



<p>If there has been a delay (more <b>than 72 hours</b> after becoming aware of the incident and reporting it to the Data Protection and Privacy Office)</p> <p><i>Please provide your justifications for the delay</i></p>	<p><i>Please provide your justifications for the delay</i></p>
---	--

**Description of the personal data breach**

<b>Type</b> <i>(Tick as appropriate)</i>	<b>Nature</b> <i>(Tick as appropriate)</i>	<b>Cause</b> <i>(Tick as appropriate)</i>
<input type="checkbox"/> Confidentiality breach <i>(i.e. unauthorised disclosure of or access to personal data)</i>  <input type="checkbox"/> Integrity breach <i>(i.e. alteration of data)</i>  <input type="checkbox"/> Availability breach <i>(i.e. loss or destruction of data)</i>	<input type="checkbox"/> Accidental Disposal <input type="checkbox"/> Cyberattack (e.g. hacking) <input type="checkbox"/> Email Leakage <input type="checkbox"/> Postal Leakage <input type="checkbox"/> Loss of Physical Documents <input type="checkbox"/> Loss of Electronic Devices <input type="checkbox"/> Employee Misconduct <input type="checkbox"/> Program Bug <input type="checkbox"/> Server Misconfiguration <input type="checkbox"/> Burglary <input type="checkbox"/> Others: Specify.....	<input type="checkbox"/> Employee error or omission <input type="checkbox"/> Employee intentional act <input type="checkbox"/> Contractor error or omission <input type="checkbox"/> Contractor intentional act <input type="checkbox"/> External intentional act <input type="checkbox"/> External unintentional act <input type="checkbox"/> Former employee error or omission <input type="checkbox"/> Former employee intentional act <input type="checkbox"/> Unknown

<p>Additional detail about the personal data breach (if any)</p>	
--	--

<p>What are categories of data subjects affected?</p> <p><i>Examples of categories are employees, clients, suppliers, shareholders, students, children, subscribers, patients, etc.</i></p>	
---	--

<p>What are the categories of personal data records concerned?</p> <p><i>Examples of categories are identification data, professional data, health data, ,biometric data, genetic data, financial data, behavioral data, etc.</i></p>	
---	--

<p>What is the approximate number of data subjects affected?</p>	
--	--

<p>Has any affected data subject complained to the Data Controller? If so, how many complaints have been received?</p>	
--	--

<p>Is there any risk of harm to any affected individual/s?</p> <p><i>Please explain why there is / there is no real risk of such harm</i></p>	
---	--

**SECTION 3 – CONTAINMENT AND RECOVERY**

Describe all measures taken or which will be taken to address the personal data breach	
What measures have or will be taken to mitigate the possible adverse effects of the personal data breach?	
Has any assistance been provided or will be provided to affected individuals to help them mitigate the consequences of the data breach?	
What measures have been taken or envisaged to be taken to prevent recurrence of such similar breach/es?	

**SECTION 4 – APPROVAL TO COMMUNICATE**

**Applicable**    **Not Applicable** (Tick as appropriate)

If applicable, please fill in the details below	If Not applicable, please tick as appropriate below
<i>Please explain why you want concerned data subjects to be aware of the personal data breach</i>	<input type="checkbox"/> The data controller has implemented appropriate technical and organisational protection measures in relation to personal data breached such that the personal data breach is unlikely to result in a high risk to the rights and freedoms of the data subject
<b>Channel of Communication</b> (Tick as appropriate) <input type="checkbox"/> In-writing <input type="checkbox"/> Electronically	<input type="checkbox"/> The data controller has taken measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize
<b>Timelines to communicate data subjects</b>  DD../..MM../..YYY...   ..HH.. : ..MM..	<input type="checkbox"/> The data controller communicated it to the public whereby the data subject is informed in an equally effective manner

**Did the Data Controller notify/report to any other regulator or law enforcement agency on the personal data breach?**

**YES**    **NO** (If Yes, list the names).

.....  
.....

**I certify that the above information is correct and complete and hereby report on personal data breach under the Law N° 058/2021 of 13/10/2021 relating to the protection of personal data and privacy.**

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Position: \_\_\_\_\_ Signature: \_\_\_\_\_

**Notes:**

- 1. Pursuant the article 44 of Rwanda’s Law on protection of personal data and privacy, in case of personal data breach, the data controller, within seventy-two (72) hours after being aware of the incident, draws up a report on personal data breach with all facts and submit to the personal data breach to the Data Protection and Privacy Office*
- 2. Please send the complete report form to [databreach@dpo.gov.rw](mailto:databreach@dpo.gov.rw) and [dpp@ncsa.gov.rw](mailto:dpp@ncsa.gov.rw) by writing name of Data Controller in the email’s subject.*