National Cyber
Security Authority

DPO

Data Protection and
Privacy Office

STANDARD CONTRACTUAL CLAUSES FOR PERSONAL DATA TRANSFER OUTSIDE RWANDA UNDER THE LAW Nº 058/2021 OF 13/10/2021 RELATING TO THE PROTECTION OF PERSONAL DATA AND PRIVACY

www.dpo.gov.rw

dpp@dpo.gov.rw

9080

February 2024

SECTION I

Clause 1
Purpose and scope

(a)   The purpose of these standard contractual clauses ("**Clauses**") is to ensure that the transfer of personal data from Rwanda is carried out in compliance with Article 49 of Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.

(b)   The Parties to these Clauses are:

   (i)   A natural person, public or private corporate body, or legal entity transferring personal data outside Rwanda, hereinafter referred to as (the "**Discloser**");

   (ii)   A natural person, public or private corporate body, or legal entity located outside Rwanda receiving personal data directly or indirectly from the Discloser hereinafter referred to as (the "**Recipient**").

   (iii)   These Clauses apply with respect to the details of personal data to be transferred outside Rwanda as described in Annexes I.A and I.B.

(c)   These Clauses apply without prejudice to other relevant applicable laws which the Parties may be subjected to.

Clause 2
General Undertakings

(a) Each Party warrants and undertakes to the other Party that it has full capacity and authority to enter into and to perform its obligations under and in accordance with these Clauses.

(b) Each Party agrees to comply with all laws and regulations in connection with the performance of its obligations under these Clauses.

(c) Each Party acknowledges that, it may prohibit or suspend transfer of Personal Data in order to protect the rights and interests of data subjects with regard to the processing of their personal data in accordance with the respective Parties' legal framework.

Clause 3
Interpretation

(a)   Where these Clauses use terms that are defined in the Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy, those terms shall have the same meaning.

(b)   These Clauses shall be read and interpreted in the light of the provisions of the Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.

(c)   The term "Supervisory Authority" in these Clauses shall refer to the National Cyber Security Authority (NCSA).

Clause 4
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, these Clauses shall prevail.

SECTION II: OBLIGATIONS OF THE PARTIES

Clause 5
Data protection safeguards

The Parties warrant that they have implemented appropriate technical and organizational measures, to fulfil their obligations under these Clauses.

Clause 6
Binding Principles of Transfer of personal data from the Discloser to the Recipient

6.1   Purpose limitation

The Recipient shall process personal data only for the specific purpose(s) of the transfer. However, he/she may also process personal data for another purpose if:

(i)   It has obtained the data subjects' prior written consent;

(ii)   Necessary for the establishment, exercise or defence of a legal claim in the context of specific administrative regulatory or judicial proceedings;

(iii)   Necessary in order to protect the vital interests of the data subjects;

(iv)   It is done for public interest grounds;

(v)   Any other Lawful exceptional grounds of transfer provided for by Article 48 of the Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.

6.2   Transparency

(a)   In order to enable data subjects to effectively exercise their rights, the Discloser shall inform the data subjects of the following:

(i)   Identity and contact details of the recipient;

(ii)   The categories of personal data to be transferred;

(iii)   The involvement of any third party who shall access the personal data that is subject to transfer;

(iv)   The available personal data protection security measures, both technical and organization measures;

(v)   The Discloser's ability to comply with the required personal data breach remedial mechanisms.

(b)   On request by a data subject, the Parties shall make a copy of these Clauses available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the relevant text of the clauses prior to sharing a copy.

In this case, the Parties shall provide a meaningful summary of the redacted data if the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions to the extent possible.

6.3   Accuracy and data minimisation

(a)   The Discloser shall ensure that the personal data transferred is accurate and, where necessary, kept up to date. The Discloser shall take every reasonable step to ensure that any personal data that is inaccurate is rectified without delay upon becoming aware that such data is inaccurate.

(b)   The Parties shall ensure that the processing of personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

6.4   Storage limitation

The Parties shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical and organizational measures to ensure compliance with this obligation, including erasure or anonymization of personal data and deletion of all back-ups at the end of the retention period.

6.5   Security of processing

(a)   The Parties, during transmission of personal data, shall implement appropriate technical and organisational measures to ensure the security of personal data, including protection against a breach of security leading to unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the personal data.

(b)   In assessing the appropriate level of security, parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing of personal data.

(c)   The Parties have agreed to put in place technical and organisational measures set out in Annex II. The Parties shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(d)   The Parties shall ensure that persons authorised to process personal data have committed themselves under an appropriate statutory obligation of confidentiality. Furthermore, Parties shall ensure that any person or entity acting under their authority processes personal data only on their direct instructions.

