GDPR - Standard Governing Data Protection and Privacy for Individuals within European Union

ROWAN UNIVERSITY POLICY

Title: General Data Protection Regulation (GDPR)
Subject: Corporate Compliance and Privacy
Policy No: CCP:2018:01
Applies: Rowan University
Issuing Authority: President
Responsible Officer: Chief Audit, Compliance & Privacy Officer and Director of Information Security
Date Adopted: 06/27/2018
Last Revision: 04/30/2021
Last Reviewed: 04/30/2021

I. PURPOSE

Rowan University ("University") must collect and use data for a number of purposes relating to its faculty, staff, applicants, students, customers, donors, and other individuals who interact with the University. In collecting and using this data, the University is committed to protecting an individual's right to privacy with regard to the processing of personal data, and this policy has been implemented to support this commitment. Rowan University intends to fully comply with all requirements of the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") in so far as it affects the University's activities.

II. ACCOUNTABILITY

Responsibility for compliance is delegated to senior staff and faculty members, and Data Custodians and Stewards within each department who are responsible for encouraging data processing best practices within the University. However, compliance with this policy is the responsibility of everyone within the University who processes personal information.

1. **Controllers**:
   Individual responsible for decisions about the collection, use and protection of personal data. At Rowan University, controllers make management level decisions about the confidentiality, integrity and availability of information for which they are responsible. Controllers include Data Custodians and Data Stewards per Rowan University's Data Governance Policy, as well as any individual responsible for the implementation and management of University systems using data. Controllers may advise Division leaders of the University about the financial and other resources necessary to protect data according to laws and University rules/policies. Controllers collaborate with the Data Protection Officer on issues related to the protection of personal data**.**
2. **Data Protection Officer (DPO)**:
   The DPO is appointed to develop a strategy for protecting personal data and developing policies, training and resources that assist University units in assessing and implementing necessary protections for personal data. The DPO performs a review of data protection or privacy-related impact or risk assessments and leads the response to and management of incidents involving personal data or allegations of privacy violations. If needed, the DPO reports incidents to external regulators. The DPO for Rowan University is: Ray Braeunig, Chief Compliance Officer, Email address: braeunrc@rowan.edu
3. **Processor**:
   Individual responsible for processing, analyzing, storing and deleting personal data on behalf of the

controller. Processors include technical owners, system operators, or research staff, who are responsible for the activities or operations associated with the use of the data or information system. Processors collaborate with the Data Protection Officer on issues related to the protection of personal data.

III. APPLICABILITY

The GDPR Policy is applicable to all activities at Rowan University and its auxiliary organizations that collect or process personal data about individuals residing in the European Union ("EU") or who are located in an EU country when their data is collected and processed.

IV. DEFINITIONS

1. "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. "sensitive personal data" means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership; data concerning health status, sexual orientation, genetic data or biometric data.
3. "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
4. "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
5. "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
6. "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
7. "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
8. Data Custodians – University officials and their staff who have operational-level responsibility for data capture, data maintenance, and data dissemination
9. Data Stewards – University officials who have policy-level responsibility for managing a segment of the University's data resource.

V. REFERENCES

1. GDPR Regulations – https://gdpr-info.eu/art-4-gdpr/
2. Sensitive data and lawful processing – https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/25--guide-to-the-gdpr--sensitive-data-and-lawful-processing.pdf?la=en
3. Records Retention - https://confluence.rowan.edu/display/POLICY/Records+Retention
4. Data Governance Policy - https://confluence.rowan.edu/display/POLICY/Data+Governance+Policy

VI. POLICY

1. **Personal Data Use Record Requirement**
    a. At the University, the personal data use registry assists the University in documenting pertinent information that aids the University in being a responsible steward of personal data. Controllers and processors must make a record of their use of personal data by completing the Rowan Privacy Office personal data use registry.

b. The record includes the following pertinent information, which may also be used to meet additional requirements related to assessing the nature, scope, context and purpose for collecting and using personal data:
    i. Identification of the controller and/or processor
    ii. Purpose for collecting, using, or sharing personal data
    iii. Location of data storage
    iv. Categories of personal data included in the data set
    v. How long the data will be retained
    vi. Whether notification or consent is provided to the individuals
    vii. If personal data are routinely share with other parties internal or external

