UNIVERSITY SYSTEM
OF GEORGIA

DATA SUBJECT REQUESTS PROCESS GUIDE

Version 1

Table of Contents

1.0 Introduction

The University System of Georgia (USG) comprises public institutions of higher learning, a University System Office (USO), Georgia Public Library System (GPLS), Shared Services Center (SSC), Georgia Archives and Georgia Film Academy; hereinafter referred to as USG organizations.

The following terms of **Shall**, **Will**, **Must**, **May**, **May Not**, and **Should** are used throughout this document.

1. **Shall**, **Will** and **Must** indicate a legal, regulatory, standard or policy requirement. **Shall** and **Will** are used for persons and organizations. **Must** is used for inanimate objects.
2. **May** indicates an option.
3. **May Not** indicates a prohibition.
4. **Should** indicates a recommendation that, in the absence of an alternative providing equal or better protection from risk, is an acceptable approach to achieve a requirement.

This document should be used in conjunction with the USG *Business Procedures Manual* (BPM) Section 12.

1.1 Definitions

The following definitions are used throughout this document.

- **Access** is the allowance of a data subject to obtain a copy or confirmation concerning the possession or processing of personal data.
- **Analysis** refers to a specific review by a particular organizational unit in regard to what the data subject is requesting be done in regard to their data.
- **Communication** refers to written dialogue directly with a data subject in regard to their DSR.
- **Data subject** is any person whose personal data is being 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** is the allowance of a data subject to request personal information obtained to be removed/deleted if it meets the criteria of validation.
- **Founded** refers to a DSR that has 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 the processing of 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 the processing of 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 in a safe and secure manner without affecting usability.
- **Process Manager** refers to an individual employee and/or a specific unit of a USG organization 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 of the processing activities that a process manager or sub-processor at the direction of the process manager performs.
- **Records** refers to stored data around the historical and/or real-time management of a DSR and/or any actions taken in relation to 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 organization is going to utilize/put in place in order 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.

2.0 Data Subjects Request Overview

A DSR is a request to an organization from someone (a data subject) for which data is being stored.

2.1 Process Flow

In accordance with BPM Sections 12.4.2, 12.6.2 and 12.6.5 (pending approval), USG organizations must provide a way for a data subject to submit a DSR. The DSR process shall include 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 (to include who needs to be involved and what systems[1]) and determine any necessary actions.
- Step Six: The necessary actions requested are analyzed and verified.

[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.

- Step Seven: Verified actions to the DSR are implemented.
- Step Eight: The completed DSR is reviewed by legal 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***)

3.0 DSR Process Ownership and Governance (Step One)

3.1 Ownership and Governance – USO-Level Overview

The USO Data Privacy Committee will serve as the system-level governance entity for DSRs throughout the USG. The USO Data Privacy Committee will directly manage any DSRs submitted to the USO using the DSR Process Flow, as well as oversee organizational DSR management. The USO Data Privacy Committee is currently managed by the USG Office of Organizational Effectiveness.

3.2 Ownership and Governance – Organizational Data Governance Overview

In accordance with BPM Section 12.2.1, USG organizations should determine an individual employee and/or a specific unit of the organization which is the "process manager" and principle processor of the organization's overall DSR process. Once determined, this individual/unit's information should be provided to the USO Data Privacy Committee as a point of contact. Each organization shall report, at a minimum, on a quarterly basis to the USO Data Privacy Committee in regard to any DSRs the organization is managing.

USG organizations should use existing data governance structure or establish new structure to govern the DSR process, herein referred to as the Organizational Data Privacy Governance Committee. Recommendations for representatives from the following organizational departments/units should be considered in the charge of an already established committee or in forming a new committee:

- Information Technology
- Cybersecurity
- Legal Counsel
- University Relations/Communications
- Risk/Compliance/Management
- Human Resources
- Registrar

4.0 DSR Tracker for Management and Records (Step Two)

Tracker Management and Records

USG organizations shall determine a method, utilizing current resources, to track DSRs. This tracker should allow for historical and real-time access to any DSR for the organization.

5.0 Identity and Legitimacy Verification Process (Step Three and Four)

5.1 Identity Verification Process

USG organizations shall establish a process in order to verify the identity of any data subject submitting a DSR to the institution for review/processing. It is critically important that the institution knows for sure that the DSR has been submitted by the actual data subject.

