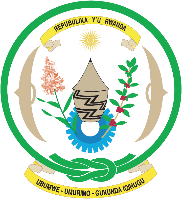
**REPUBLIC OF RWANDA**



**NATIONAL CYBER SECURITY AUTHORITY**

**DATA PROTECTION AND PRIVACY OFFICE**

**COMPLIANCE SELF-ASSESSMENT FORM**

The purpose of checklistis to obtain a compliance image of personal data processing operations within your organization in accordance with Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy (DPP Law).

# **STEP1 - Information about your organisation**

|  |  |  |
| --- | --- | --- |
| Name of organisation |  | |
| Nature of entity (*Tick as appropriate)*  Public  Private  Faith Based organisation  NGO  Political organisation  Development Partner  Others: ............................................. (specify) | | |
| Address of organisation | Country: | Province: |
| District: | Sector: |
| Cell: | Phone Number: |
| Email: | Website (if any): |
| Designated Data Protection Officer | Name: | |
| Phone number: | |
| Email: | |

# **STEP 2 -Operational details**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Is your organisation registered and/or licensed to operate in Rwanda? |  |  |  | *please specify name(s) of regulator(s), license type(s), and license number(s).* |
| 1. Is your organisation registered with the Data Protection and Privacy Office? |  |  |  | *please specify registration type(s) and registration number(s).* |
| 1. Have you designated a Data Protection Officer responsible for data protection and privacy compliance within your organization? |  |  |  |  |
| 1. Have you conducted a [Data Inventory](https://dpo.gov.rw/assets/documents/guidance-on-personal-data-inventory-and-readness-assessment-checklist.pdf)? |  |  |  | *please check* [*https://dpo.gov.rw/assets/documents/guidance-on-personal-data-inventory-and-readness-assessment-checklist.pdf*](https://dpo.gov.rw/assets/documents/guidance-on-personal-data-inventory-and-readness-assessment-checklist.pdf) *for further guidance* |

# **STEP 3- Principles of processing personal data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| **Transparency -** Are data subjects fully informed of how your organization uses their personal data in a concise, transparent and easily accessible form using clear and plain language? |  |  |  |  |
| **Purpose limitation-** Is personal data only used for the purposes for which it was originally collected? |  |  |  |  |
| **Data minimization -** Is personal data collected limited to what is necessary for the purposes for which it is processed? |  |  |  |  |
| **Accuracy-** Are there procedures in place to ensure personal data is kept up to date and accurate and where a correction is required and are the necessary changes made without delay? |  |  |  |  |
| **Storage limitation -** Are there retention policies and procedures in place to ensure personal data is held for no longer than is necessary for the purposes for which it was collected? |  |  |  |  |

# **STEP 4- Rights of Data Subjects**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Are there procedures in place for data subjects to exercise their rights? |  |  |  |  |
| 1. Are there procedures in place for handling complaint and rights of data subjects to their personal data? |  |  |  |  |

# **STEP 5- Collection of personal data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Are personal data collected in paper format? |  |  |  |  |
| 1. Are personal data collected digitally? |  |  |  |  |
| 1. Are personal data collected directly from data subjects themselves? |  |  |  |  |
| 1. Are personal data collected indirectly from other Data Controllers or/and third parties? |  |  |  | *please specify name(s) of Data Controllers or/and third parties* |
| 1. Do you provide the information described in article 42 of DPP Law to data subjects when personal data is collected? |  |  |  |  |

# **STEP 6 - Storage of personal data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Does your organization store personal data outside Rwanda? |  |  |  | *please specify the name(s) of hosting service provider(s).* |
| 1. Is your organization authorised to store personal data outside Rwanda? |  |  |  | *please specify authorisation number(s).* |
| 1. Does your organization have hosting agreements with your hosting service provider(s)? |  |  |  |  |

# 

# **STEP 7 - Share, Transfer, Access to personal data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Does your organization share and/or transfer personal data to organisations/ individuals based outside Rwanda? |  |  |  |  |
| 1. Does your organization provide remote access to personal data to organisations/individuals based outside Rwanda? |  |  |  |  |
| 1. Do you have contract for transfer with recipient(s) outside Rwanda? |  |  |  |  |
| 1. Is your organization authorised to transfer personal data outside Rwanda? |  |  |  |  |
| 1. Do you share personal data with other Data Controllers in Rwanda? |  |  |  |  |
| 1. Do you have Data Sharing Agreements in place? |  |  |  |  |
| 1. Do you involve Data Processor(s) in processing of personal data? |  |  |  |  |
| 1. Do you have Data Processing Agreements in place? |  |  |  |  |

# **STEP 8- Grounds for processing of personal data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Do you rely on consent of data subjects for processing of personal data? |  |  |  |  |
| 1. Have you reviewed your organisation’s mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that the data subject has chosen to agree to the processing of their personal data by way of statement or a clear affirmative action? |  |  |  |  |
| 1. Are there procedures in place to demonstrate that the data subject has consented to their data being processed? |  |  |  |  |
| 1. Where services are provided to a child, are procedures in place to verify age and get consent of a parent/ legal guardian required? |  |  |  |  |
| 1. Where services are provided to people with disability, are there procedures in place to verify and get consent of a parent/ legal guardian required? |  |  |  |  |
| 1. Are there procedures in place to allow the data subject to withdraw their consent to the processing of their personal data? |  |  |  |  |
| 1. Are there other legal grounds other than consent that you base on while collecting/processing personal data? |  |  |  | *please list other legal ground(s) you base on while processing personal data* |

# **STEP 9- Personal Data Breach**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Does your organisation have a documented personal data breach response plan? |  |  |  |  |
| 1. Are there procedures in place to notify and report data subjects of a personal data breach? |  |  |  |  |
| 1. Are there procedures in place to communicate data subjects of a personal data breach? |  |  |  |  |
| 1. Are there procedures in place to document all personal data breaches? |  |  |  |  |

**STEP 10 - Safeguards/ Data Security of Personal data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment question** | **YES** | **NO** | **N/A** | **Remarks / Additional explanation** |
| 1. Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them? |  |  |  | *please list risks identified and measures in place to mitigate against them* |
| 1. Is there a document that specifies the technical and organisational measures for personal data? |  |  |  |  |
| 1. Do security controls or procedures include measures to ensure pseudonymisation and encryption employed for transferring, storing, and receiving personal data? |  |  |  |  |
| 1. Is personal data systematically destroyed, erased, or anonymised when it is no longer legally required to be retained. |  |  |  |  |
| 1. Do you have an audit log of activities performed on these personal data repositories? |  |  |  |  |
| 1. Do you maintain records of processed personal data? |  |  |  |  |
| 1. Is access to personal data controlled and based on role? |  |  |  |  |
| 1. Do you carry out DPIA for high risks processing operations? |  |  |  | *please specify high risks processing operations* |