TRACKWIZZ®
Compliance Without Compromise

# Data Principal Access Request Procedure

| Date | Version | Prepared by | Reviewed & Approved by |
|---|---|---|---|
| 13.01.2025 | 1.0 | DPDP Consultants | Data Protection Officer |
| 28.01.2026 | 1.1 | DPDP Consultants | Data Protection Officer |

## 1. Scope, Purpose and Users

This procedure sets out the key features regarding handling or responding to requests for access to personal data made by data principals, their nominees. This procedure will further TSS Consultancy to comply with legal obligations mentioned under Section 11 of the Digital Personal Data Protection Act, provide better customer care, improve transparency, enable individuals to verify that information held about them is accurate, and increase the level of trust by being open with individuals about the information that is held about them.

This procedure applies broadly across all entities or subsidiaries owned or operated by the Company but do not affect any laws or regulations which may otherwise be applicable.

This procedure applies to employees that handle data principal access requests such as the DPO.

## 2. Reference Documents

- The Digital Personal Data Protection Act, 2023, 11th August 2023, (22 of 2023)
- Personal Data Protection Policy

## 3. Data Principal Access Request (“DPAR”)

A Data Principal Access Request (DPAR) is any request made by an individual or an individual’s legal nominee for information held by the Company about that individual. The Data Principal Access Request provides the right for Data Principals to see or view their own digital personal data as well as to request copies of the data.

A Data Principal Access Request must be made in writing. In general, verbal requests for information held about an individual are not valid DPARs. In the event a formal Data Principal Access Request is made verbally to a staff member of the Company, further guidance should be sought from DPO, who will consider and approve all Data Principal Access Request applications.

A Data Principal Access Request can be made via any of the following methods: email, fax, post, corporate website or any other method. DPARs made online must be treated like any other Data Principal Access Requests when they are received, though the Company will not provide personal information via social media channels.

## 4. The Rights of a Data Principal

As stated under Section 11 (DPDPA, 22 OF 2023) the rights to data principal access include the following:

- Know whether a data fiduciary holds any personal data about them.
- Receive a description of the data held about them and, if permissible and practical, a copy of the data.
- Be informed of the purpose(s) for which that data is being processed, and from where it was received.
- Be informed whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
- If the data is being used to make automated decisions about the data principal, to be told what logic the system uses to make those decisions and to be able to request human intervention.

The Company must provide a response to the data principal requesting access to their data within a reasonable period of receiving the Data Principal Access Request unless Digital Personal Data Protection Act dictates otherwise.

## 5. Requirements for a valid DPAR

In order to be able to respond to the Data Principal Access Requests in a timely manner, the data principal should:

- Submit his/her request using a Data Principal Access Request Form.
- Provide the Company with sufficient information to validate his/her identity (to ensure that the person requesting the information is the data principal or his/her authorized person).

Subject to the exemptions referred to in this document, the Company will provide information to data principal whose requests are in writing (or by some other method explicitly permitted by the DPDPA) and are received from an individual whose identity can be validated by Company.

However, Company will not provide data where the resources required to identify and retrieve it would be excessively difficult or time-consuming. Requests are more likely to be successful where they are specific and targeted at particular information.

Factors that can assist in narrowing the scope of a search include identifying the likely holder of the information (e.g. by making reference to a specific department), the time period in which the information was generated or processed (the narrower the time frame, the more likely a request is to succeed) and being specific about the nature of the data sought (e.g. a copy of a particular form or email records from within a particular department).

## 6. DPAR Process

### 6.1 Request

Upon receipt of a DPAR, the DPO will acknowledge the request. The requestor may be asked to complete a Data Principal Access Request Form to better enable the Company to locate the relevant information.

### 6.2 Identity Verification

The DPO needs to check the identity of anyone making a DPAR to ensure information is only given to the person who is entitled to it. If the identity of a DPAR requestor has not already been provided, the person receiving the request will ask the requestor to provide two forms of identification, one of which must be a photo identity and the other confirmation of address.
If the requestor is not the data principal, written confirmation that the requestor is authorized to act on behalf of the data principal is required.

