User Guide

for

Dpo Portal

for the

Data Protection Office

(Version No. 7.1)

June 2023
1. Introduction

The DPO Portal (e-DPO) is an online platform where Companies, Organisations and Individuals can register as Processors or Controllers and submit eForms. It is a single platform where user can submit, query their application status, download certificate, and pay application fees using the various modes of payment including Online Payment (Credit Card) facilities. It is the one-stop shop for interacting with the Data Protection Office.

Register as administrator before using the DPO eservices platform where you will receive user credentials (username and password) to log into the system. The administrator will also be responsible to manage organisations, register representative(s) in the three scenarios explained in the next diagram and assign organisation(s) to representative(s).

A representative is a person assigned by the Administrator to perform operations such as submit applications or submit eForms for the controller/processor. A Representative is relevant to 3 types of Administrator and is not applicable to the individual “Administrator” one. All representatives need to have a Maupass account in order to gain access to the system. A representative can also submit complaint for his organization(s), if required.
2. **Process Flow**

**DPO Portal for Eservices – Help Sheet**

1. You need to register as an Administrator

2. There are four types of Administrators as follows

   1. Individual
   2. Organisations
   3. Management Companies
   4. Group of Companies

3a. Individual is his own representative  
3b. The three types of Administrators have to add one or more representatives

4. Individual or Representative can Register Controller/Processor, make payment and submit Eforms

   **Controller/Processor Application**
   - Payment
   - Search
   - Submit Eforms

5. The system will send email notifications in the process

6. You can query Applications/Print Certificates

7. You can query Transactions

8. Please read this DPO portal guide for detailed instructions
3. **Main Page**

The main page of the Portal allows user to login using their respective Credentials or redirect to links to Register on the system. **Companies/Organisations registered will login using credentials generated by the system whereas individuals will login using their Maupass credentials.**

Clicking on:

- ‘Create an account as DPO Administrator’ will redirect user to register as an administrator on the platform.
- ‘Forgot Password?’ will redirect user to generate One-time Password to reset Password of user. To note that this function will only work for Companies/Organisations registered as Administrators and not Individuals.
- ‘Maupass Forgot Password?’ – for Individual with Maupass Account.
- ‘Maupass Registration?’ – for individual to register on Maupass.
- ‘Register Anonymous Complaint’ – redirect to page to register an anonymous complaint.
There are 4 types of administrator.

The four types are listed as (as per Screenshot):

1. Individual
   A maupass account is required to log in to the system. You have to create and activate the maupass account first.
   Both Foreigners and Local users should register as individuals to use the DPO system and use their Maupass account to login once access has been granted.
User will have to choose whether he/she will register using a BRN if available and if he/she is a foreigner.

If Individual selects to register using BRN, the latter will be prompted to enter the BRN. Once input, click on the ‘search icon’ next to the input box and if Information will be retrieved from InfoHighway for BRN typed in. If Searching using BRN is not getting any data, individual can still input their National Identity Card Number in the ‘MNIC’ input box and search their respective information. Information such as Name and address will be retrieved from InfoHighway.

If individual is a foreigner, their passport number is required in order to register on the system.
If individual chooses to register without the BRN, type in only the MNIC or the Passport Number as required depending on the type of individual (Foreigner or local).
2. Management Companies Administrator Type

Management Companies can register controllers/processors under his management after registering as Management Companies Administrator.

If registering using BRN, input BRN in text Box provided and click on the ‘search icon’ and then proceed to fill in other details.

If not registering using BRN then data will not be retrieved and all fields need to be typed in manually.
3. Group of companies Administrator Type

Under the Group of companies Administrator type, one can register as one main entity (company) or have the possibility to add other companies which they are responsible for.

This type of Administrator will have to choose if the Group of company will have several companies to register as Processor/Controller (option Yes) or only one company (option No).

4. Organisation Administrator Type

This type is catered for organisation such as societe, trust, ministries having or not having a BRN.