5.2 Legitimacy Verification Process

USG organizations shall establish a process for legal counsel to verify the DSRs legitimacy. A DSR that is determined legitimate is a ***founded*** DSR and may be accepted and processed accordingly. A DSR that is determined to be illegitimate is an ***unfounded*** DSR and may be denied.

6.0 DSR Analysis (Step Five)

6.1 Analysis Process

There will be different levels of analysis by the organization in regard to each DSR, to include:

- Initial analysis by the governance committee upon receipt of the DSR;
- Analysis by legal counsel, and
- Analysis by process manager, if the DSR is legitimate and the data impacts their 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: *It is important for the organization to capture documentation of the analysis at each level within the determined tracking system.*

7.0 DSR Processing–Verification and Implementation (Step Six and Seven)

7.1 Processing Levels

There will be different levels of processing by the organization regarding each DSR. In certain instances, the process manager may not have control of the data requested and will have to reach out to a sub-processor to 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 organization consideration. It is important for the organization to capture documentation of what is processed for the DSR within the determined tracking system and report this to the USO Data Privacy Committee on, at a minimum, a quarterly basis.*

8.0 DSR Closure (Step Eight)

8.1 Closure Process

USG organizations must create procedures around closure of a DSR and the possible dispositions (i.e. completed and/or fulfilled; partial fulfillment; denied; not legitimate; etc.) It is recommended that organizations engage legal counsel in confirming/approving closure.

Note: *It is important for the organization to capture documentation of DSR closure, including request disposition, within the determined tracking system.*

