The MPI Group
People. Purpose. Profits.

Higher Education and the GDPR

New Standards, New Risks — and New Opportunities

Brought to you by Canon U.S.A., Inc.

Canon

www.cusa.canon.com

The enactment of the General Data Protection Regulation (GDPR) in the European Union is challenging higher education institutions and their management of personal information as never before. Yet amid general concern and uncertainty in the sector about GDPR compliance, some institutions see opportunity.

Why?

Because leaders at these organizations understand that streamlined information workflows can not only help with security and GDPR compliance efforts, but also deliver a competitive edge. With best practices and technology-enhanced information workflows in place, institutions can become more responsive, agile, and efficient — and create models for personal information management that can serve them for years to come.

New Standards and New Risks

Higher education institutions hold vast amounts of private information, where much of it can be under the purview of the GDPR, such as:

- EU student records
- EU student applications for admission
- EU alumni records
- EU staff records
- Research and institutional data containing EU personal data
- Communications with and marketing to EU individuals (website, email, Facebook, etc.).

In response to individuals' demands for greater control over their information, including understanding who holds and uses it, other privacy regulations are also emerging around the globe, sometimes modeling on the GDPR. The array of penalties that governments can impose on institutions to protect personal information has increased in some jurisdictions as well.

After decades in the making and a two-year period for organizations to prepare, on May 25, 2018 the European Union began enforcement of the GDPR. Some consumers and privacy rights activists argue that laws such as GDPR are long overdue, with regulators lagging behind technological advances. This means that while GDPR compliance may seem daunting now, tomorrow it could likely be viewed as just another cost of doing business in the EU — or anywhere.

GDPR covers the "protection of natural persons with regard to the processing of personal data and on the free movement of such data,"[1] and can dramatically increase data security responsibilities and risks for businesses of all types *(see GDPR Basics)*. Even more significant is GDPR's establishment of new standards for data privacy rights that other lawmakers may replicate. For example, in June 2018, California passed a digital privacy law, effective January 1, 2020, that gives consumers more control over personal information that covered businesses collect from them.[2] And as inappropriate uses of personal data by holders and hackers continue to make news, increasingly stringent regulations may arise.

The California Consumer Privacy Act reflects the intent of lawmakers around the world to regulate data-collection and -sharing practices, and illustrates how important it is for U.S. organizations to comply with emerging global standards (i.e., GDPR) — and that includes higher education institutions.

Unfortunately, although most U.S. institutions must hold and process personal information to meet federal, state, and other reporting requirements, some lag in adoption of effective data security practices as prescribed by GDPR. The number of records involved in education breaches increased to approximately 33.5 million in 2017, up from 4.5 million in 2016, and the number of breach incidents also has risen *(Figure 1)*.[3]

- *Purdue University* — A data breach of 26,598 applicants was due to an employee from Purdue's Division of Financial Aid inadvertently sending a prospective parent a list of applicant names, birthdays, and Social Security numbers.[4]
- *Oklahoma University* — Nearly 29,000 education records were exposed due to lax privacy settings in a campus file-sharing network; information included Social Security numbers, financial aid information, and grades dating to at least 2002.[5]
- *University of Buffalo* — A data breach of external third-party accounts affected more than 2,500 records, of which about 1,800 were student accounts. Logins were stolen from those who may have visited a website not associated with the university and then entered their login information.[6]

Figure 1. Breach Incidents in Education[7]

Year	Breach Incidents
2017	199
2016	166
2015	166
2014	174
2013	36

[1] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

[2] California Consumer Privacy Act, caprivacy.org.

[3] *2017: The Year of Internal Threats and Accidental Data Breaches,* Breach Level Index

[4] Purdue responds to data breach of 26,598 applicants, *wlfi.com,* July 13, 2018.

[5] Dana Branham, "OU shuts down file sharing service after failing to protect thousands of students' records," *The Oklahoma Daily,* June 13, 2017.