4.1 Organisation with BRN

User Type: Organisation

Register using Business Registration Number (BRN)?

Business Registration Number (BRN): *

Issue Date of Bus. Reg. Card: *

Organisation Name: *

Company Number:

Date of Incorporation:

Contact Details
4.2 Organisation without BRN

The remaining fields below must be typed in manually and fields highlighted in red are mandatory fields for all the four types of Administrator.

Once all fields are filled, the applicant can upload required documents before submitting the application.

The Administrator will get an acknowledgement email and will be notified once Data Protection Office (DPO) has verified the request and granted Administrator access to the portal.
5. **Home Page**

Once respective administrator is granted access, they will be able to start their application or manage their organisations or representatives depending on which type of administrator is logged in.

Depending on the type of Administrator, the menu displayed on the left will be different.

- **Logged in as Management Company.**
  - Will get menu to manage Organisations, query applications for Controllers/Processors and to query Transaction’s history for all organisations being managed by the Company.
- **Logged in as Organisation**
  - Will get menu to add Representatives who will be granted access to register Controller/Processor on behalf of the company, Query list of applications and list of transactions.

- **Logged in as Individual/Representative**
  - A representative will get the menu to register as Controller/Processor as well as to renew application once expiry date is near (that is 3 months prior of expiry date).
This function is used by Administrators registered as Management Companies or Group of companies to add or terminate companies falling under their management. Each of the companies listed will have their own controller/processor certificate. The Administrator can upload document related to each company as well as list down all the representatives who will register applications their behalf.

To add a new organisation under your management, click on the ‘New Organisation’ button, and fill in form accordingly.
7. Manage Representatives

Manage Representatives function is used by all Administrators. This function allows administrator to list down the different representatives who will make applications for controller/processor on their behalf. They can upload relevant document to the representative as well as terminate its access using this function.
To add new Representative, click on the ‘New Representative’ button on the right top corner.

If a representative already exists for organisations, select and choose it in the dropdown list from the Existing Representative tab as shown next.

In case it is a new representative, fill details for new Representative.

If administrator needs to terminate a representative access to the system or is no longer acting as its representative, the former can modify the representative details and terminate its access by click on the ‘Disactivate’ button. Once clicked, termination date will be filled with current date and representative will receive an email acknowledging that his/her access have been revoked for company concerned.
This function is used to link existing Certificates to a specific registered controller/processor. If the certificate number of a controller/processor does not appear in the portal, choose the button Link Certificate on the left menu and input all relative details:

1. Certificate Number
2. Name Displayed on Certificate
3. Certificate start Date.

Note: If the certificate is already shown on the Dashboard under the ‘Registered Certificate’ section, user does not need to link certificate.
9. **Register Application by representative**

To register new application as controller or processor, representative has to select which organisation application is being made for.

Once organisation is selected, the application form will be opened to fill in application and quit anytime and come back to where they left it. The application will be saved as draft in the applicant’s dashboard.

Click on ‘Next’ to move on to the next section until Declaration and Documents section is reached and submit application.

- Step 1 displays the controller/Processor Details
- Step 2 displays the representative data.

Both steps are auto populated upon application and can be amended accordingly if there are changes.

- On step 3, user must select from Drop down list or typed in value in the other box for each category.
- On step 4 and step 5, fill in details only if applicable.
- Same as step 1, Select from drop down list or input in ‘other’ box.

<table>
<thead>
<tr>
<th>Measures for protection of personal data</th>
<th>Safeguards/security measures</th>
<th>Implementation to protect personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>Visitor's logbook</td>
<td></td>
</tr>
<tr>
<td>Unauthorized recordings of video recordings of students' hours online</td>
<td>Privacy policy</td>
<td></td>
</tr>
<tr>
<td>Unauthorized disclosure Theft</td>
<td>Information security policy</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Other:</td>
<td></td>
</tr>
</tbody>
</table>

Step 7 (Contract with Controller) is only shown when applying for Processor only.

