



UNIVERSITY SYSTEM OF GEORGIA

RECORD of PROCESSING ACTIVITIES (RoPA) PROCESS GUIDE

Version 1

Table of Contents

1.0 Introduction	2
1.1 Definitions	2
2.0 Record of Processing Activity (RoPA) Overview	2
2.1 RoPA Requirements	3
2.2 Process Flow.....	3
3.0 Establishing RoPA Process Ownership and Maintenance (Step One)	3
3.1 Ownership and Maintenance – USO Overview.....	3
3.2 Ownership and Maintenance – Organizational Overview	3
4.0 RoPA Tracker for Management and Records (Step Two)	4
5.0 Identify Division/Department Processors of Personal Data (Step Three)	4
6.0 Identify Mission Critical Systems & Data Owners (Step Four)	4
7.0 Develop List of Data Usage Activities for each Mission Critical System (Step Five)	4
7.1 Description of the Activity	4
7.2 Purpose and Legal Basis of the Activity	5
7.3 Data Collection and Data Processing	5
7.4 Data Storage and Deletion	5
8.0 Develop a RoPA Report and Maintenance Schedule (Step Six)	5
Appendix A: RoPA Process Flow Diagram	6

1.0 INTRODUCTION

The University System of Georgia (USG) is composed of 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 Section 12 of the USG Business Procedures Manual (BPM).¹

1.1 Definitions

The following definitions are used throughout this document:

- **Data subject** is any person whose personal data is being collected, processed, or stored.
- **Mission-Critical Systems** are systems whose failure or malfunction will result in not achieving organizational goals and objectives. Criteria are that the system a.) contains confidential or sensitive data (i.e., personally identifiable information (PII) and other regulated information), and/or b.) serves a critical and necessary function for daily operations.
- **Personally Identifiable Information** refers to any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the institution.
- **Process Manager** refers to an individual employee and/or a specific unit of a USG organization that has ownership and is the principal processor over the RoPA process.
- **Processing** refers to fulfilling or addressing the details of the RoPA.
- **Record of Processing Activities (RoPA)** is a comprehensive inventory of all 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 an organization's RoPA.

2.0 RECORD OF PROCESSING ACTIVITY (RoPA) OVERVIEW

The record of processing activities is an internal record that contains the information of all personal data processing activities carried out on behalf of the organization and/or a reviewed and approved request of a data subject.

¹ BPM Section 12.6 Data Privacy: https://www.usg.edu/business_procedures_manual/section12/C3013.

2.1 RoPA Requirements

1. Inventory all systems processing or storing data to inform the RoPA.
2. RoPA should include the baseline information:
 - a. List each mission-critical system by name that is processing PII.
 - b. List a short description of the systems purpose.
 - c. List the system owner/point-of-contact (POC) information.
 - d. List the data owner/POC information – who can edit data for each system.
 - e. List third-party relationships and POC information for each third-party system.
 - f. List the data processing activities associated with each system.
3. Conduct an annual review of the RoPA to ensure information remains current.

2.2 Process Flow

USG organizations shall document and maintain a RoPA that must include the following iterative six-step process.

- Step One: Determine who will own and maintain the RoPA process.
- Step Two: Determine the media/platform in which the RoPA will be managed and updated.
- Step Three: Create an inventory of the different divisions and/or departments that process data for the USG organization.
- Step Four: Using the inventory of the divisions and/or departments,
 - a) Identify (inventory) the data processing systems, specifically identifying those mission-critical systems that record PII of the USG organization's data subjects,
 - b) Create the RoPA from the mission-critical systems identified, and
 - c) Identify the system/data owners of the USG organization's systems.
- Step Five: Analyze and document the system's data usage activities.
- Step Six: Develop a RoPA report and maintenance schedule for the USG organization.

Note: For a visual representation of process flow, please refer to the USG Record of Processing Activity Process Flow Diagram (*Reference Appendix A*).

3.0 ESTABLISHING ROPA PROCESS OWNERSHIP AND MAINTENANCE (STEP ONE)

Ownership of the process is discussed in the following two perspectives, the University System Office (USO) and the individual USG organizations.

