Procedure: **Data Subject Request (DSR) Process**

Authority for Procedure granted by **UWG PL #5003, Privacy**

The University of West Georgia (UWG), as a member of the University System of Georgia (USG), has implemented a Data Subject Request process to maintain compliance with the [USG Business Process Manual (BPM)](https://www.usg.edu/). This procedure defines the terms, roles, responsibilities, and actions associated with the DSR Process.

Use this document in conjunction with the [USG Business Procedures Manual (BPM)](https://www.usg.edu/), Section 12.

### A. Data Subjects Request Overview

A DSR is a request to an organization from an individual (aka a Data Subject) for which data is stored.

#### 1. Process Flow

The DSR process at UWG includes the following **eight-step** process.

- **Step One:** The DSR is submitted by a Data Subject to a Process Manager and governance within the organization.
- **Step Two:** The DSR is managed using a tracking system, which includes recording the request and any actions taken.
- **Step Three:** The Data Subject’s identity is verified.
- **Step Four:** The DSR’s legitimacy is verified.
- **Step Five:** Analyze the DSR (including who needs to be involved and what systems data is within) and determine necessary actions.
- **Step Six:** The necessary actions requested are analyzed and verified.
- **Step Seven:** Verified actions to the DSR are implemented.
- **Step Eight:** The completed DSR is reviewed by General Counsel and closed.

**Note:** For a visual representation of process flow, please refer to the USG Data Subject Request Process Flow Diagram *(Reference Appendix A)*

1 The determination of who needs to be involved and what systems data is within is the Record of Processing Activities (RoPA) process. See USG RoPA Process Guide for more details.

### B. DSR Process Ownership And Governance (Step One)

#### 1. Ownership and Governance – USO-Level Overview

The USO Data Privacy Committee serves as the system-level governance entity for DSRs for all USG institutions. The USO Data Privacy Committee directly manages any DSRs submitted to the USO using the DSR Process Flow and oversees organizational DSR management. The USG Office of Organizational Effectiveness currently manages the USO Data Privacy Committee.
2. **Ownership and Governance – Organizational Data Governance Overview**

Information Technology Services is designated as UWG’s Process Manager.

UWG’s Data Privacy Governance Committee includes representatives from the following units to review DSRs and may, as needed, include additional personnel as content experts.

- Information Technology Services (ITS)
- Cybersecurity (ITS)
- Legal Counsel (OLA)
- University Relations/Communications (UCM)
- Risk/Compliance/Management (OLA)
- Human Resources (HR)
- Registrar

C. **DSR Tracker For Management And Records (Step Two)**

UWG will track Data Subject Requests via a secured Smartsheet. The sheet, developed and maintained by the process owner (ITS), will facilitate the collection, management, and historical tracking of all DSRs received by UWG. The sheet will also facilitate automated workflows to streamline the processing of DSRs.

D. **Identity And Legitimacy Verification Process (Steps Three And Four)**

1. **Identity Verification Process**

UWG will rely primarily on the methods listed below for identity verification:

- Method 1 – Knowledge-based authentication
- Method 2 – User Login/Account credentials
- Method 3 – Multi-factor authentication
- Method 4 – Outsource to a third party

2. **Legitimacy Verification Process**

The Process Owner, in coordination with the Office of Legal Affairs, will review the request and determine its legitimacy based on the nature of the request, the type of request, and the systems/data involved in the request. If the request can reasonably be fulfilled, it will be marked as legitimate. If the request cannot be fulfilled, the requestor will be notified as to why at which time the requestor may modify their request. A DSR that is determined to be illegitimate is “Unfounded” and may be denied.

E. **DSR Analysis (Step Five)**

1. **Analysis Process**

There will be different levels of analysis by the institution with each DSR, including

- Initial analysis by the Governance Committee upon receipt of the DSR;
- Analysis by General Counsel or designee, and
- Analysis by the Process Manager, if the DSR is Founded (legitimate) and the data impacts applications and/or systems. These applications/systems and their Process Managers or Sub-Processors are identified within the Record of Processing Activities process (RoPA).