- Table of fees is displayed.
- In exceptional case, applicant has to check whether they are exempted to any fee payment and input the number of employees they have. The fee to pay will be updated with respect to the table displayed on top.
Choose mode of payment, insert captcha and submit application. There are four modes of payment that are accepted by the DPO which are Cash, Cheque, Adjustment Voucher (Government Department only) and E-Payment by credit card. Once application is submitted, applicant will be able to check the application status on the application query screen.

On submission of application, applicant will receive an acknowledgement email, requesting the latter on the amount of fees to pay. If fees are paid using the online payment facility, the applicant will receive a payment acknowledgment email and the receipt on the email.
Upload necessary documents
10. **Renew Application**

Ensure that you have completed the link certificate as described in section 8 above.

In order to renew application, click on the ‘Renew Application’ menu. Once clicked, you will be prompted with the renew Dialog Box in which you will be required to select organisation’s certificate to be renewed and input the respective Certificate Number.
In case Certificate could not be found, user will be prompted to input additional Details. Details include the Name on the Previous Certificate and the Start Date of Previous Certificate. Once Certificate is found, user will be redirected to fill in the pre-filled application form with previously input data. You can then proceed to amend application and submit to DPO for vetting once payment completed.
11. **Query Application**

Application query is separated into 2 categories, one for controller and one for processor. The next Screen shows a history of all application, and applicant can download the application or certificate once completed.

Status of application shown are as follows:

1. **Completed**
   Indicates application has been fully processed and Certificate Generated.
2. **Submitted**
   Indicates Application has been submitted to be vetted by the DPO.
3. **Awaiting Payment**
   Applicant need to pay Registration or Renewal Fee for Application.
4. **In Process**
   Application is being processed at the DPO.
5. **Awaiting Amendments**
   Application was sent back to applicant on the portal to make necessary amendments. Applicant will receive a mail with all information that need to be amended, and need to re-submit application once completed.
6. **Rejected**
   Application has been rejected by the DPO and no certificate generated.
12. **Online Payment**

If any payment is pending to be made by the applicant, the application will appear on the Dashboard as shown in the screenshot below.

When applicant click on the ‘Click to Pay’, the latter will be directed to the SBM Online Platform to effect payment. Once payment is successful, the applicant will receive an acknowledgement email with the receipt attached as an attachment.
Sample of email received to applicant with receipt.

12. **View Certificate**
After the application for controller/processor is approved, a server signed certificate will be generated in the portal of the applicant and an email will be sent to the applicant. This certificate can be viewed in the applicant’s portal under registered certificate.

13. **Query Transactions**
Screen used to query transactions made. User can view what kind of payment method was used in each transaction and if not paid, can pay fee using the various mode of payment including E-payment facility.
14. Register Online Complaint

A legal entity, that is, a person or corporate body is given the facility to lodge a complaint online as well as to track the status of the complaint.

The user can create his/her ONLINE complaint using the “New Complaint” in the Complaints page.

The complaint has 5 sections:

- Section 1, Complainant. The “Complainant” tab allows the user to input data about the Complainant. The complainant can be individual or organisation. In case of organisation, a representative must fill company data and its data. There are some mandatory fields that cannot be empty:
  - Organisation: name, street and town/village
  - Representative: NID, name, email and phone number
  - Individual: NID, name, email and phone number
Section 2, Respondent. The “Respondent” tab allows the user to input data about the Respondent as well as the person dealt with if the respondent is an organisation. “Name of organisation or individual” cannot be empty.
- Section 3, Complaint Details. The “Complaint Details” tab allows the User to input data about the details of
the complaint event. “This is my complaint” cannot be empty. The User can select the “Type of Complaint”
by clicking on the dropdown list. Other option is available if the complaint type is not in the list. If the
complaint exceeds 10000 characters, the user can upload a document under the “Documents” section.