3.1 Ownership and Maintenance – USO Overview

The USO Data Privacy Committee will serve as the university system-level governance entity for the USO RoPA and provide assistance to each USG organization in developing and maintaining their organization's RoPA. The USO Data Privacy Committee can be contacted through the Enterprise Service Desk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3607 (toll free in Georgia).

3.2 Ownership and Maintenance – Organizational Overview

USG organizations shall determine an individual employee and/or a specific unit of the organization which is the "process manager" and principal processor of the organization's overall RoPA process. Once determined, this individual/unit's information shall be provided to the USO Data Privacy Committee as a point of contact through the Enterprise Service Desk (helpdesk@usg.edu) at 706-

583-2001, or 1-888-875-3607 (toll free in Georgia). Each organization shall report annually to the USO Data Privacy Committee regarding the organization's RoPA (*Reference Section 8.0*).

USG organizations may use an existing data governance structure or establish a new structure to govern the RoPA process. 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

Note, this may be the same committee that is overseeing the data subject request (DSR) process.

4.0 ROPA TRACKER FOR MANAGEMENT AND RECORDS (STEP TWO)

Each USG organization shall determine the media/platform in which the RoPA will be managed and updated. USG organizations shall determine a method, form or format utilizing current resources to develop and maintain a RoPA for the organization. The baseline tracker (record) must:

1. List each mission-critical system by name that is processing PII.
2. List a short description of the systems purpose.
3. List the system owner/point-of-contact (POC) information.
4. List the data owner/POC who can edit that data for each system.
5. List third-party relationships and POC at third-party.
6. List the data processing activities associated with each system.

5.0 IDENTIFY DIVISION/DEPARTMENT PROCESSORS OF PERSONAL DATA (STEP THREE)

USG organizations shall establish a list of all divisions and departments within the organization that process data subject information. This can be accomplished by interviewing lead personnel within each identified division and department. This will be a requirement to accomplish Step Four.

6.0 IDENTIFY MISSION CRITICAL SYSTEMS & DATA OWNERS (STEP FOUR)

Using the inventory of the divisions and/or departments, USG organizations shall create an inventory of the data processing systems. Using the inventory of systems to inform the RoPA, USG organizations shall:

1. Identify the mission-critical systems that process PII of the organization's data subjects, and
2. Identify the system/data owners of each system.

7.0 DEVELOP LIST OF DATA USAGE ACTIVITIES FOR EACH MISSION CRITICAL SYSTEM (STEP FIVE)

USG organizations shall identify and list major data usage activities for each mission critical system identified within the organization.

7.1 Description of the Activity

This information to be collected shall include:

1. What the activity is (e.g., adds, moves, changes, and deletions), and
2. The contact person responsible for the activity.

7.2 Purpose and Legal Basis of the Activity

If the activity uses personal data, show the legal justification concerning how the data is obtained (e.g., through consent, processing a contract, or other means). This is the most critical part of records of processing activities.

7.3 Data Collection and Data Processing

There are two fundamental areas of concentration to consider, which are:

1. Understanding the PII collected, if the collected data is to be processed and stored and was it collected with consent, and
2. Determining if the collected data is to be provided to third parties and if so, identify the POCs and confirm they are protecting the data (e.g., through contract review and supplier risk management processes).

7.4 Data Storage and Deletion

Utilizing the data retentions schedule² and the legal basis information collected in *7.2 Purpose and Legal Basis of the Activity* above, determine and list:

1. How long the data is to be stored,
2. The exact location of this storage, and
3. Under what conditions should the data be deleted.

8.0 DEVELOP A ROPA REPORT AND MAINTENANCE SCHEDULE (STEP SIX)

USG organizations shall create procedures around both the initial development of the organization's RoPA and the ongoing maintenance schedule, which at minimum must be on an annual basis.

The USO Data Privacy Committee does not require the USG organizations to submit the procedures for review; however, they must be in place and may be requested (e.g., In support of a legal action, program review or audit engagement).

The required report shall consist of the content within the USG RoPA Report Template, which is found at <https://www.usg.edu/policies/dataprivacy> and shall be submitted to the USO Data Privacy Committee through the Enterprise Service Desk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3607 (toll free in Georgia) by July 31st annually.

² https://www.usg.edu/records_management/schedules/

APPENDIX A: RoPA PROCESS FLOW DIAGRAM

