



Data Protection Governance & Grievance Management Policy



Table of Contents

1. Introduction.....	3
2. Definitions	3
3. Purpose.....	4
4. Scope	5
5. Roles and Responsibilities	6
6. Grievance Redressal Procedure	7
7. Confidentiality and Data Security.....	9
8. Record keeping and Reporting.....	9
9. Review of Policy.....	9
10. Exceptions	9
11. Provisions of Non-Compliance	10



Data Protection Governance & Grievance Management Policy

1. Purpose

This Data Protection Governance & Grievance Management Policy is designed by AdGlobal360 to ensure the effective management of grievances related to personal data processing, handling, and protection. The policy aims to establish a transparent, accessible, and accountable process for individuals (data principals) to lodge complaints, seek resolutions, and have their concerns addressed in a timely and efficient manner.

2. Definitions

- **“Data Fiduciary”** means any person who alone or in conjunction with other people determines the purpose and means of processing of personal data.
- **“Data Principal”** means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.
- **“Data Processor”** means any person who processes personal data on behalf of a Data Fiduciary.
- **“Data Protection Board of India”** means the adjudicatory body established under the Digital Personal Data Protection Act, 2023, responsible for determining non-compliance, imposing penalties, and overseeing the enforcement of the provisions of the Act.
- **“Data Protection Officer”** means the person who oversees compliance with data protection laws and acts as the primary contact for data subjects and regulatory authorities.
- **“Digital personal data”** means personal data in digital form.
- **“Grievance”** means any concern, complaint, or objection raised by the Data Principal regarding the collection, processing, storage, sharing, or other handling of their personal data.
- **“Grievance Officer”** means the designated person responsible for overseeing the grievance redressal process by receiving, reviewing, and resolving grievances raised by Data Principals regarding the processing of their personal data.



Data Protection Governance & Grievance Management Policy

- **“Grievance Redressal”** means the process and mechanism established by the Data Fiduciary to receive, address, and resolve complaints or concerns raised by Data Principals regarding the processing of their personal data.
- **“Personal Data”** refers to any information relating to an identified or identifiable natural person ("Data Principal"). This includes identifiers such as name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

3. Purpose

The purpose of this policy is to provide a structured mechanism for individuals to:

- Register grievances related to the collection, use, processing, or handling of their personal data.
- Seek redress in case of non-compliance with the DPDP Act, 2023.
- Ensure the fair and equitable resolution of data privacy concerns.
- Promote transparency and accountability within the organization’s data protection practices.

4. Scope

This policy applies to:

- **Data Fiduciaries** and **Data Processors** involved in the collection, processing, and management of personal data:
 - In the context of job applicants and employees, the Human Resources (HR) department serves as a Data Fiduciary, as it directly collects and processes personal data from these individuals for legitimate employment and recruitment purposes
- **Data Principals** whose personal data is being processed or controlled:
 - All Employees: Including full-time, part-time, contract workers, interns, and consultants of AdGlobal360.
 - All Employment Phases: From recruitment and onboarding to the duration of employment and post-employment data retention.



Data Protection Governance & Grievance Management Policy

- The **Grievance Redressal Mechanism** shall be applicable to all complaints related to data privacy under the jurisdiction of the DPDP Act, 2023.



Data Protection Governance & Grievance Management Policy

The policy covers complaints related to:

- Infringement of the **Rights of Data Principals** under the DPDP Act, 2023 (such as the right to access, correction, erasure, grievance redressal, consent withdrawal and nomination).
- Breaches of data protection practices, including but not limited to improper data handling or processing of personal data.
- Complaints concerning non-compliance with the **Data Protection Principles** under the DPDP Act, 2023.
- Violations of obligations and responsibilities of **Data Processors** and **Data Fiduciaries**.

5. Roles and Responsibilities

➤ **Grievance Officer**

The organization shall appoint a Grievance Officer responsible for:

- Overseeing the grievance redressal process.
- Providing guidance and assistance to data principals in lodging grievances.
- Resolving complaints in a timely manner.
- Reporting to the Data Protection Board (DPB) when required.
- Ensuring compliance with the DPDP Act, 2023.

➤ **Data Protection Officer (DPO)**

The **DPO** supports the Grievance Officer by:

- **Assisting in Investigations:** Providing legal, technical, and procedural support during investigations.
- **Ensuring Compliance:** Ensuring that grievance handling practices align with the provisions of the DPDP Act.
- **Documentation and Reporting:** Maintaining a record of grievances and resolutions and reporting to the **Data Protection Board** as required.



