MIDDLE GEORGIA STATE UNIVERSITY
OFFICE OF THE CHIEF PRIVACY OFFICER

Effective Date: 5/28/2020

Title: Privacy Standard

1. Overview

Privacy is a component of security and is related to the proper handling of Personally Identifiable Information. Personally Identifiable Information (PII) is 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. Some PII is not sensitive, such as the PII on a business card, while other PII is considered Sensitive Personally Identifiable Information (Sensitive PII), as defined below.

Sensitive Personally Identifiable Information (Sensitive PII) is personally identifiable information that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such as a Social Security number or alien number (A-number). Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if compromised.

HIPAA uses the term Protected Health Information (PHI) to refer to protected information, but the concept is very similar to PII.

GDPR refers to PII as personal data.

2. Purpose

The purpose of this policy is to protect the privacy of individuals who have sensitive PII stored (either in electronic or paper form) on assets owned by Middle Georgia State University, while at the same time providing the University the ability to share this information with authorized entities as required by legitimate academic or business need or by law.

3. Scope

The MGA Privacy Standard applies to all faculty, staff, students, affiliates, and third-party service providers. This policy is not intended to replace or supersede other existing University policies and procedures relating to the use of maintenance of sensitive information such as those related to FERPA compliance, GLBA compliance, or human subjects research.

4. Standard

MGA shall enact and maintain permanent privacy processes and procedures in adherence with this standard, which includes, but is not limited to, the following principles:

1. Personally identifiable information may only be obtained through lawful means.
2. The purposes for which personally identifiable data are collected must be specified at or prior to the time of collection, and any subsequent use of the data shall be limited to and consistent with the fulfillment of those purposes previously specified.
3. Personal data may not be disclosed, made available, or otherwise used for a purpose other than those specified, except with the consent of the subject of the data, or as required by law or regulation.
4. Personal data collected must be relevant to the purpose for which it is needed.
5. The general means by which personal data is protected against loss, unauthorized access, use, modification or disclosure must be posted, unless the disclosure of those general means would compromise legitimate USG entity objectives or law enforcement purposes.

MGA will implement this privacy standard by:

1. Designating a Chief Privacy Officer responsible for the implementation of and adherence to this privacy standard. This person will be responsible for compliance and awareness of these policies with a focus on functional units involved with collecting, classifying, handling and releasing sensitive and confidential information. This individual will also perform the role of GDPR Data Protection Officer.
2. Prominently posting the standard physically in its offices and on its website.
3. Distributing the standard to each of its employees and contractors who have access to personal data.
4. Complying with the State and Federal laws pertaining to information privacy and treating covered information as Sensitive PII.
    a. Georgia Personal Identity Protection Act of 2007 (O.C.G.A. 10-1-910 through 10-1-912), or GPIPA. - Personal information protected by GPIPA includes the combination of an individual's full name, or first initial and last name with one of the following, when not encrypted or redacted:
        - Social Security Number
        - Driver's license number or state ID card number
        - Account, credit card, or debit card number
        - Account passwords, personal identification numbers, or other access codes
    b. Family Educational Rights and Privacy Act of 1974 (FERPA) - Protects the rights of students by controlling the creation of, maintenance of, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.
    c. Health Insurance Portability and Accountability Act of 1996 (HIPAA) - Protected Health Information - individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. Laws require special precautions to protect from unauthorized use, access, or disclosure.
    d. The European Union General Data Protection Regulation ("EU GDPR") imposes obligations on entities, like Middle Georgia State University, that collect or process personal data about people in the EU. The EU GDPR applies to personal data collected or processed about anyone located in the EU, regardless of whether they are a citizen or permanent resident of an EU country.
    e. Identity Theft Protection – Red Flag Rule – identify, detect and respond to Red Flags by following procedures defined in USG IT Handbook section 5.14 Identity Theft Prevention - Red Flags Rule.
5. Using appropriate means to successfully implement and adhere to this privacy standard.
    a. Maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the sensitive PII.
    b. Ensure each University department/unit is implementing, reviewing and monitoring internal procedures, practices, etc. to assure compliance with this policy.