2. **Notification Requirement**
    a. At Rowan University, privacy notices offer transparency to constituents regarding how any personal information they provide to the University will be used, retained, shared and secured.
    b. Pursuant to the GDPR, notification must be provided at the time personal data is obtained. Thus, notification is required the first time you contact someone whose data you did not directly obtain, or when using data for a purpose that is different than the one originally stated when the data was collected. If notification is required, then as a best practice, the University notification form includes the required elements of notification in understandable language.
    c. The use of personal data requiring notification must be recorded in the personal data use registry.
    d. **Notification is not required if**:
        i. The data subject already has the required notification
        ii. It would be impossible
        iii. The University did not collect the data and is using it for archiving, scientific or historical research, or statistical purposes, as long as that research/statistical/archiving meets certain safeguards, including but not limited to standards relating to technical and organizational security measures, data minimization, and using pseudonymisation where appropriate.
    e. **Elements of notification**
    Notification under GDPR must include all of the following elements:
        i. Name and contact information for the controller(s) (or controller's representative(s)) and Data Protection Officer.
        ii. Purpose of processing including the controller's legitimate interest and one of the following lawful bases for processing:
            1. Necessary for the performance of a contract to which the individual is part of or to take steps at the data subject's request prior to entering into a contract;
            2. Necessary for compliance with a legal obligation;
            3. Necessary to protect the vital interests of the individual or another natural person;
            4. Necessary for the performance of a task carried out in the public interest or as required by an official authority;
            5. Necessary for the purposes of the legitimate interests pursued by the controller or by a third party as long as the purpose does not negate the interests or fundamental rights and freedoms related to the protection of personal data; or
            6. The individual has given consent for the specific purpose.
        iii. Whether Rowan University is required to collect the personal data as part of a statutory or contractual requirement and there are possible consequences if the individual does not provide the personal data.
        iv. The primary, and, if applicable, secondary or supplemental uses of the personal data.
        v. Recipient or types of recipients of the data.
        vi. Whether Rowan University intends to share (transfer) personal data to an organization located in another country or to an international organization.
        vii. Reference to Rowan University retention schedule for length of time data will be retained or an explanation of how that time period will be determined.
        viii. Individuals' rights to:
            1. Access, rectify or request erasure of their data
            2. Restrict processing of their data
            3. Object to processing
            4. Withdraw their consent without detriment

5. Take their data with them (portability)
6. Complain

ix. If you are using automated decision-making: the existence of automated decision-making, and meaningful information about the logic involved and its significance and consequences of such processing for the individual.

3. **Lawful Basis for Processing**
   a. The following is a description of the lawful bases for processing personal data:
      i. Necessary for the performance of a contract to which the individual is part of or to take steps at the data subject's request prior to entering into a contract;
      ii. Necessary for compliance with a legal obligation;
      iii. Necessary to protect the vital interests of the individual or another natural person;
      iv. Necessary for the performance of a task carried out in the public interest or as required by an official authority;
      v. Necessary for the purposes of the legitimate interests pursued by the controller or by a third party as long as the purpose does not negate the interests or fundamental rights and freedoms related to the protection of personal data; or
      vi. The individual has given consent for the specific purpose.
4. **Consent Requirement**
   a. At the University, consent promotes trusted relationships when collecting or using special categories of personal data. Under GDPR, consent is intended to promote transparency, fairness, lawfulness, integrity and accuracy.
   b. The controller is required to obtain valid consent from the individual if consent is the lawful basis being relied upon for processing personal data or if the data meets the definition of special categories of personal data. If consent is required, then as a best practice, the University standard consent form includes the required elements of consent in understandable language.
   c. If consent is being used as the lawful basis to process data, the University must be able to demonstrate, through documentation, that the consent was informed, clear and specific, freely given, as well as unambiguous and actively given. Individuals must be allowed to withdraw their consent at any time.
   d. The use of personal data requiring consent must be recorded in the personal data use registry.
   e. Note that other laws that relate to protection of personal data at the University may still require consent even if GDPR does not require consent.
   f. **Special Categories of Personal Data**
      The controller must obtain consent from an individual prior to special categories of personal data being obtained from the individual unless the purpose is for a defined legitimate use.
      Legitimate Uses of special categories of personal data that do not require consent:
      i. To carry out specific obligations or rights of Rowan University or data subject in employment;
      ii. To protect the vital interests of the individual or another person when the individual is physically or legally incapable of providing consent;
      iii. For legal defense;
      iv. For various healthcare-related reasons, including assessing working capacity of employee, when the individuals involved in processing have duties of confidentiality;
      v. For various specified public health related reasons;
      vi. For archiving, scientific or historical research or statistical purposes; or
      vii. If processing relates to personal data which the individual manifestly makes public.
   g. **Elements of Consent**
      Consent must include all of the following elements in understandable language:
      i. Name and contact information for the controller(s) (or controller's representative(s)) and Data Protection Officer.
      ii. Lawful basis and purpose(s) of processing.
      iii. Recipients or types of recipients of the data and their reliance on this consent.
      iv. Retention schedule for length of time data will be retained or an explanation of how that time period will be determined.
      v. Individuals' rights to:
         1. Access, rectify, or request erasure of their data
         2. Restrict processing of their data

