Status **Draft** PolicyStat ID **20569762**

UNIVERSITY OF WEST GEORGIA

Last Approved	N/A
Effective	N/A
Next Review	N/A
Area	IT/ Management (Procedures)
Responsible Party	Chief Legal Officer

Data Subject Request (DSR) Process

Authority for Procedure granted by UWG Policy #5003, Privacy.

The University of West Georgia (UWG) maintains the following Data Subject Request (DSR) process in alignment with the University System of Georgia (USG) Business Procedures Manual (BPM), Section 12: *Data Governance and Management*. This procedure outlines roles, responsibilities, and steps for receiving and responding to DSRs.

A. Data Subjects Request Overview

A Data Subject Request (DSR) is a formal request from an individual seeking to access, correct, delete, or otherwise exercise their privacy rights regarding personal data held by the University of West Georgia (UWG).

B. Governance and Ownership

1. System Level - University System Office (USO)

The USG Data Privacy Committee provides system-level oversight of DSR processes for all USG institutions and reviews institutional activity reports.

2. Institutional Level - University of West Georgia

Information Technology Services (ITS) serves as UWG's designated Process Manager for the Data Subject Request (DSR) process.

UWG's Data Privacy Governance Committee is composed of representatives from the following units, with additional subject-matter experts included as needed to support DSR review and decision-making:

- Information Technology Services (ITS)
- Cybersecurity (ITS)

- Legal Affairs (OLA)
- University Relations/Communications (UCM)
- Risk/Compliance/Management (OLA)
- Office of Human Resources (OHR)
- Registrar's Office

C. Communication Plan

Clear and consistent communication is required and integrated throughout the DSR lifecycle. All communications must:

- Acknowledge receipt within required legal or policy timelines.
- Provide status updates at key milestones, including verification, internal review, delays, extensions, and fulfillment.
- Notify internal stakeholders when their action is required.
- Use consistent and approved institutional language.
- Be logged and retained in accordance with records management requirements.

All communications are part of the official DSR record.

D. Process Summary

UWG follows an eight-step process for managing DSRs.

1. **Submission** – The Data Subject submits a request to UWG's Process Manager and governance within the institution.
2. **Tracking** – The request is logged in the secured tracking system, which includes recording the request and actions taken.
3. **Identity Verification** – UWG verifies the requester's identity.
4. **Legitimacy Verification** – UWG confirms whether the request is valid and actionable.
5. **Analysis** – The DSR is reviewed to determine necessary actions, including who needs to be involved and the relevant systems involved.
6. **Determination** – Requested actions (e.g., correction, deletion, restriction) are reviewed and confirmed.
7. **Fulfillment** – Approved actions to the DSR are completed.
8. **Closing and Documentation** – Chief Legal Officer reviews and determines final disposition; the DSR is formally closed.

Each action taken is documented in the tracking system, ensuring that all processing steps are traceable and suitable for quarterly reporting to the USG Data Privacy Committee. A visual representation of the process flow is available in the USG Data Subject Request Process Flow Diagram (Appendix A).

E. Detailed DSR Steps

1. Submission

The DSR process begins when a Data Subject submits a request through a University-approved channel (i.e., the Data Subject Request Submission Form). An acknowledgment of receipt of the DSR is issued to the requester, consistent with the Communication Plan.

2. Tracking

Upon receipt, the DSR is logged in the DSR tracking system, developed and maintained by Information Technology Services (ITS), which supports the full lifecycle of DSR management, including intake, documentation, workflow automation, and historical tracking.

The Process Owner notifies the Data Privacy Governance Committee that the University has received a DSR.

3. Identity Verification

The Process Owner, in coordination with the Office of Legal Affairs, verifies the identity of the requestor and confirms the legitimacy of the DSR before processing. If additional information is required to verify identity or validate the request, the requester is notified. Verification may include:

- Knowledge-based questions,
- UWG login credentials,
- Multi-factor authentication, or
- Third-party verification tools when appropriate.

4. Legitimacy Verification

The legitimacy (i.e., validity and actionability) of a DSR is based on the nature/type of request, as well as the systems/data involved. If the request can reasonably be fulfilled, it will be marked as Founded (i.e., legitimate). If the DSR cannot be fulfilled, the requestor is notified, and at which time the requestor may modify their request. Unfounded (i.e., illegitimate) requests may be denied, with an explanation to the requestor.

All communications related to identity and legitimacy verification comply with the Communication Plan to ensure timely and clear updates.

5. Analysis

Once a DSR is verified as Founded, UWG conducts a multi-level analysis to identify required actions and determine all systems where relevant data may reside. The analysis includes:

- **Governance Committee** – initial review of the request.
- **Process Manager** – analysis of impacts to applications or system where data is stored,

managed, processed, etc., including coordination with **Sub-Processors** when their systems contain relevant data.

This analysis is guided by the **Record of Processing Activities (RoPA)**, which identifies responsible parties, associated systems, and Sub-Processors. (See the USG RoPA Process Guide for additional details).

All analysis notes and supporting documentation are maintained in the designated tracking system.