Limits on Use of and Access to Sensitive Information

The responsible use of sensitive information requires that the University respect individual privacy, protect against unauthorized access to or use of information, and comply fully with all laws and government regulations in the collection, use, storage, display, distribution and disposal of such information. Authorized uses of sensitive information within the University are limited to uses which a) are necessary to meet legal and regulatory requirements; b) facilitate access to services, transactions, facilities and information; or c) support efficient academic and administrative processes.

Access to sensitive information is limited to:

- the individual whose information is produced or displayed;
- a University official or agent of the University with authorized access based upon a legitimate academic or business interest and a need to know;
- an organization or person authorized by the individual to receive the information;
- a legally authorized government entity or representative;
- other circumstances in which the University is legally compelled to provide access to information, such as the Georgia Open Records Act;
- or other individuals or entities, as allowed by law, for purposes judged to be appropriate or necessary for the reasonable conduct of University business.

FERPA Directory Information

FERPA defines "directory information" as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Under FERPA schools may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information. In addition, FERPA gives students the right to opt-out of directory information disclosure. The type of information MGA has designated as "directory information," as well as the procedure to opt-out of directory information disclosure is defined in the FERPA FAQ on the WWW.MGA.EDU web site.

Social Security Numbers

Social Security numbers are always considered confidential and are therefore subject to the limits of use and access described above. In addition, the University will continue to collect and process Social Security Numbers limited only to instances in which that number is required by law or contract or instances where there is a legitimate business or academic need authorized by University administration. This includes, but is not limited to, all enrolled students who are U.S. citizens or permanent residents.

MGA, its faculty, staff, and students must abide by all state legal regulations pertaining to Social Security Number protection.

It is against both state law and University policy to:

- Publicly post or display the Social Security number in any manner;
- Require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted; or
- Require an individual to use his or her Social Security number to access an Internet site unless a unique password or PIN is also required.
- Print the Social Security number on any card required to access services; or
- Establish a new process that requires the printing of a Social Security number on any materials that are mailed unless required by other state or federal agency.

Online Collection of Information

University departments must post a link to the MGA Privacy Policy on any website which collects data about website visitors.

Information Collected

Middle Georgia State University is an institute of higher education involved in education, research, and community development. In order for Middle Georgia State University to educate its students both in class and on-line, engage in world-class research, and provide community services, it is essential, necessary, and Middle Georgia State University has lawful bases to collect, process, use, and maintain data of its students, employees, applicants, research subjects, and others involved in its educational, research, and community programs. The lawful bases include, without limitation, admission, registration, delivery of classroom, on-line, and study abroad education, grades, communications, employment, applied research, development, program analysis for improvements, and records retention. Examples of data that Middle Georgia State University may need to collect in connection with the lawful bases are: name, email address, IP address, physical address or other location identifier, photos, as well as some sensitive personal data obtained with prior consent.

Most of Middle Georgia State University's collection and processing of personal data will fall under the following categories:

- Processing is necessary for the purposes of the legitimate interests pursued by Middle Georgia State University or third parties in providing education, employment, research and development, community programs.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This lawful basis pertains primarily but not exclusively to research contracts.
- Processing is necessary for compliance with a legal obligation to which Middle Georgia State University is subject.

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes. This lawful basis pertains primarily but not exclusively to the protection of research subjects, providing medical and mental health services.

There will be some instances where the collection and processing of personal data will be pursuant to other lawful bases.

Types of Personal Data collected and Why

Middle Georgia State University collects a variety of personal and sensitive data to meet one of its lawful bases, as referenced above. Most often the data is used for academic admissions, enrollment, educational programs, job hiring, provisioning of medical services, participation in research, development and community outreach. Data typically includes name, address, transcripts, work history, information for payroll, research subject information, medical and health information (for student health services, or travel), and donations. If you have specific questions regarding the collection and use of your personal data, please contact the Chief Privacy Officer at privacy@mga.edu

If a data subject refuses to provide personal data that is required by Middle Georgia State University in connection with one of Middle Georgia State University's lawful bases to collect such personal data, such refusal may make it impossible for Middle Georgia State University to provide education, employment, research or other requested services.