- Section 4, Declaration. The “Declaration” tab allows the User to input data about declaration. If the
declaration exceeds 10000 characters, the user can upload a document under the “Documents” section.
- **Section 5, Documents:** The “Documents” tab allows the User to:
  - upload documents in case the complaint or the declaration exceed 10000 characters.
  - upload any documents he wants to add for his/her complaint.

The document size cannot be higher than 5MB and the allowed documents type are zip, pdf, doc, docx, jpg, jpeg and png.

After uploading a document, the user can add a description, view the uploaded file or remove it. After submitting, the uploaded documents cannot be removed.
Before submitting a complaint, the user must tick the box for acknowledging that the declaration is true and correct.

The user can save the complaint as a draft till he/she wants to submit the same. The user will get a temporary unique reference number and he/she will be able to add new info or document to the complaint. When the complaint is complete the user can submit it. After submitting a complaint, the user will get a new unique reference number to use it to check the status in the complaint page.

The user can finally print a copy for saving the complaint as pdf. It’s possible to print a complaint if saved as draft as submitted.
15. Query Online Complaints

The user can search for his/her complaint(s) in the complaint page. He/she can find information and filter complaints by reference number, respondent, submitted date, complaint type and status.

The status can be:
- Draft
- Submitted
- In Process
- Closed

The user can view the complaint details. If the complaint is a draft, the user can add data and documents and print the complaint. If the complaint is submitted, in process or closed, the user can view data only and print the complaint.

The user can upload more documents if the complaint is submitted or in process, in order to send them to DPO office (for example: the DPO officer is asking for).
16. Register Anonymous Complaint

This function allows a complainant without any user credentials to register a complaint from the DPO website.

The user can create his/her complaint using the “New Complaint” button under the “Submit a New Anonymous Complaint” section.

The complaint has 4 sections:

- Section 1, Complainant. The “Complainant” tab allows the user to input data about the Complainant. If the complainant wishes to remain anonymous, fields may be left empty.
Section 2, Respondent. The “Respondent” tab allows the user to input data about the Respondent as well as the person dealt with if the respondent is an organisation. “Name of organisation or individual” cannot be empty.

<table>
<thead>
<tr>
<th>Complainant</th>
<th>Respondent</th>
<th>Complaint Details</th>
<th>Declaration</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>NID:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Name:</td>
<td>Last Name:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block / House No.:</td>
<td>Street:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locality:</td>
<td>Town / Village:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>District:</td>
<td>Postcode:</td>
<td>Select</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Address:</td>
<td>Occupation:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone No.:</td>
<td>Mobile No:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **My complaint is against:**
  (name of organisation or individual)

- **Block / House No.:**
  (name of your contact person, if any within the organisation)

- **Locality:**
  (name of your contact person, if any within the organisation)

- **District:**
  (name of your contact person, if any within the organisation)

- **Street:**
  (name of your contact person, if any within the organisation)

- **Town / Village:**
  (name of your contact person, if any within the organisation)

- **Postcode:**
  (name of your contact person, if any within the organisation)

Section 3, Complaint Details. The “Complaint Details” tab allows the User to input data about the details of the complaint event. “This is my complaint” cannot be empty. The User can select the “Type of Complaint”
by clicking on the dropdown list. Other option is available if the complaint type is not in the list. If the complaint exceeds 10000 characters, the user can upload a document under the “Documents” section.

<table>
<thead>
<tr>
<th>Complainant</th>
<th>Respondent</th>
<th><strong>Complaint Details</strong></th>
<th>Declaration</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Type of Complaint</strong>: Camera Surveillance System</td>
<td>on</td>
<td>Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>This is my complaint</strong>:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(10000 characters remaining)

If your complaint exceeds 10000 number of characters, kindly upload your complaint as a separate document in the document tab.

- **Section 4, Documents**: The “Documents” tab allows the User to:
  - upload documents in case the complaint details and complaint declaration exceed 1000 characters.
  - upload any documents he wants to add for his/her complaint.

