention of personal data shall be allowed in cases provided by law.”

Additionally, CISA provides a period of retention if the Basic Credit Data refers to a negative credit information, *viz*:

“A. Retention Period for Negative Information in the Database

Any negative information on a borrower shall stay in the Corporation’s database for not more than 3 years from and after the date the negative information shall have been rectified through the following:

- i. Payment or liquidation of debt; or
- ii. Settlement of debt through compromise agreement or court decision exculpating the borrower from any liability.

Negative information shall be corrected and updated within 15 days from receipt of notice of payment, liquidation or settlement of debt in accordance with the prescribed rules of the Corporation.”<sup>21</sup>

Thus, although PICs cannot retain personal data in perpetuity, the continued processing thereof may be permitted if it is anchored on Sections 12 and 13 of the DPA. And, if negative information is involved, FFAI must also comply with the three-year limitation provided in the CISA. Please note that the repurposing of Personal Data retained other than for what the law prescribes may constitute as a violation of the DPA.

*DPA violation for denial of data subject rights.*

As mentioned above, the continued processing of the Data Subjects data and, in effect, the denial of the right to delete, may be justified pursuant to Sections 12 and 13 of the DPA in relation to CISA.

On this note, the existence of a lawful ground for processing does not give PICs an unbridled power to process personal data. PICs are still required under the law to observe the data privacy principles of legitimate purpose, transparency, and proportionality. In this regard, we observed that your contract provisions appear to violate some of the data privacy principles and hence cannot serve to justify the retention of the Data Subject’s personal data.

You may want to revisit the contract provisions involved as it is inconsistent with the principle of transparency which requires that the data subject should be aware of the nature, purpose,

---

<sup>21</sup> Rules and Regulations Implementing the Credit Information Systems Act of 2008, Rule 4 (4.5) (A). (2009).

and extent of the processing of his or her personal data, including the risks and safeguards involved, his or her rights as a data subject, and how these can be exercised.<sup>23</sup>

Also, in accordance with the principle of proportionality, the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably fulfilled by other means.<sup>24</sup>

We emphasize that should FFAI deny or limit the exercise of data subject rights, it should ensure that the data subject is clearly and fully informed of the reasons for the denial or limitation.<sup>25</sup>

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

**Sgd.**  
**FRANKLIN ANTHONY M. TABAQUIN, IV**  
Director IV, Privacy Policy Office

---

<sup>23</sup> Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18 (2016)

<sup>24</sup> Id.

<sup>25</sup> NPC Advisory No. 2021 – 01, § 14.