Data Subject Access Request (DSAR)

DATA SUBJECT ACCESS REQUEST

TERAPAGE

www.terapage.ai

Terapage Data Subject Access Request (DSAR)

1. **Purpose:** The purpose of this Data Subject Access Request (DSAR) Measures Document is to outline the procedures and measures Terapage has implemented to ensure compliance with data protection regulations, including GDPR, CCPA, and PIPEDA. This document provides a clear process for handling requests from individuals seeking to exercise their rights to access personal data held by Terapage.
2. **Scope:** This document applies to all personal data processed by Terapage, including data collected from employees, customers, vendors, and other stakeholders. It covers all employees, contractors, and vendors involved in processing personal data and responding to DSARs.
3. **Definitions:**
    - **Data Subject:** An individual whose personal data is processed by Terapage.
    - **Personal Data**: Any information relating to an identified or identifiable individual.
    - **Data Subject Access Request (DSAR)**: A request made by a data subject to access their personal data held by Terapage.
    - **Data Protection Officer (DPO)**: The person responsible for overseeing data protection strategy and compliance at Terapage. Data Protection Officer (DPO): The person responsible for overseeing data protection strategy and compliance at Terapage.
4. **Roles and Responsibilities:**
    - **Data Protection Officer (DPO):**
        - Oversees the DSAR process and ensures compliance with data protection regulations.
        - Coordinates responses to DSARs and maintains records of all requests.
    - **IT Department:**
        - Assists in locating and retrieving personal data in response to DSARs.
        - Ensures the security and integrity of personal data during the DSAR process.
    - **Legal Department:**
        - Provides legal guidance on DSAR compliance and handles any legal challenges or queries.
    - **Employees and Contractors:**

- Forward any received DSARs to the DPO promptly.
- Assist in the DSAR process as needed.

5. DSAR Process:

5.1. Receipt of Request

- **Submission Methods:**
  - DSARs can be submitted via email to dpo@Terapage.ai
  - Requests can also be submitted through the Terapage website's DSAR portal.
  - Written requests can be sent to Terapage's corporate address.
- **Acknowledgment:**
  - Upon receipt of a DSAR, the DPO will acknowledge the request within 5 business days.
  - The acknowledgment will include information about the next steps and the expected timeline for response.

5.2. Verification of Identity

- **Verification Process:**
  - The DPO will verify the identity of the requestor to ensure the request is legitimate.
  - Acceptable verification methods may include government issued identification, recent utility bills, or other relevant documents.
  - If the identity cannot be verified, the DPO will request additional information from the requestor.

5.3. Data Collection

- **Data Identification:**
  - The DPO will coordinate with relevant departments to identify and locate the personal data requested.
  - Data sources may include databases, email systems, physical records, and third-party systems.
- **Data Retrieval:**
  - The IT Department will assist in retrieving the identified data.
  - Ensuring that all retrieved data is secure and maintains its integrity throughout the process.

5.4. Data Review and Redaction

- **Review Process:**
  - The DPO will review the retrieved data to ensure it complies with the DSAR.
  - Any data that may infringe on the privacy rights of other individuals will be redacted.
  - The Legal Department will review the redacted data to ensure compliance with legal requirements.

5.5. Response to Request

- **Data Delivery:**
  - The personal data will be provided to the requestor in a secure and accessible format.
  - Data may be delivered electronically via secure email or through the DSAR portal, or in hard copy if requested.
- **Timeframe:**
  - Terapage will respond to DSARs within 30 days of receipt.
  - If additional time is needed, the requestor will be informed, and an extension of up to 60 days may be applied as allowed by law.

5.6. Record Keeping

- **Documentation:**
  - All DSARs and responses will be documented and stored securely.
  - Records will include the request, verification steps, data retrieved, and the final response provided.
- **Retention Period:**
  - Records of DSARs will be retained for a minimum of five years or as required by law.

6. Legal and Regulatory Compliance:

- **GDPR Compliance:** Ensure DSARs comply with Article 15 of the GDPR, allowing data subjects to access their personal data.
- **CCPA Compliance**: Adhere to CCPA requirements, providing data subjects with access to their personal information upon request.
- **PIPEDA Compliance**: Comply with PIPEDA regulations, ensuring data subjects can access their personal data held by Terapage.

7. Training and Awareness:

- **Employee Training:**
  - Provide regular training on data protection and DSAR procedures to all employees.
  - Include DSAR training in new employee onboarding programs.
- **Awareness Programs:**
  - Conduct regular awareness campaigns to reinforce the importance of data protection and the DSAR process.
  - Use newsletters, posters, and intranet updates to disseminate information.

8. Monitoring and Review:

- **Regular Monitoring:**
  - Monitor compliance with DSAR procedures through regular audits.
  - Use automated tools to track DSAR requests and responses.
- **Policy Review:**
  - Review and update this DSAR Measures Document annually or whenever significant changes occur in data protection laws or business operations.
- **Approval:**
  - Obtain approval from senior management for policy updates and changes.

9. Reporting and Incident Management:

- **Incident Reporting:**
  - Report any incidents related to DSARs promptly to the DPO.
  - Investigate and document all incidents, implementing corrective actions as necessary.
- **Incident Response:**
  - Develop and maintain an incident response plan to address issues related to DSARs.
  - Ensure incidents are resolved promptly to minimize impact.

Reviewed by:	Moses Lion
Title:	Compliance Analyst
Date:	05/07/2024

Approved by:	Mandeep Sidhu
Title:	Head of Compliance

Date:	31/07/2024