General Data Protection Regulation of the European Union

Background

The European Union (EU) Parliament enacted the General Data Protection Regulation (GDPR) as its primary regulation designed to protect personal data that businesses and organizations compile, process, and, maintain on individuals. The GDPR became effective on May 25, 2018.

The GDPR is premised on the principle that the privacy of personal data is a fundamental human right in a world where there are ever-increasing amounts of personal data stored by businesses and organizations, including higher education.

GDPR is enforceable for any business or organization of any size that controls or processes the personal data of individuals in the EU, regardless of where the controller or processor is physically located or where the actual data processing occurs. Entities which are found to be in violation of the GDPR are subject to the imposition of significant monetary penalties.

Any U.S. university or college that recruits and admits students who are physically located in the EU is subject to the stipulations of the GDPR. If university or college officials located outside the EU interact with prospective students, current students, faculty, or staff who are located inside the EU, then GDPR applies. However, GDPR does not apply to prospective or current students (currently enrolled in a U.S. institution) who are EU citizens if the personal data on them is gathered while they are outside the EU.

All University activities that collect personal data from natural persons in the EU shall obtain written consent from the person concerning the collection of the information using University approved forms.

Application of the GDPR

The GDPR applies whenever personal data is being collected on or from *a person who is physically present* in an EU member country. This includes recruitment and admissions activities conducted by universities and colleges located or based in the United States which are directed toward people who are in the EU.

Since the GDPR applies to any natural person located in the EU, it also extends its protections to U.S. students, faculty, and staff when they are in the EU.

This law does not apply to students, faculty, and staff including individuals from the EU, while they are physically located in the U.S., provided that their personal data not obtained while they were physically present in an EU country.

must make explicit the rights of individuals on whom data is processed, maintained and stored and this must include protocols for such individuals to have access to their data, to provide consent to disclose/share their personal data, to rescind such consent, and to challenge the content or substance of their personal data

Some Important Definitions in GDPR

'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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'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;

'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 affirmation, signifies agreement to the processing of personal data relating to him or her;

'personal data breach' means a breach or security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'data subject' means a natural person (not a corporate or other organizational entity);

'European Union (EU)' means those countries that have ratified membership in the Union. See: https://europa.eu/european-union/about-eu/countries_en

'supervisory authority' means an independent public authority which is established by an EU state pursuant to GDPR.

SVSU Obligations Regarding the GDPR

All University activities that collect personal data from natural persons in the EU shall obtain written consent from the person concerning the collection of the information, using University approved forms. The consent secured must both reveal the reason the personal data is being collected and how the data will be used.

Any personal data collected from a natural person in the EU shall be stored, secured, and accessed consistent with the SVSU ITS data security policies.

Any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed shall be reported to the Supervisory Authority of the EU member state within 72 hours of notice of the breach.

The individual rights of persons in the EU regarding their personal data includes the rights of access, ratification, removal, restriction, portability, to object, and not to be subject to automated individual decision making, and those rights shall be respected consistent with the procedures implementing this policy.

Concerning academic data, including course work attempted and/or completed as well as grades associated with those courses, the University must preserve that data for legal and accrediting requirements.

Implementation

All University operations that collect data should perform an analysis to determine whether and to what extent the office collects personal data that could originate from natural persons in EU member states.

All University third party contracts within those offices should be reviewed for compliance with the GDPR.

All personnel who deal with GDPR covered data shall receive appropriate training.

Communication

All academic and administrative offices will be made aware of this policy though appropriate University mechanisms.

Full text of the law

The EU GDPR and U.S. FERPA: The GDPR does not rescind, annul, or revoke in any way the U.S. FERPA law that applies to institutions of higher education in the United States with respect to individuals not covered by the EU GDPR. However, the GDPR applies to any person (student, staff, or faculty) who is physically present in the EU and on whom the University is collecting personal data irrespective of the reason for the person's presence in the EU.

Link to Information Technology Services Data Security Policy _____

Responsible Office and Enforcement Official: Provost/Vice President for Academic Affairs

Last Updated – 5/29/18

Questions and inquiries related to GDPR can be directed to the Office of the Registrar or the Office of the General Counsel.

Institutional Working Group: SVSU has established a subcommittee on the GDPR reports to the SVSU Committee on Data Governance chaired by the Director of the Office of Institutional Research whose mission is to "enhance our understanding of what the GDPR requires of American universities, to determine how the law will affect SVSU, and to identify what policy and protocol changes we need to implement to ensure compliance. The Subcommittee's recommendations will be conveyed to the SVSU Committee on Data Governance."

The following university officials are represented on the subcommittee:

- Registrar/FERPA Officer
- General Counsel
- Executive Director of Information Technology Services
- Manager of Information Systems Security
- Director of the Academic Advisement Center
- Associate Director of the Office of Scholarships and Financial Aid
- Accountant, Campus Financial Services Center
- Director of International Programs
- Director of Study Abroad Programs
- Athletic Compliance Officer
- Head of Library Access Services