9.0 DSR Communication Plan

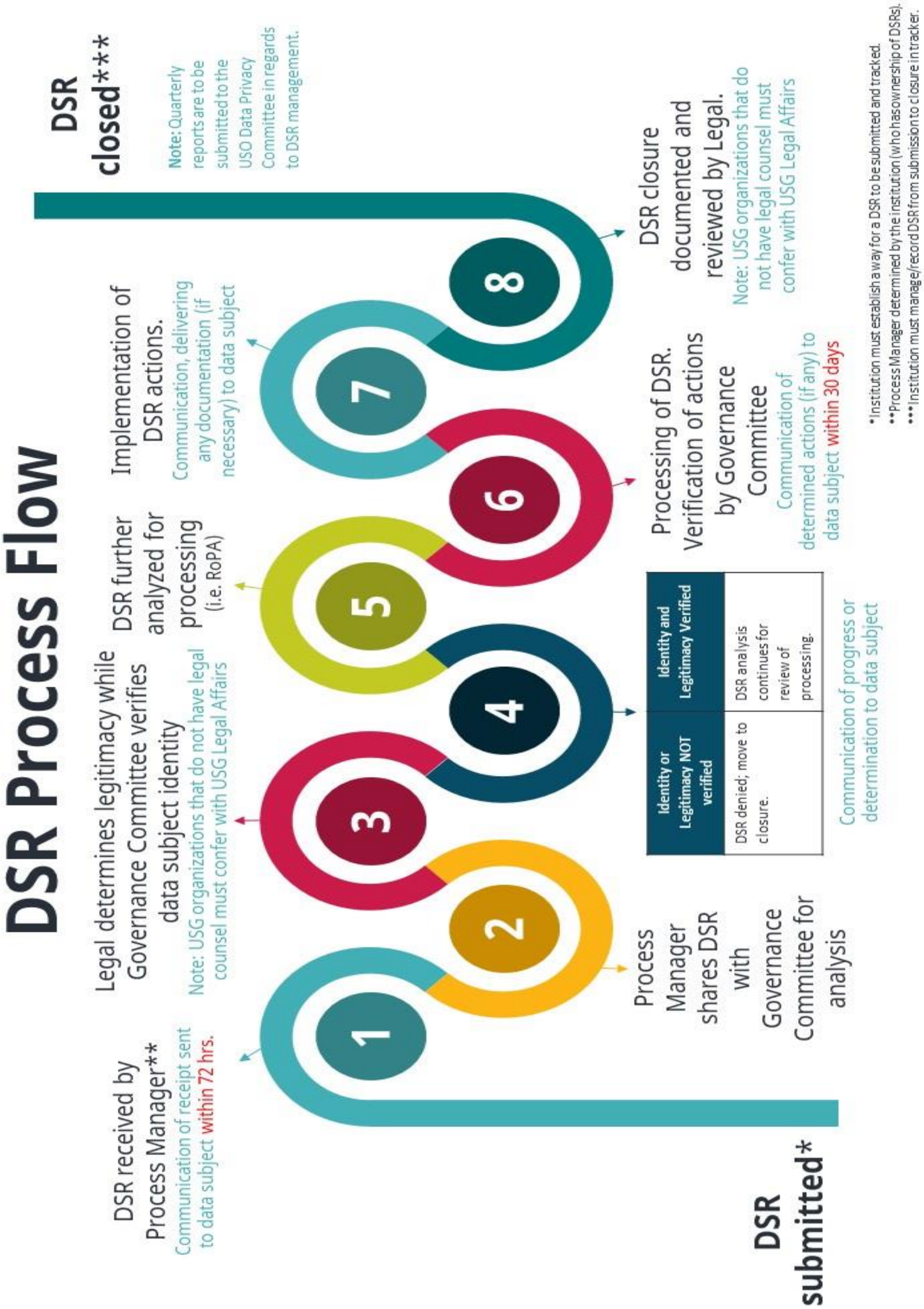
9.1 Communication Triggers

USG organizations should build into each step of their DSR processes the following communications:

- Acknowledgement 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 legal counsel to verify legitimacy of the DSR. Note: USG organizations that do not have legal counsel must confer with USG Legal Affairs (Step Three);
- Communicate with the data subject to verify identity (Step Four);
- Communicate with any 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 in regard to progression of their DSR (Step Six);
- Communicate with the data subject in regard to actions/determinations around their DSR (Step Seven); and
- Communicate with the data subject in regard to closing/conclusion of their DSR (Step Eight).

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

APPENDIX A: DSR PROCESS FLOW DIAGRAM



Appendix B: Example of Procedures 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 is 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 he/she needs 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, he/she reviews the request and search results and, if necessary, escalate to legal counsel. Escalation to legal 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, he/she must reach out and request assistance 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 entered into between the USG/organization and the sub-processor.

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

6. Description: The process manager determines, based on the DSR request and instruction from the Organizational Data Privacy Governance Committee, whether the data subject requested that his/her data be made portable or simply accessible.

    Accountable: Process Manager

7. Description: If the process manager determines that the data subject requested that his/her data be made accessible, the process manager sends a copy of the personal data

requested to the Organizational Data Privacy Governance Committee. The Organizational Data Privacy Governance Committee performs a quality review and drafts an email response to the data subject.

Accountable: Process Manager and Organizational Data Privacy Governance Committee

8. Description: If the process manager determines that the data subject requested that his/her data be made portable, the process manager must convert the data into an appropriate electronic format (structured, commonly used, and machine-readable format) so that it can be transferred or migrated to the requested organization.

   Accountable: Process Manager

9. Description: The Organizational Data Privacy Governance Committee sends an email notice to the data subject that the request has been fulfilled and provides a link/secure folder of requested personal data and then closes DSR tracker entry.

   Accountable: Organizational Data Privacy Governance Committee

10. Description: The data subject receives an email response to his/her data request from the Organizational 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 Organizational Data Privacy Governance Committee that the request has been fulfilled and closes the DSR tracker entry.

    Accountable: Process Manager

Appendix C: Example of Procedures 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 DSR tracker entry with a record of the search parameters used and the locations of responsive personal data identified.

   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 he/she is able to fulfill the erasure request without needing to reach out to sub-processors or other technical resources. If the process manager is unsure, he/she should reach out to sub-processors and request assistance with searching their systems for data responsive to the erasure request. The process manager reports its findings to the Organizational 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 Organizational Data Privacy Governance Committee in writing (email). The Organizational Data Privacy Governance Committee makes a determination whether:

   (a) Erasure of the identified data is possible, and

   (b) Whether any exceptions exist to allow the Organizational 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 Organizational Data Privacy Governance Committee. Questions the Organizational Data Privacy Governance Committee may use to assist with this determination:

   (a) Is the data still necessary for the Organizational Data Privacy Governance Committee's purposes?

   (b) Is the data subject to a legal hold?

   (c) Does the Organizational Data Privacy Governance Committee need to retain the data for regulatory or compliance purposes?

   Accountable: Process Manager and Organizational Data Privacy Governance Committee

5. Description: If erasure is possible, and the Organizational 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 make the decision to permanently and irreversibly mask the personal data in order to anonymize the records. This decision must be recorded and reported to the Organizational Data Privacy Governance Committee.