The document size cannot be higher than 5MB and the allowed documents type are zip, pdf, doc, docx, jpg, jpeg and png.

After uploading a document, the user can add a description, view the uploaded file or remove it. After submitting, the uploaded documents cannot be removed.
Before submitting a complaint, the user must tick the box for acknowledging that the declaration is true and correct.

After submitting a complaint, the user will get a unique reference number to use it to check the status. The user can finally print a copy for saving the complaint as pdf.
17. Search for an Anonymous Complaint

The anonymous user can search for his/her complaint(s) by inputting the reference number, got it after submission, in the “Reference” field under the “Search for an Anonymous Complaint” section and clicking on the “Search” button. The status will appear in the “Status” field.

The status can be:
- Submitted
- In Process
- Closed
- No Complaint Reference found, if reference number isn’t correct.

![Search for an Anonymous Complaint Interface](image)
18. Eforms

The following eForms are available on the DPO Portal for Controllers/Processors to submit a request:
- Transfer of personal data abroad
- Notification of personal data breach
- Data Protection Impact Assessment (DPIA)
- Compliance Audit
- Certification Form

18.1 Transfer of Personal Data Abroad

The transfer of personal data abroad eform has 5 sections:

- Section 1, Organisation’s Details. The “Organisation’s Details” tab allows the user to choose the controller / processor certificate data. All data will be automatically filled after choosing in the drop-down list. There are some mandatory fields that cannot be empty:
  o Company Name
  o Street, town / village
  o Telephone Number, Email Address

- Section 2, Organisation’s Details. The “Organisation’s Details” tab allows the user to input the purpose of the proposed transfer/s and the types of personal data to be transferred.
- Section 3, Country/ies to transfer data. The “Country/ies to transfer data” tab allows the user to input the list of countries and their respective data protection rules. The list is empty initially. The user can add a country, using the ‘Add Country’ button. It’s possible to remove a country using the ‘Remove Country’ button.

- Section 4, Appropriate Safeguards. The “Appropriate Safeguards” tab allows the user to input a description for each appropriate safeguard. If a control is ticked, its description is mandatory.
Section 5, Documents. See chapter 0

18.2 Notification of Personal Data Breach

The notification of personal data breach eform has 3 sections:

- Section 1, Particulars of controller giving the notification. The “Particulars of controller giving the notification” tab allows the user to choose the controller / processor certificate data. All controller’s data will be automatically filled after choosing in the drop-down list. There are some mandatory fields that cannot be empty:
  - Company name
  - Street, town / village
  - Telephone Number, Email Address

The user must fill some additional data. There are some mandatory fields that cannot be empty:
  - Name of processor, where the data breach occurred (if applicable)
  - Designation Data of protection officer:
    - Name
    - Designation
    - Telephone Number
    - Email address
Section 2, Details. The “Details” tab allows the user to response to all the controls, adding description.

<table>
<thead>
<tr>
<th>Nature of the personal data breach</th>
<th>2. Nature of the personal data breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controls</td>
<td>Short Description</td>
</tr>
<tr>
<td>(a) When did the personal data breach happen?</td>
<td></td>
</tr>
<tr>
<td>(b) If there has been a delay (more than 72 after becoming aware of the incident and reporting it to the Data Protection Office), please provide your justifications for the delay</td>
<td></td>
</tr>
</tbody>
</table>

In the page a ‘Notes’ button is available to have more information about the eform
18.3 Data Protection Impact Assessment (DPIA)

The data protection impact assessment eform has 3 sections:

- Section 1, Particulars of controller giving the notification. The “Particulars of controller giving the notification” tab allows the user to choose the controller / processor certificate data. All controller’s data will be automatically filled after choosing in the drop-down list. There are some mandatory fields that cannot be empty:
  - Company name
  - Street, town / village
  - Telephone Number, Email Address

  The user must fill some additional data. There are some mandatory fields that cannot be empty:
  - Name of processor, where the data breach occurred (if applicable)
  - Designation Data of protection officer:
    - Name
    - Designation
    - Telephone Number
    - Email address

Notes

1. Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2. Controller means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.