3. Object to processing
4. Withdraw their consent without detriment
5. Take their data with them to another entity
6. Complain

vi. Notice that subsequent withdrawal of consent does not impact the lawfulness of prior data processing.

h. **Valid Consent**

Consent is only valid if it is:

i. Informed by including the required elements of consent (above).
ii. Freely given and not a condition of receiving a product or service unless the information being provided is required for the delivery of the product or service. Additionally, the controller is required to allow the individual to withdrawal consent without detriment.
iii. Specific to the purpose and use and not bundled with other terms and conditions.
iv. Clear and prominently presented information about the purpose and use and whether consent is being sought or given.
v. Active and Unambiguous with an opt-in approach. Passive, default and auto-box tick approaches are invalid.

i. **Invalid Consent**

Conversely, consent may not be valid if:

i. There are doubts over whether the Data Subject has consented.
ii. The Data Subject doesn't realize they have consented.
iii. No clear record demonstrating the Data Subject consented can be produced.
iv. There was no genuine free choice over whether to opt in.
v. The Data Subject would be penalized for refusing consent.
vi. There is a clear imbalance of power between the Controller and the Data Subject.
vii. It was a precondition of a service, but the processing is not necessary for that service.
viii. It was bundled with other terms and conditions in an unclear way.
ix. The consent request was vague or unclear.
x. Auto-ticked opt-in boxes or other methods of default consent were used.
xi. The Controller was not specifically identified.
xii. Data Subjects were not informed of their right to withdraw consent.
xiii. Data Subjects cannot easily withdraw consent.
xiv. The purposes or uses have evolved.

5. **Incident Management Requirement**
   a. At the University, there are various laws that relate to the protection of personal data and set forth requirements about how the University must respond to personal data breaches. Under the GDPR, organizations are required to report certain types of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.
   b. Controllers and processors must promptly notify the DPO if a potential or actual personal data breach has occurred. The DPO will work closely with other University personnel to investigate and manage internal reporting procedures. Additionally, the DPO will determine if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, and if the University must:
      i. Inform relevant supervisory authority or external regulator; or
      ii. Inform the individuals whose personal data was involved in the personal data breach.
6. **Retention of Personal Data Requirement**
   a. Under the GDPR, the controller must specify the period that the personal data will be retained or how the retention period will be determined. Such determinations must be included in notification, consent, agreements and documents that describe the purpose and use of personal data about individuals that reside in the EU. Carefully review the relevant records retention schedule(s) or consult with the appropriate Records Management Services department to determine what period of retention to specify when collecting personal data.
7. **Policy Maintenance**
   a. This standard will be updated periodically as the GDPR is interpreted and applied and additional official information about the regulations becomes available. The University Privacy Official shall

review and approve this standard at least every three years or more frequently as needed to respond to changes in the regulatory environment. For more information see the update history at the end of the standard.