*Note: UWG will capture documentation of the analysis at each level within the determined tracking system.*

F. **Verification And Implementation (Steps Six And Seven)**
1. **Processing Levels**

There are different levels of processing by the institution regarding each DSR. In certain instances, the Process Manager may not have control of the requested data and will have the Sub-Processor acquire the requested data. The DSR may include requests for:

- Access and Portability (Appendix B);
- Erasure (Appendix C);
- Rectification (Appendix D);
- Objection (Appendix E); and
- Restriction (Appendix F).

**Note:** Process examples are provided in the Appendix for institutional consideration. It is essential for the institution to capture documentation of what is processed for a DSR within the determined tracking system and report to the USO Data Privacy Committee on, at a minimum, a quarterly basis.

G. **DSR Closure (Step Eight)**

1. **Closure Process**

UWG’s General Counsel will determine final disposition (i.e., completed and/or fulfilled; partial fulfillment; denied; not legitimate; etc.) of all DSRs and will be documented within the designated tracking system.

H. **DSR Communication Plan**

1. **Communication Triggers**

UWG’s process includes the following communications:

- Acknowledgment of receipt of the DSR to the Data Subject (Step One);
- Communicate with the governing committee that a DSR has been received (Step Two);
- Communicate with General Counsel or designee to verify DSR legitimacy. (Step Three)
- Communicate with the Data Subject to verify identity, if needed (Step Four);
- Communicate with the Process Manager and/or Sub-Processors (systems where data is stored, managed, processed, etc.) around any necessary actions (e.g., data corrections, restrictions, erasures, etc.) (Step Five);
- Communicate with the Data Subject the progression of their DSR (Step Six);
- Communicate with the Data Subject the actions/determinations around their DSR (Step Seven); and
- Communicate with the Data Subject the closing/conclusion of their DSR (Step Eight).

**Note:** It is an expectation that each USG institution shall provide, at a minimum, a quarterly DSR report to the USO Data Privacy Committee.

**Definitions**

**Access** - is the allowance of a data subject to obtain a copy or a confirmation concerning the possession or processing of personal data.

**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.

**Objection** - is the allowance of the data subject to object to processing their personal data in certain circumstances (e.g., direct marketing).

**Portability** - is the allowance of a data subject to move, copy, or transfer personal data from one digital environment to another safely and securely without affecting usability.

**Process Manager** - refers to an individual employee and/or a unit of a USG institution that has ownership and is the Principle 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.

**Rectification** - is the allowance of a data subject to request inaccurate or incomplete personnel data to be rectified.

**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.

**Forms**

**Data Subject Request Submission Form**
APPENDIX B: PROCESS FOR ACCESS AND PORTABILITY REQUESTS

1. **Description**: The Process Manager defines the search parameters to generate a report on all locations where data responsive to the DSR request may be found. Utilization of the RoPA will be instructive for this purpose. Searches are run on all applicable systems. Search results containing relevant information on the Data Subject are compiled, and data collected. The Process Manager verifies the accuracy and completeness of the search results.

   **Search recommendation:**
   
   (a) Utilize the Process Manager’s identification system to help identify all documents responsive to the DSR request.
   
   (b) Update the DSR tracker with a record of the search parameters used, locations of responsive personal data identified, and search results.

   **Accountable: Process Manager**

2. **Description**: The Process Manager fulfills any technical search requests, and a summary of technical search steps taken should be recorded in the DSR tracker.

   **Accountable: Process Manager**

3. **Description**: The Process Manager determines if all responsive data was available and accessible or if they need to reach out to any Sub-Processors to request that they search their systems.