6. Determination

Based on the analysis results, UWG issues, upon review and approval of the Chief Legal Officer, a formal determination to the requester, which may include:

- **Access** – Providing a copy of or confirmation about personal data held.
- **Portability** – Supplying data in a transferable format.
- **Rectification** – Correcting inaccurate or incomplete information.
- **Erasure** – Deleting eligible personal data that meets required criteria.
- **Objection or Restriction** – Limiting or ceasing processing in appropriate circumstances.
- **Denial or Partial Fulfillment** – When legal limitations prevent full compliance, UWG provides justification.

Documentation of the decision is maintained for reporting and audit purposes.

7. Fulfillment

Once the determination notice is issued, UWG implements the required actions and communications. The **Process Manager**, **Data Stewards**, or **Sub-Processors** carry out the applicable steps noted above, such as providing access, correcting data, deleting records, denying the request (with justification), or partially fulfilling it when only certain portions of the request are eligible for action.

When data resides in systems outside UWG's direct control, **Sub-Processors** or system vendors may be engaged to complete the request. Process examples for institutional reference are included in Appendices B-F.

If additional time is required due to volume or complexity, progression and/or extension notices will be issued to the requester in accordance with the Communication Plan.

All determination and actions follow the Communication Plan.

8. Closing and Documentation

After fulfillment is complete, UWG issues final communications and confirmations to the requester in accordance with the Communication Plan.

Once a determination is issued, the final disposition (i.e., completed and/or fulfilled; partial fulfillment; denied; not legitimate; etc.) of the DSR is reviewed by UWG's Chief Legal Officer. Information Technology Services (ITS), as Process Manager and administrator of the DSR tracking system, is responsible for the

operational closing, workflow automation, and retention/storage management of the DSR record within the designated system.

All documentation (e.g., communications, decisions, data logs, and supporting materials) are archived in accordance with UWG Records Retention Schedules. The request is then marked as complete in the tracking system, formally closing the case.

Reporting

It is essential that all actions taken on a DSR be fully documented in the designated tracking system, ensuring that all processing steps are traceable and suitable for quarterly reporting to the USG Data Privacy Committee.

Timelines

Timelines for processing DSRs will follow applicable laws, regulations, and contractual obligations. When extensions are legally permissible, the requestor will be notified promptly.

Recordkeeping

The University of West Georgia is governed by federal, state, and local laws that may limit our ability to satisfy a DSR in full. The University has a Records Retention Policy that governs the required retention and deletion timelines for University records, including those that contain personal data.

Definitions

Analysis - refers to a specific review by a particular organizational unit regarding what the data subject requests be done with their data.

Communication - refers to written dialogue directly with a data subject regarding their DSR.

Data Subject - any individual whose personal data is collected, processed, or stored.

Data Subject Request (DSR) - is a petition to an organization by a data subject looking to confirm whether or not the organization is holding personal data about the data subject petitioning, and if so, data subject has the right to access that data, amend that data, or where permitted by law request the data to be erased.

Erasure - allowance of a data subject requesting personal information to be removed/deleted if it meets the validation criteria.

Founded - refers to a DSR with both a verified data subject and a legitimate data subject request and can be accepted and processed accordingly.

Governance - refers to all employees and/or parties involved in processing the organization's DSRs.

Management - refers to the process and organization of steps in fulfilling a DSR.

Process Manager - refers to an individual employee and/or a unit of a USG institution that has ownership and is the Principal Processor over the DSR process.

Processing - refers to fulfilling or addressing the details of the DSR.

Record of Processing Activities Process (RoPA) - is a comprehensive inventory of all processes that a Process Manager or Sub-Processor performs.

Records - refers to stored data around the historical and/or real-time management of a DSR and/or any actions taken concerning specific DSRs.

Sub-Processors - are any businesses or contracted services that have been engaged to process data at the request of a USG organization (e.g., vendors, contractors, other USG organizations).

Timely - refers to acknowledging receipt of a DSR, in writing, within 72 hours and determining actions within 30 days, then conveying those actions to the data subject, in writing.

Tracker - refers to a system the institution will utilize/put in place to track DSR requests.

Unfounded - refers to a DSR where either the data subject cannot be verified and/or there is not a legitimate data subject request, or both and cannot be accepted and is denied processing.

Guidelines/Related material

- USG DSR Process Guide webpage
- USG DSR Process Guide (PDF)
- Business Procedures Manual (BPM), Section 12: *Data Governance and Management*
    - BPM Section 12.04.02 Classification
    - BPM Section 12.06.02 Data Risk Management
    - BPM Section 12.06.05. Data Processing Awareness

Forms

Data Subject Request Submission Form

Attachments

- APPENDIX A: DSR PROCESS FLOW DIAGRAM.pdf
- APPENDIX B: PROCESS FOR ACCESS AND PORTABILITY REQUESTS.pdf
- APPENDIX C: PROCESS FOR ERASURE REQUESTS.pdf
- APPENDIX D: PROCESS FOR RECTIFICATION REQUESTS.pdf
- APPENDIX E: PROCESS FOR OBJECTION REQUESTS.pdf
- APPENDIX F: PROCESS FOR ACCESS RESTRICTION REQUESTS.pdf

Approval Signatures

Step Description	Approver	Date