### 6.3 Information for Data Principal Access Request

Upon receipt of the required documents, the person receiving the request will provide the DPO with all relevant information in support of the DPAR. Where the DPO is reasonably satisfied with

the information presented by the person who received the request, the DPO will notify the requestor that his/her DPAR will be responded to within reasonable time. The reasonable period begins from the date that the required documents are received. The requestor will be informed by the DPO in writing if there will be any deviation from the timeframe due to other intervening events.

6.4 Review of Information

The DPO will contact and ask the relevant department(s) for the required information as requested in the DPAR. This may also involve an initial meeting with the relevant department to go through the request, if required. The department which holds the information must return the required information by the deadline imposed by the DPO and/or a further meeting is arranged with the department to review the information. The DPO will determine whether there is any information which may be subject to an exemption and/or if consent is required to be provided from a third party.

The DPO must ensure that the information is reviewed/received by the imposed deadline to ensure the timeframe is not breached. The DPO will ask the relevant department to complete a "Data Principal Disclosure Form" to document compliance with the reasonable timeframe.

6.5 Response to Access Requests

The DPO will provide the finalized response together with the information retrieved from the department(s) and/or a statement that the Company does not hold the information requested, or that an exemption applies. The DPO will ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The Company will only provide information via channels that are secure.

6.6 Archiving

After the response has been sent to the requestor, the DPAR will be considered closed and archived by the DPO.

The procedure is presented as a flow chart in the Annex of this document.

## 7. Exemptions

As defined under Section 14 sub-section (1) Data Principals have the right, as prescribed by law, to nominate any individual who, in the event of Data Principal death or in case of Data Principal inability to exercise the rights under this law, will exercise Data Principal rights as prescribed here.

The Company is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data principal making the request.

In principle, the Company will not normally disclose the following types of information in response to a Data Principal Access Request:

- Information about other people – Data Principals have the right, as prescribed by law, to nominate any individual who, in the event of Data Principal death or in case of Data Principal inability to exercise the rights under this law, will exercise Data Principal rights as prescribed here.
- Repeat requests – Where a similar or identical request in relation to the same data principal has previously been complied within a reasonable time period, and where there is no significant change in personal data held in relation to that data principal, any further request made within reasonable period of the original request will be considered a repeat request, and the Company will not normally provide further copy of the same data
- Publicly available information – The Company is not required to provide copies of documents which are already in the public domain.
- Opinions given in confidence or protected by copyright law – The Company does not have to disclose personal data held in relation to a data principal that is in the form of an opinion given in confidence or protected by any other law.
- Privileged documents – Any privileged information held by Company need not be disclosed in response to a DPAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and his/her lawyer) and is created for the purpose of obtaining or giving legal advice.

## 8. Data Principal Access Request Refusals

There are situations under Section 11(2), where data principals do not have a right to see information relating to them. For instance:

- Nothing contained in clause (b) or clause (c) of sub-section (1) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorised by law to obtain such personal data, where such sharing is pursuant Right to access information about personal data to a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.
- Requests made for other, non-data protection purposes can be rejected.

If the responsible person refuses a Data Principal Access Request on behalf of the Company, the reasons for the rejection must be clearly set out in writing. Any individual dissatisfied with the outcome of his/her Data Principal Access Request is entitled to make a request to the DPO to review the outcome.

## 9. Responsibilities

The overall responsibility for ensuring compliance with a DPAR rests with the DPO.

If the Company acts as a data fiduciary towards the data principal making the request, then the DPAR will be addressed based on the provisions of this procedure.

If the Company acts as a data processor the DPO will forward the request to the appropriate data fiduciary on whose behalf the Company processes personal data of the data principal making the request.

## 10. Managing records kept on the basis of this document

| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
|---|---|---|---|---|
| Data Principal Access Request Forms | Compliance Department | DPO | Only authorized persons may access the folder | NA |
| Data Principal Disclosure Form | Compliance Department | DPO | Only authorized persons may access the folder | NA |

## 11. Validity and document management

This document is valid as of 2026.

The owner of this document is DPO, who must check and, if necessary, update the document at least once a year.

# Annex: Data Principal Access Request Flowchart