   **Accountable: Process Manager**

4. **Description**: If the Process Manager determines that all responsive data is available and accessible on their systems, the request and search results is reviewed and, if necessary, escalates to General Counsel. Escalation to General Counsel may be necessary where the results contain:

   (a) Privileged information (e.g., requests for legal advice from outside counsel, etc.);
   
   (b) Information related to other Data Subjects, including employees;
   
   (c) Proprietary information that may reveal business confidential information; and
   
   (d) Information relating to the prevention or detection of criminal activities.

   **Accountable: Process Manager**

5. **Description**: If a Process Manager believes a Sub-Processor(s) may have data responsive to the access request, a request for assistance is sent to determine whether or not this is the case. The requirement for Sub-Processors to assist in this endeavor should be contained in the contract between the USG/institution and the Sub-Processor.

   **Accountable: Process Manager and any Sub-Processor(s)**

6. **Description**: Based on the DSR request and instruction from the Institutional Data Privacy Governance Committee, the Process Manager determines whether the Data Subject requested that their data be made Portable or simply Accessible.

   **Accountable: Process Manager**

7. **Description**: If the Process Manager determines that the Data Subject requested that their data be made Accessible, the Process Manager sends a copy of the personal data requested to the Institutional Data Privacy Governance Committee. The Institutional Data Privacy Governance Committee performs a quality review and drafts an email response to the Data Subject.

   **Accountable: Process Manager and Institutional Data Privacy Governance Committee**

8. **Description**: If the Process Manager determines that the Data Subject requested that their data be made Portable, the Process Manager must convert the data into an appropriate electronic format (structured, commonly used, and machine-readable format) to transfer or migrate to the requested organization.

   **Accountable: Process Manager**
9. **Description:** The Institutional Data Privacy Governance Committee sends an email notification to the Data Subject that the request has been fulfilled, provides a link/secure folder of requested personal data and then closes the DSR tracker entry.

   **Accountable:** Institutional Data Privacy Governance Committee

10. **Description:** The Data Subject receives an email response to their data request from the Institutional Data Privacy Governance Committee containing (1) a data file, (2) a link to a secure site containing the data pertinent to the DSR request, or (3) a confirmation that the data has been transferred or migrated (if applicable).

    **Accountable:** Data Subject

11. **Description:** The Process Manager receives notice from the Institutional Data Privacy Governance Committee that the request has been fulfilled and closes the DSR tracker entry.

    **Accountable:** Process Manager
APPENDIX C: PROCESS FOR ERASURE REQUESTS

1. **Description**: The Process Manager defines the search parameters to generate a report on all locations where data responsive to the DSR request may be found. Utilization of the RoPA will be instructive for this purpose. The Process Manager updates the DSR tracker entry with a record of the search parameters and the locations of the identified responsive personal data.

   **Accountable**: Process Manager

2. **Description**: The Process Manager fulfills any technical search requests, and a summary of technical search steps taken by the Process Manager should be recorded in the DSR tracker.

   **Accountable**: Process Manager

3. **Description**: Based on the RoPA and the search results, the Process Manager determines if the institution can fulfill the erasure request without Sub-Processor assistance or other technical resources. If the Process Manager is unsure, assistance will be requested from the Sub-Processor to search their systems for data responsive to the erasure request. The Process Manager reports its findings to the Institutional Data Privacy Governance Committee.

   **Accountable**: Process Manager and Sub-Processor(s)

4. **Description**: The Process Manager reports the findings from its search report to the Institutional Data Privacy Governance Committee in writing (email). The Institutional Data Privacy Governance Committee determines whether:

   (a) Erasure of the identified data is possible, and
   (b) Whether any exceptions exist to allow the Institutional Data Privacy Governance Committee to refuse the erasure.

   The Process Manager may suggest a course of action to reject the erasure request, but the decision ultimately lies with the Institutional Data Privacy Governance Committee. Questions the Institutional Data Privacy Governance Committee may use to assist with this determination:

   (a) Is the data still necessary for the Institutional Data Privacy Governance Committee’s purposes?
   (b) Is the Data Subject to a legal hold?
   (c) Does the Institutional Data Privacy Governance Committee need to retain the data for regulatory or compliance purposes?