Data Protection Governance & Grievance Management Policy

➤ Data Fiduciaries and Processors

Data Fiduciaries and Processors are responsible for:

- **Providing Assistance:** Cooperating with the grievance officer in addressing complaints related to their respective data processing activities.
- **Addressing Data Concerns:** Taking necessary actions to mitigate any violation of data protection principles during the processing of personal data.

➤ Data Principals

Data Principals have the right to:

- **Lodge a Grievance:** Register complaints regarding any data privacy violations or concerns.
- **Be Informed:** Be kept informed of the grievance status and resolution within the statutory timelines.
- **Request Escalation:** Escalate grievances to the **Data Protection Board (DPB)** if not resolved within the prescribed timelines.

6. Grievance Redressal Procedure

➤ How to Lodge a Grievance

Data principals (individuals) can lodge grievances related to their personal data in the following ways:

- Email: grievance@adglobal360.com
- Written Complaints: Submission of a written grievance to the grievance officer via postal mail or physical delivery.

➤ The grievance must include the following details:

1. Name and contact details of the data principal.
2. Description of the grievance (including the nature of the data concern and specific complaint).



Data Protection Governance & Grievance Management Policy

3. Details of any relevant data processing activity (if available).
4. Any communication previously made with the organization regarding the grievance.
5. Any supporting documents or evidence.

➤ **Acknowledgment of Grievance**

Upon receipt of a grievance, the Grievance Officer will:

- Acknowledge receipt of the grievance within 7 calendar days.
- Provide the data principal with an acknowledgment receipt, detailing the grievance tracking number, the expected timeline for resolution, and contact information.

➤ **Investigation and Resolution**

The Grievance Officer will:

- Investigate the grievance by reviewing the facts and gathering relevant data.
- Consult with the Data Protection Officer (DPO) and other relevant departments as needed.
- Seek clarification or further information from the data principal, if necessary.
- Take corrective action, including remediation of privacy violations, if required.
- Offer compensation or remedies to the data principal if there is a violation of rights or non-compliance with the DPDP Act.

➤ **Escalation Mechanism**

If the data principal is not satisfied with the resolution or if the grievance is not addressed within the prescribed timeframe, the data principal can escalate the matter to the Data Protection Board (DPB), as provided under the DPDP Act, 2023. The DPB will review the grievance and make a binding decision.



7. Confidentiality and Data Security

All grievances, personal data, and associated communication shall be handled with the utmost confidentiality, and personal data will only be disclosed as required to investigate the grievance or as mandated by law. The organization will take appropriate technical and organizational measures to secure data, in accordance with the DPDP Act, 2023.

8. Record keeping and Reporting

The organization will maintain a record of periodic reports regarding the number and nature of grievances received and their resolution.

9. Review of Policy

This Data Protection Governance & Grievance Management Policy will be reviewed at regular intervals, at least twice every year, to ensure compliance with the DPDP Act, 2023, and to address emerging issues and concerns regarding data privacy.

10. Exceptions

While the organization is committed to adhering to the grievance redressal process outlined in this policy, certain exceptional circumstances may affect the ability to resolve grievances within the normal procedure. These exceptions include:

1. **Force Majeure:** In cases of natural disasters, unforeseen events, or other circumstances beyond the organization's control, such as national emergencies, the grievance resolution



Data Protection Governance & Grievance Management Policy

process may be delayed. In such cases, the organization will notify the data principal as soon as possible, outlining the reasons for the delay and providing an updated timeline for resolution.

2. **Grievances Outside the Scope of DPDP Act:** If the grievance relates to matters that are not directly related to personal data processing or fall outside the scope of the **DPDP Act, 2023**, such as general service-related complaints, the organization will notify the data principal and direct them to the appropriate department or external authority.
3. **Invalid or Insufficient Information:** If the grievance is not supported by sufficient or valid information for the organization to process or resolve the issue, the data principal will be informed and given an opportunity to provide the required documentation or clarification. If the data principal fails to do so, the grievance may be closed.
4. **Grievances Already Resolved or Repeated Complaints:** If a grievance has already been addressed and resolved previously, or if the complaint is a repeated one without new information, the grievance may be closed after notifying the data principal.

11. Provisions of Non-Compliance

1. For the Organization:

- **Regulatory Actions:** In the event of non-compliance with grievance redressal obligations, the organization may be liable to a penalty of up to ₹50 crores, as prescribed under the DPDP Act.
- **Reputation Damage:** Loss of customer trust and business.

2. For the Data Principal:

- **Regulatory Actions:** In cases of intentional misuse or negligence or breach in observance of the duties under section 15, the Data Principal may be liable for a penalty of up to **10,000 Rs**, as prescribed under the DPDP Act.