3. Processor means a person who, or public body which, processes personal data on behalf of a controller.

4. Data subject means an identified or identifiable individual; in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

5. Special categories of personal data in relation to a data subject, means personal data pertaining to:
   (a) his racial or ethnic origin;
   (b) his political opinion or adherence;
   (c) his religious or philosophical beliefs;
   (d) his membership of a trade union;
   (e) his physical or mental health or condition;
   (f) his sexual orientation, practices or preferences;
   (g) his genetic data or biometric data uniquely identifying him;
   (h) the commission or alleged commission of an offence by him;
   (i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or
   (j) such other personal data as the Commissioner may determine to be sensitive personal data.
Section 2, Details. The “Details” tab allows the user to respond to all the controls, adding description.
### Step 5: Risks Assessment

<table>
<thead>
<tr>
<th>Risks No</th>
<th>Description</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Risk 1</td>
<td>Frequent</td>
<td>Critical</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Risk 2</td>
<td>Occasional</td>
<td>Insignificant</td>
<td>Low</td>
</tr>
</tbody>
</table>

### Step 5: Measures to mitigate risks

<table>
<thead>
<tr>
<th>Risks No</th>
<th>Measures to mitigate risks</th>
<th>Effect of Measures on risks</th>
<th>Residual Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Measure 1</td>
<td>Eliminated</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Measure 2</td>
<td>Reduced</td>
<td>Low</td>
</tr>
</tbody>
</table>
18.4 Compliance Audit

The compliance audit eform has 3 sections:

- Section 1, General Information. The “General Information” tab allows the user to choose the controller / processor certificate data. All controller’s data will be automatically filled after choosing in the drop-down list. There are some mandatory fields that cannot be empty:
  o Company name
  o Street, town / village
  o Telephone Number, Email Address

  The user must fill some additional data. There is a mandatory field that cannot be empty:
  o Name of data protection officer
- Section 2, Details. The “Details” tab allows the user to response to all the controls, replying yes, no or N/A and adding description to each control.

- Section 3, Documents. See chapter 0
18.5 Certification Form

The certification eform has 3 sections:

- **Section 1, Particulars of controller/processor.** The “Particulars of controller/processor” tab allows the user to choose the controller / processor certificate data. All controller’s data will be automatically filled after choosing in the drop-down list. There are some mandatory fields that cannot be empty:
  - Company name
  - Street, town / village
  - Telephone Number, Email Address

The user must fill some additional data. There are some mandatory fields that cannot be empty:
  - Contact person details:
    - Name
    - Designation
    - Telephone Number, Email Address

- **Section 2, Details.** The “Details” tab allows the user to response to all the controls, replying yes, no or N/A and adding evidence and relevant section in the uploaded document. The user must press the button to
upload one or more document for each control. It is possible to upload the same document in different controls.

**APPLICATION CERTIFICATION FORM**

<table>
<thead>
<tr>
<th>Particulars of controller/processor</th>
<th>Details</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Registration and Renewal (Sections 17 & 18)**

<table>
<thead>
<tr>
<th>Audit Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Evidence / Document</th>
<th>Upload / annex relevant documents</th>
<th>Relevant section(s) in document</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How do you ensure that a change in any of the particulars referred to in your application form for registration as controller/processor is communicated to the Data Protection Office?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Is your registration as controller/processor up to date?</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**APPLICATION CERTIFICATION FORM**

**Attachments**

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Uploaded by</th>
<th>Add Description</th>
<th>Submitted</th>
<th>View</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFORMS-FLow.pdf</td>
<td>APEIM</td>
<td></td>
<td>NO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- **Section 3, Documents. See chapter 0**

In the page a ‘Notes’ button is available to have more information about the eform.