   **Accountable**: Process Manager and Institutional Data Privacy Governance Committee

5. **Description**: If erasure is possible, and the Institutional Data Privacy Governance Committee determines that there are no reasons to reject the erasure request, the Process manager must delete all responsive personal data identified.

   (a) The Process Manager must record the erasure methods used, including the systems and assets targeted for erasure.
   (b) If the Process Manager determines that personal information is contained in records that need to be maintained, the Process Manager can decide to permanently and irreversibly mask the personal data to anonymize the records. This decision must be recorded and reported to the Institutional Data Privacy Governance Committee.
   (c) If the Process Manager determines that the responsive data also lies on its Sub-Processors’ systems, the Process Manager must communicate the requirement to erase the responsive data down its chain of Sub-Processors.

   **Accountable**: Process Manager

6. **Description**: If the Process Manager requests, the Sub-Processor must erase the responsive data identified in their systems. The Sub-Processors must confirm to the Process
Manager when this is completed and the steps taken to erase the personal data.

Accountable: Sub-Processor

7. **Description:** The Process Manager marks the DSR tracker entry as complete once either:
   
   (a) Confirmation of deletion has been communicated to the Institutional Data Privacy Governance Committee; or
   
   (b) The Institutional Data Privacy Governance Committee informs the Process Manager that it does not have to delete the personal data based on one or more reasons.

Accountable: Process Manager

8. **Description:** The Institutional Data Privacy Governance Committee notifies the Data Subject of the action it has taken based on the erasure request, either that:
   
   (a) The Data Subject’s personal data has been erased, along with a high-level summary of the steps taken to delete the data; or
   
   (b) The Institutional Data Privacy Governance Committee is rejecting the Data Subject’s erasure request, along with the reason for the rejection and the possibility of lodging a complaint.

Accountable: Institutional Data Privacy Governance Committee
APPENDIX D: PROCESS FOR RECTIFICATION REQUESTS

1. **Description**: The Process Manager defines the search parameters to generate a report on all locations where data responsive to the DSR request may be found. Utilization of the RoPA will be instructive for this purpose.

   (a) The request must be strictly followed if the Data Subject requests that contact details be updated for only one property or contract, the search and rectification should be limited and should not involve all of the places where the Data Subject’s contact details can be found.

   (b) The Process Manager updates the DSR tracker entry with a record of the search parameters and the locations of the identified responsive personal data.

   Accountable: Process Manager

2. **Description**: The Process Manager fulfills any technical search requests and a summary of technical search steps taken by the Process Manager should be recorded in the DSR tracker.

   Accountable: Process Manager

3. **Description**: The Process Manager determines whether, based on the RoPA and the search results, Process Manager can fulfill the rectification request without needing to reach out to Sub-Processors.

   (a) If the Process Manager is unsure, they should contact the Sub-Processors and request assistance with searching their systems for data responsive to the erasure request.

   (b) The Process Manager reports its findings to the Organizational Data Privacy Governance Committee.

   Accountable: Process Manager

4. **Description**: If the Process Manager believes that a Sub-Processor(s) may have data responsive to the rectification request, the Process Manager must reach out and request assistance to determine whether or not this is the case.

   Accountable: Process Manager and Sub-Processor

5. **Description**: Based on the nature of the request and the responsive information identified, the Organizational Data Privacy Governance Committee determines whether it is possible to rectify the personal data at issue.

   Accountable: Institutional Data Privacy Governance Committee

6. **Description**: If the Institutional Data Privacy Governance Committee determines that making the correction requested by the Data Subject is not possible, the Institutional Data Privacy Governance Committee must communicate this decision to the Data Subject and allow the Data Subject to submit a supplementary statement to be attached to the record(s) in question.