[6] Marissa Pearlman, "Thousands of UB logins stolen in third-party data breach," *WIVB.com,* May 21, 2018.

[7] *2017: The Year of Internal Threats and Accidental Data Breaches,* Breach Level Index

GDPR Basics[8]

The GDPR replaced Data Protection Directive 95/46/EC, and is intended to harmonize data privacy laws across EU member states. It assigns control of personal data to individuals in the EU and incorporates an array of new rights for EU data subjects, including the right to:

Access information about personal data: An EU data subject has the right to obtain from data controllers confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to such personal data. Such EU data subjects can also have the right to obtain information on, among other things, the purpose of the processing, the categories of personal data, the recipients or categories of recipient to whom personal data has been disclosed, etc.

Be forgotten: An EU data subject has the right to obtain from controllers the erasure of personal data concerning him or her, without undue delay, and controllers are obligated to erase personal data without undue delay, if certain circumstances apply.

Automated individual decision-making, including profiling: An EU data subject has the right to not be subject to a decision based solely on automated processing, including profiling. The law regulates, among other things, the profiling of a person for the purpose of analyzing or predicting the individual's personal preferences, behaviors, and attitudes.

Consent: Unless expressly allowed by law, an EU data subject's personal data cannot be processed without his or her consent. Consent must be freely given, specific, informed, via an unambiguous indication of the EU data subject's agreement to the processing of personal data (e.g., by a written statement, ticking a box when visiting an internet website). Pre-ticked boxes or inactivity do not constitute consent.

Data portability: An EU data subject has the right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, machine-readable format, and has the right to transmit the data to another controller, if certain circumstances apply.

[8] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Time limits: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

GDPR is likely to alter the ways organizations collect and manage personal information. It defines and may require "data controller" and "data processor" roles for organizations dealing with EU data subjects, and identifies required processes that may apply to both (appointment of a "data protection officer," response to a breach, etc.):

Controller is the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of the processing of personal data. The controller implements appropriate technical and organizational measures to ensure and demonstrate that data processing is performed in accordance with GDPR, including application of data-protection policies.

Processor is the natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. Processors need to meet the standards set forth by controllers. Where processing is done for a controller, the controller needs to ensure that the processor has sufficient guarantees to implement appropriate technical and organizational measures to comply with GDPR and can ensure the protection of the rights of EU data subjects.

Data protection officer: Controller and processor shall designate a data protection officer in any case where processing is carried out by a public authority or body, except for courts acting in their judicial capacity; the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 of the GDPR and personal data relating to criminal convictions and offenses referred to in Article 10 of the GDPR.

Lastly, and of importance to U.S. higher education institutions, GDPR extends to foreign organizations processing the data of individuals in the EU. For example, if a student is located in the EU, all EU personal data handled by the U.S. institution can be subject to the GDPR. Non-EU established businesses are subject to the GDPR where they process personal data of data subjects in the EU in connection with behavior of individuals in the EU.

With or without the requirements being imposed by GDPR, one thing is certain: breaches can be more costly in the future, given that penalties for violating GDPR data security regulations are severe. Fines for GDPR non-compliance, for example, can reach up to €20 million or 4 percent of an organization's annual worldwide revenue of the preceding financial year, whichever is greater.[9]

While compliance *risks* grab much of the attention around GDPR and other regulatory changes, *opportunities* for institutions abound as well. Many of the new processes and new technologies that may help institutions with data security and GDPR compliance efforts can also help to improve document workflows in ways that boost efficiency and reduce costs.

While compliance *risks* grab much of the attention around GDPR and other regulatory changes, *opportunities* for institutions abound as well.

[9] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Catching Up to GDPR

The GDPR is a complex set of regulations; it's no wonder that even two years after the EU approved them in April 2016, compliance challenges remain for many organizations, including:

- Addressing accountability requirements — both compliance and proof of compliance are required
- Documenting data-management protocols and processes (i.e., information workflows)
- Reviewing data-collection procedures to ensure consent
- Proving the necessity of processing personal data, if and when collected
- Securing vulnerable systems against a range of cyberthreats (malware, ransomware, etc.)
- Establishing procedures to quickly report breaches.