Where Middle Georgia State University gets Personal Data and Special Categories of Sensitive Personal Data

Middle Georgia State University receives personal data and special categories of sensitive personal data from multiple sources. Most often, Middle Georgia State University gets this data directly from the data subject or under the direction of the data subject who has provided it to a third party (for example, application for admission to Middle Georgia State University through use of our online admissions application web app).

Individual Rights of the Data Subject under the EU GDPR

Individual data subjects whose information is collected under MGA's European Union General Data Protection Regulation Compliance Standard will be provided the following information at the time the information is collected from them:

a) information about the controller collecting the personal data;
b) contact details for the data protection officer (if assigned);
c) the purposes and lawful basis of the data collection/processing, including the legitimate interest for the processing (if applicable);
d) who the recipients or categories of recipients of the personal data are;
e) whether MGA intends to transfer personal data to another country or international organization;
f) the period for which the personal data will be stored;
g) the existence of the right to access, make corrections to, or erase personal data, the right to restrict or object to processing, and the right to data portability;
h) the existence of the right to withdraw consent at any time (if applicable);
i) the right to lodge a complaint with a supervisory authority (established in the EU);
j) justification for why the personal data are required, and possible consequences of the failure to provide the personal data;
k) the existence of automated decision-making, including profiling; and
l) if the collected personal data are going to be further processed for a purpose other than that for which it was collected.

Individual data subjects whose information is collected under MGA's European Union General Data Protection Regulation Compliance Standard will be provided the following rights (as applicable), provided that MGA determines that the exercise of the right is permitted and/or required by the EU GDPR:

a) the right to receive confirmation from MGA as to whether the data subject's personal data is being processed by MGA, and if so, the right to access such personal data and the right to receive information regarding, among other things, the categories of personal data collected and how such personal data is being used;
b) the right to correct inaccurate personal data concerning the data subject;
c) the right to obtain erasure of personal data concerning the data subject;

d) the right to restrict or object to the processing of the data subject's personal data; and
e) the right to request a copy of personal data concerning the data subject.

Any data subject who wishes to exercise any of the above-mentioned rights may do so by filling such request with the Chief Privacy Officer at privacy@mga.edu.

Cookies
Cookies are files that many websites transfer to users' web browsers to enable the site to deliver personalized services or to provide persistent authentication. The information contained in a cookie typically includes information collected automatically by the web server and/or information provided voluntarily by the user. Our website uses persistent cookies in conjunction with a third-party technology partner to analyze search engine usage and web traffic patterns. This information is used in the aggregate to monitor and enhance our web pages. It is not used to track the usage patterns of individual users.

Security of Personal Data subject to the EU GDPR
All personal data and sensitive data collected or processed by MGA under the scope of the European Union General Data Protection Regulation Compliance Standard must comply with the security controls and systems and process requirements and standards set forth in MGA's Data Classification and Management Standard.

We will not share your information with third parties except:

- as necessary to meet one of its lawful purposes, including but not limited to,
  - its legitimate interest,
  - contract compliance,
  - pursuant to consent provided by you,
  - as required by law;
- as necessary to protect MGA's interests;
- with service providers acting on our behalf who have agreed to protect the confidentiality of the data.

Data Retention
MGA keeps the data it collects for the time periods specified in the University System of Georgia Records Retention Schedules.

5. Enforcement
Violation of this policy may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

6. References

Other Policies, Standards and Procedures
This standard incorporates by reference the following policies, standards and procedures:

URL: https://policies.mga.edu/
- Middle Georgia State University Policy, "Privacy Policy"
- Middle Georgia State University Policy, "Appropriate Use Policy"
- Middle Georgia State University "FERPA"
- Middle Georgia State University "Cybersecurity Policy"
- Middle Georgia State University "Cybersecurity Standard"

URL: https://www.usg.edu/information_technology_services/it_handbook/
- University System of Georgia IT Handbook Section 5.14 Identity Theft Prevention - Red Flags Rule

URL: https://www.usg.edu/business_procedures_manual/
- USG Business Procedures Manual Section 12

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

- USG Records Retention Schedules

URL: https://www.mga.edu/health-clinic/docs/HIPAA_Notice_of_Privacy_Practices.pdf

- (HIPAA) Notice of Privacy Practices

7. Definitions

"Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."
A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

8. Revision History

04/21/2020 - Original