   Accountable: Institutional Data Privacy Governance Committee

7. **Description**: The Data Subject may provide a supplementary statement pertaining to their request to rectify the personal data.

   Accountable: Data Subject

8. **Description**: If it is possible to rectify the personal data in question, the Process Manager makes the rectification in its systems. The Process manager may request assistance from any Sub-Processor(s) to fulfill the request. If it is not possible to rectify the personal data in question, but the Data Subject has provided a supplementary statement, the Process Manager attaches that statement to the records in question and records the rectification in the DSR tracker entry and notifies the Institutional Data Privacy Governance Committee of same.

   Accountable: Process Manager
9. **Description**: If the Process Manager determined that the responsive data was partially located on the systems of its Sub-Processor(s), the Process Manager requests that the relevant Sub-processor(s) either:

   (a) Rectify the personal data in question; or

   (b) Add the supplied supplementary statement to the records. **Accountable: Process Manager**

10. **Description**: If the Process Manager requests, the Sub-Processor either rectifies the personal data in question or attaches the supplied supplementary statement to the records. **Accountable: Sub-Processor**

11. **Description**: The Process Manager closes the DSR tracker entry once notified by the Institutional Data Privacy Governance Committee of the actions the Sub-Processors, if necessary, have taken. **Accountable: Process Manager**

12. **Description**: The Institutional Data Privacy Governance Committee notifies the Data Subject of the action its action to rectify (or supplement) the personal data in question. **Accountable: Institutional Data Privacy Governance Committee**
APPENDIX E: PROCESS FOR OBJECTION REQUESTS

1. **Description**: The Institutional Data Privacy Governance Committee determines whether the DSR request relates to personal data that has been processed based on legitimate interests as a legal basis. If Institutional Data Privacy Governance Committee is uncertain for any reason as to the legal basis for processing the personal data in question, it may reach out to the Process Manager for assistance.

   **Accountable**: Institutional Data Privacy Governance Committee and Process Manager

2. **Description**: If the Institutional Data Privacy Governance Committee determines that either:
   
   (a) The DSR request does not relate to personal data, the processing of which is/was based on legitimate interests; or
   
   (b) The DSR request relates to personal data, the processing of which is/was based on legitimate interests, but that it has a compelling legitimate interest in continuing to process the data that overrides the Data Subject’s right to object to the processing

   The Institutional Data Privacy Governance Committee communicates to the requestor its rejection of the request and the underlying rationale, including the Data Subject’s right to lodge a complaint.

   **Accountable**: Institutional Data Privacy Governance Committee

3. **Description**: If the Institutional Data Privacy Governance Committee is uncertain whether the DSR request is based on legitimate interests as a legal basis, and it reaches out to the Process Manager to confirm its understanding, the Process Manager can assist as needed. The institution’s RoPA will be instructive for this purpose

   **Accountable**: Process Manager

4. **Description**: If the Institutional Data Privacy Governance Committee determines that the processing of the DSR request is based on legitimate interests as a legal basis, the Institutional Data Privacy Governance Committee then has the opportunity to determine whether it has any compelling legitimate interest(s) that may override the Data Subject’s right to object to the Institutional Data Privacy Governance Committee’s processing of that personal data.

   **Accountable**: Institutional Data Privacy Governance Committee

5. **Description**: If the Institutional Data Privacy Governance Committee cannot identify a compelling legitimate interest that would allow it to override the Data Subject’s right to object to its processing, it must stop its processing of the in-scope personal data and send a request to the Process Manager to do the same.

   **Accountable**: Institutional Data Privacy Governance Committee

6. **Description**: Upon receipt of notice from the Institutional Data Privacy Governance Committee to stop processing the in-scope personal data, the Process manager halts said processing and communicates the order to all relevant business units (e.g., marketing, customer relations).

   **Accountable**: Process Manager

7. **Description**: If an objection request relates to any information that the Sub-Processor is processing, the sub-Processor halts its processing of the in-scope personal data.