(e)   In the event of a personal data breach concerning personal data, the Parties shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(f)   In the event of a personal data breach that is likely to result in a high risk to the rights and freedoms of the data subjects, the Discloser shall without undue delay notify the data subject pursuant to Article 45 of the Law N° 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.

(g)   In event of a personal data breach, the Recipient shall notify the Discloser within forty-eight (48) hours after being aware of the incident. The Discloser shall within forty-eight (48) hours after being aware of the incident communicate the breach to the Supervisory Authority pursuant to Article 43 of the Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy. The Discloser shall report the personal data breach to the Supervisory Authority not later than seventy- two (72) hours with all facts available pursuant to Article 44 of the same Law.

(h)   The Parties shall document all relevant facts relating to the personal data breach including its effects and any remedial action taken, and keep a record thereof.

6.6   Sensitive personal data

Where personal data include personal data revealing a person's race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or family details ("**Sensitive personal data**") both Parties shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved in accordance with Articles 10 and 11 of the Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.

6.7   Documentation and compliance

(a)   Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the Parties shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b)   The Parties shall make such documentation or information available to the Supervisory Authority on request.

Clause 7
Governing law and jurisdiction

(a) These Clauses shall be governed by the laws of Rwanda.
(b) Any claim arising from these Clauses shall be resolved by the competent courts of Rwanda.

Clause 8
Liability

(a) Each Party shall be liable to the other Party for any damages caused in relation to these Clauses.

(b) Where both parties are responsible for the damage caused to the data subject as a result of a breach of these Clauses, both parties shall be jointly and severally liable. However, the Discloser or the Recipient is exempted from liability if he/she proves that he/she is not responsible for the damage caused.

Clause 9
Dispute resolution

(a)   In the event of a complaint or dispute brought by a data subject concerning the processing of transferred personal data, both parties will inform each other about such complaints or disputes and will cooperate with the intention to settle amicably in a timely manner.

(b)   In case the parties fail to resolve the dispute amicably, parties shall refer the case to the Supervisory Authority as an organ in charge of settling disputes in relation to Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.

Clause 10
Notification

Both Parties agree to notify each other, where possible regarding changes in the processing, access or disclosure of transferred personal data. They shall provide as much information as possible about the changes. The timeline for notification is decided by the Parties.

Clause 11
Suspension of Transfer

In the event that the Discloser or the Recipient is in breach of its obligations under these Clauses or the Law relating to the protection of personal data and privacy, then the other party may suspend the transfer of the transferred personal data until the breach is remediated or terminate the processing of personal data covered by these Clauses. This is without prejudice to any other applicable legal redress provided for by the Law.

Clause 12
Personal data transferred prior to the termination of the contract

Upon termination of these Clauses, the Recipient shall, at the request of the Discloser, either return or delete the transferred personal data and all copies and back-ups.

ANNEXURES

ANNEX I

A. PARTIES

The Discloser:

1. Name: ………………………………….

2. Address………………………………

3. Registration number as a Data Controller / Data Processor in Rwanda:
   …………………………

4. Data Protection Officer's name, email and contact details: …………………………..

5. Activities relevant to the data transferred under these Clauses: ………………………

6. Signature and date: ………………………….

The Recipient:

1. Name: ….………………………….

2. Address: ………………………

3. Registration number as a Data Controller / Data Processor (where applicable) with representative's name, email and contact details in Rwanda in accordance with Article 39 of the Law relating to the protection of personal data and privacy:…………………………………………………..

4. Data Protection Officer's name, email and contact details: …………………….

5. Activities relevant to the data received under these Clauses: ……………………

6. Signature and date: ………………………….

B. DESCRIPTION OF TRANSFERRED PERSONAL DATA

Categories of data subjects whose personal data is transferred

………………………....

Categories of personal data transferred

…………………………

Sensitive personal data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

………………………..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

……………………….

Nature of the processing (transfer or storage)

……………………….

Purpose(s) for transfer of personal data and further processing.

………………………..

The period for which the personal data transferred shall be retained

……………………….

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE TRANSFER OF PERSONAL DATA

Description of technical and organisational measures implemented by the Parties (including any relevant certifications) to ensure an appropriate level of security of transferred personal data, taking into account the nature, scope, context and purpose of the processing, and the risks assessment made to ensure the rights and freedoms of data subjects.

Examples of possible measures:

- *Measures of pseudonymisation and encryption of personal data.*

- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of transferred personal data.*

- *Measures for user identification and authorisation.*

- *Measures for the protection of personal data during transmission.*

- *Measures for the protection of personal data during storage.*

- *Measures for ensuring physical security of locations at which personal data are stored.*

- *Measures for ensuring personal data logging.*

- *Measures for ensuring system configuration, including default configuration.*

- *Measures for internal and IT security governance and management.*