**Data Protection Certification Assessment**

Instructions to controller/processor:
- Please provide clear, factual and accurate answers to the questions in the Data Protection Certification Assessment.
- Please tick Yes, No or N/A as appropriate.
- If the answer is Yes, please attach additional details and evidence as annexure.
- If the answer is No or N/A, please attach the reasons and justifications as annexure.
- Please use the Annexure to provide additional details and evidences.
- Each question should be labelled as per the Question No. in the document.
- For e.g Annex for Question 8 should be labelled as Annex 8.
- Please use the formatting as it is in the document and update the table of content accordingly.
- Please attach a printed copy of the filled Data Protection Certification Assessment Questionnaire and the evidence upon submission of the application for Certification.
- A copy of the filled Data Protection Certification Assessment Questionnaire should be emailed to dpo@govmu.org and the email should be titled as “Data Protection Certification Assessment.”

**18.6 Uploading Documents and Submitting Eforms**

The “Documents” tab allows the user to upload any document which is necessary for the eform. In this section the user can SUMBIT the eform. This section is available in each eform page.

The document size cannot be higher than 5MB and the allowed documents type are zip, pdf, doc, docx, jpg, jpeg and png.

After uploading a document, the user can add a description, view the uploaded file ore remove it, if necessary. After submission, the uploaded documents cannot be removed.
The user can save the eform as a draft till he/she wants to submit the same. The user will get a temporary unique reference number and he/she will be able to add new info or document to the eform. When the eform is complete the user can submit it. After submitting an eform, the user will get a new unique reference number to use it to check the status in the eform page. The DPO and the applicant will receive an email about the new eform with the unique reference number.

The user can finally print a copy for saving the eform as pdf. It’s possible to print an eform if saved as draft as submitted.

18.7 Action Required and Response

DPO can ask the user to modify any control or upload additional or updated files. When DPO needs more information, the user will receive an email with a list of action to complete. The user can query the eform page in order to find the eform needed to be updated. The eform status is ‘Action Required’. When the user opens the eform page, a new button ‘Action Required’ and a new section ‘Action Required’ will appear in the page. The button will show the action required description as the DPO requested for the eform. The user must complete the action required, modifying control, or uploading new documents. When the user has completed its action, he must open the ‘Action Required section’. The user must add an action response description and press the button ‘Send Action Response’. The application will send a mail to DPO officer and to the applicant about the action completed. The eform status is ‘Action Completed’.
### Application Certification Form

**Ref Number:** CERT/2022/1

<table>
<thead>
<tr>
<th>Particulars of controller/processor</th>
<th>Details</th>
<th>Documents</th>
<th>Action Required</th>
</tr>
</thead>
</table>

**Controller / Processor Certificate:** Select

**Name of controller/processor:** Omnicane Management & Consultancy Firm Ltd

**Name of controller:** Omnicane Thermal Energy Plant

<table>
<thead>
<tr>
<th>Block / House No. :</th>
<th>Street :</th>
<th>Town / Village :</th>
</tr>
</thead>
<tbody>
<tr>
<td>no 2</td>
<td>ADOLPH DE PLEVITZ STREET</td>
<td>Souillac</td>
</tr>
</tbody>
</table>

---

**Action Request:**

To submit Records of Processing report updated version.

**Action Response:**

(500 characters remaining)

---

**Action Required from DPO**

To submit Records of Processing report updated version.
18.8 Query EForms

The user can search for his/her eform(s) in the eform page. He/she can find information and filter eforms by reference number, category, submitted date and status.

The status can be:
- Draft
- Submitted
- In Process
- Action Required
- Action Completed
- Approved
- Rejected

The user can view the eform details. If the eForm is a draft or is action required (see the previous chapter), the user can add data and documents and print the eform. If the eform is submitted, in process, action completed, approved, or rejected, the user can view data only and print the eForm.

The user can finally download the letter in case of transfer of personal data abroad and certificate. Once it is approved by DPO.