   **Accountable**: Sub-Processor

8. **Description**: The Process Manager confirms to the Institutional Data Privacy Governance Committee that the processing of the in-scope personal data is halted and close the DSR tracker entry.

   **Accountable**: Process Manager

9. **Description**: The Institutional Data Privacy Governance Committee notifies the Data Subject that it has halted processing their in-scope personal data.

   **Accountable**: Institutional Data Privacy Governance Committee
APPENDIX F: PROCESS FOR ACCESS RESTRICTION REQUESTS

1. **Description**: The Institutional Data Privacy Governance Committee decides whether the restriction request is valid, for example:

   (a) The Data Subject contests the accuracy of the personal data held by the USG organization;

   (b) The USG organization does not (or no longer has) a lawful basis under which to process the Data Subject’s personal data, but the Data Subject does not want the data erased;

   (c) The USG institution no longer needs the personal data for the purposes it originally collected the data, but the Data Subject needs the organization to retain the data to establish, exercise, or defend a legal claim; and/or

   (d) The Data Subject exercised (according to regulations) their right to object.

   **Accountable**: Institutional Data Privacy Governance Committee

2. **Description**: If the Institutional Data Privacy Governance Committee determines that the request is invalid, it informs the Data Subject of the rejection and the underlying rationale, as well as the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

   **Accountable**: Institutional Data Privacy Governance Committee

3. **Description**: If the Institutional Data Privacy Governance Committee determines that the request is valid, it marks the in-scope personal data to restrict its processing and sends a request to the Process Manager. If the restriction is only temporary, when available, the Institutional Data Privacy Governance Committee must include the timeline for restriction and release of restriction to the Process manager.

   **Accountable**: Institutional Data Privacy Governance Committee

4. **Description**: Upon receipt of Institutional Data Privacy Governance Committee’s instruction to restrict processing the in-scope data, the Process Manager marks the in-scope personal data in its systems to restrict its processing. If any of the in-scope data is, or might be, contained on Sub-Processors’ systems, the Process Manager instructs Sub-Processor(s) to do the same. If the restriction is only temporary, when available the Process Manager must include the timeline for restriction and release of restriction to its Sub-Processor(s).

   **Accountable**: Process Manager

5. **Description**: The process manager sends confirmation to the Organizational Data Privacy Governance Committee that the restriction request has been fulfilled. The process manager updates the DSR tracker entry and either:

   (a) Closes the DSR tracker entry if the restriction is permanent; or

   (b) Calendars the date that the restriction will be lifted in the DSR tracker. **Accountable**: Process Manager

6. **Description**: The Institutional Data Privacy Governance Committee notifies the Data Subject that their restriction request has been fulfilled.

   **Accountable**: Institutional Data Privacy Governance Committee

7. **Description**: If the restriction was temporary, but the Institutional Data Privacy Governance Committee is unable to give the Process Manager a specific date on which the restriction would be lifted, then when lifted the Institutional Data Privacy Governance Committee instructs the Process Manager to restart processing the in-scope personal data.

   **Accountable**: Institutional Data Privacy Governance Committee

8. **Description**: If and when notified by the Institutional Data Privacy Governance Committee of the lifting of the restriction on processing, the Process Manager restarts processing the in-scope personal data. If the Process Manager originally instructed Sub-Processor(s) to
restrict the processing of the in-scope data, the Process manager instructs Sub-Processors that the restriction has been lifted and to restart processing the in-scope personal data. The Process Manager records in the DSR tracker the entry the date the processing the in-scope personal data restarted, the instruction from the Institutional Data Privacy Governance Committee to do so, and closes the entry.

Accountable: Process Manager

9. **Description:** If the restriction request related to any information that the Process manager Sub-Processor was processing, the Sub-Processor restarts its processing of the in-scope personal data.

Accountable: Sub-Processor