DataKeep™

INDUSTRY BULLETIN

(GDPR) General Data Protection Regulation and the Potential Impact upon U.S. Higher Education Institutions

The European Union (EU) General Data Protection Regulation (GDPR) applies to anyone inside or outside the European Union who regularly processes personal data of Europeans. One of the key changes that GDPR brings when compared to previous regulations is the ability to levy very steep fines, up to either 20 million euros or 4 percent of annual global turnover (revenue), whichever is higher.

The GDPR is centered around the concept that privacy is considered a fundamental human right, and most of the core Articles in the regulation support individual rights. At a high-level these are some of the rights that educational institutions processes need to support:

- The Right to know what data is being collected, how it will be used, and how long it is needed
- The Right to see the data in a readable format and have any errors corrected
- The Right to have access to the data in a format that can be portable, even to other institutions
- The Right to be forgotten and have all identified data deleted
- The Right to be notified of a data breach based upon severity and determination of a data controller

While the GDPR doesn't specifically define how to protect personal data and support privacy rights, it does define tasks that need to be part of the processing of said data:

- Minimize the personal data that is collected and processed, and retain it only for the time required
- Implement pseudonymization and encryption of personal data
- Only allow access to personal data based upon job requirements and data subject consent
- Implement data security by design and default, so protects personal data as process

Criteria Considerations for U.S. Based Colleges and Universities

- Advertise, invite and register students from EU countries
- Have employees (professors, administrators…) from EU countries
- Offer and support student-abroad programs in EU countries
- Have programs that retain information, solicit and collect donations from alumni in EU countries
- Other funding, grants etc. that come from persons or institutions in EU countries

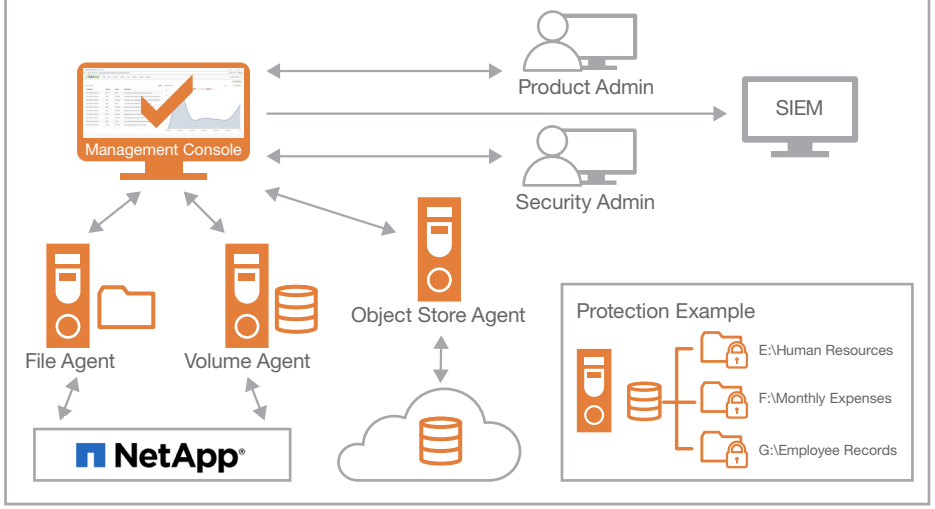
Steps to Compliance

- Identify any EU personal data
- Pseudonymize and encrypt that data
- Control who has access to EU personal data
- Allow data subjects to request personal data
- Establish ability to delete personal data upon request
- Appoint a Data Protection Officer as applicable
- Establish an EU supervisory authority

DataKeep Capabilities to Support GDPR Data Protection Requirements

- Encrypt personal data
- Manage access to personal data (by role or process)
- Audit data access requests / denials for encrypted personal data
- Provide data erasure through cryptographic shredding
- RESTful API to support Security by Design and Security by Default requirements

Fig. 1 - DataKeep Deployment Model



DataKeep™ from SecurityFirst can help your institution start protecting this data today, while you continue to develop long-term processes to be implemented from data creation to deletion. DataKeep seamlessly integrates into your existing environment and works with your existing storage vendors.

SecurityFirst™ delivers advanced security solutions that build a firewall around your data to protect against ever increasing threats and to aid in meeting regulatory requirements such as GDPR, HIPAA, NYCRR and many others.

DataKeep™, our flagship product, serves as your data firewall by using advanced encryption, scalable hierarchical key management, extensive policy enforcement and monitoring of unauthorized access to deliver the highest levels of availability, resiliency and time to value. Security requires a layered approach and protection of the data itself is your last line of defense.

SecurityFirst™
Protecting Critical Data

For a product demonstration or more information contact:
sales@securityfirstcorp.com
888-884-7152
securityfirstcorp.com