(c) If the process manager determined that the responsive data also lies on its sub-processors' systems, he/she 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 he/she identified in his/her systems. The sub-processor 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 Organizational Data Privacy Governance Committee; or

   (b) The Organizational 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 Organizational 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 Organizational 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: Organizational Data Privacy Governance Committee

Appendix D: Example of Procedures 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) It is important that the request is 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 as such, and should not involve all of the places where the data subject's contact details can be found.

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

    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, the process manager will be able to fulfill the rectification request without needing to reach out to sub-processors.

    (a) If the process manager is unsure, he/she should reach out to 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: Organizational Data Privacy Governance Committee

6. Description: If the Organizational Data Privacy Governance Committee determines that making the correction requested by the data subject is not possible, the Organizational 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: Organizational Data Privacy Governance Committee

7. Description: The data subject may provide a supplementary statement relating to his/her 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 the process manager records that he/she has made the rectification in the DSR tracker entry and notifies the Organizational 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 requested by the process manager, 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 he/she has notified the Organizational Data Privacy Governance Committee of the actions he/she, and his/her sub-processors if necessary, have taken.

    Accountable: Process Manager

12. Description: The Organizational Data Privacy Governance Committee notifies the data subject of the action it has taken to rectify (or supplement) the personal data in question.

    Accountable: Organizational Data Privacy Governance Committee

Appendix E: Example of Procedures for Objection Requests

1. Description: The Organizational Data Privacy Governance Committee determines whether the DSR request relates to personal data that has been processed on the basis of legitimate interests as a legal basis. If Organizational 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: Organizational Data Privacy Governance Committee and Process Manager

2. Description: If the Organizational 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 does relate 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; then

   The Organizational Data Privacy Governance Committee communicates to the requestor its rejection of the request and the underlying rationale, which includes the right of the data subject to lodge a complaint.

   Accountable: Organizational Data Privacy Governance Committee

3. Description: If the Organizational 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 provide assistance as needed. The institution's RoPA will be instructive for this purpose

   Accountable: Process Manager

4. Description: If the Organizational Data Privacy Governance Committee determines that the processing of the DSR request is in fact based on legitimate interests as a legal basis, the Organizational 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 Organizational Data Privacy Governance Committee's processing of that personal data.

   Accountable: Organizational Data Privacy Governance Committee

5. Description: If the Organizational 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: Organizational Data Privacy Governance Committee

6. Description: Upon receipt of notice from the Organizational 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 Organizational Data Privacy Governance Committee that he/she has halted its processing of the in-scope personal data and closes its DSR tracker entry.

   Accountable: Process Manager

9. Description: The Organizational Data Privacy Governance Committee notifies the data subject that it has halted the processing of his/her in-scope personal data.

   Accountable: Organizational Data Privacy Governance Committee

Appendix F: Example of Procedures for Access Restriction Requests

1. Description: The Organizational Data Privacy Governance Committee makes a determination whether the restriction request is valid, for example:

    (a) The data subject contests the accuracy of his/her 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 organization 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 many regulations) his/her right to object.

    Accountable: Organizational Data Privacy Governance Committee.

2. Description: If the Organizational 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 lodging a complaint with a supervisory authority and seeking a judicial remedy.

    Accountable: Organizational Data Privacy Governance Committee.

3. Description: If the Organizational 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 for same. If the restriction will only be temporary, when available the Organizational Data Privacy Governance Committee must include the timeline for restriction and release of restriction to the process manager.

    Accountable: Organizational Data Privacy Governance Committee

4. Description: Upon receipt of Organizational Data Privacy Governance Committee's instruction to restrict processing the in-scope data, the process manager marks the in-scope personal data in its own 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 will only be 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 Organizational Data Privacy Governance Committee notifies the data subject that his/her restriction request has been fulfilled.

   Accountable: Organizational Data Privacy Governance Committee.

7. Description: If the restriction was temporary, but the Organizational Data Privacy Governance Committee was not able to give the process manager a specific date on which the restriction would be lifted, then when lifted the Organizational Data Privacy Governance Committee instructs the process manager to restart processing the in-scope personal data.

   Accountable: Organizational Data Privacy Governance Committee

8. Description: If and when notified by the Organizational 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 entry the date he/she restarted processing the in-scope personal data, as well as the instruction from the Organizational 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.