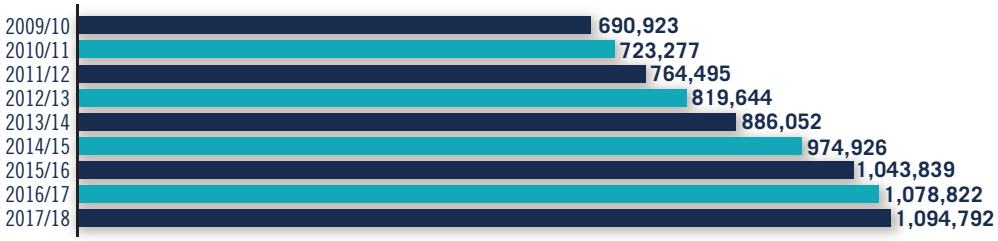
Even worse, many U.S. institutions may be unaware of the full extent of the GDPR and its impact. For example, Barmak Nassirian, director of federal relations and policy analysis at the American Association of State Colleges and Universities, expressed surprise in early 2018 regarding the sector's lack of GDPR awareness: "Candidly, the conversations I've had have been shocking in that people didn't even know that this [GDPR] existed, let alone taken steps to comply."[10]

Exposure to GDPR does not require *physically* conducting business in the EU or selling goods or services into the EU; mere *holding* of data on EU data subjects is also covered under GDPR. U.S. institutions that process information of EU data subjects must establish policies and infrastructures that meet the GDPR threshold for information that they may hold, such as:

- EU student applications
- EU individual job applications
- Study abroad communications with U.S. students and EU hosts
- Alumni association communications with EU graduates
- Collaborative research programs with EU organizations
- Organizations and processes that support the institution.

Higher education institutions are increasingly likely to process EU personal data *(Figure 2)*, and therefore subject to GDPR. The top EU countries with students in U.S. higher education in 2017/18 were the UK (11,460), Germany (10,042), France (8,802), and Spain (7,489).[11]

Figure 2. International Students in U.S. Higher Education[12]



[10] Lindsay McKenzie, "European Rules (and Big Fines) for American Colleges," *Inside Higher Ed,* March 13, 2018.
[11] Institute of International Education.
[12] Ibid.

Minimize GDPR Risks

Institutions capturing and holding personal data of EU data subjects should know what data is collected; why data is being collected; where data is held and processed; and who has access. Legacy systems and myriad applications in use across an institution — and its business partners and affiliates — may make it difficult to find these answers. To do so, institutions typically need to develop campus-wide, data-centric strategies for which all functions and technology platforms contribute to the solution (i.e., no rogue plans) with role-specific objectives and activities:

- *Institution:* It is important for institutions to have an overall information strategy based on a review of types of information needed to fulfill its mission, where personal data is held (systems), and its ability to manage this information in ways that are compliant with GDPR. An institution-wide strategy can establish GDPR awareness, requirements, and enforcement methods for business and academic units and roles.
- *Information technology (IT) departments:* It is important for IT departments to develop technical strategies that align with those of their institutions, which may include integrating new systems and networks with legacy technologies to accommodate personal data requirements and requests; improving information security; and deploying breach-awareness capabilities. IT also plays a key role in data governance and systems strategies.
- *Procurement:* It is important for institutions to develop or refine guidelines and support contracts to minimize GDPR-compliance risks associated with vendors for both goods (systems, applications, office devices) and services (data processors, hosting firms). Use of purchasing associations and contracts pre-vetted for specific concerns can streamline compliance reviews.

The institution and all parties involved with it can take steps to minimize risks of GDPR non-compliance and help streamline personal information workflows by, among other things:

Understanding why data is collected, and where it's kept

It is important for institutions to document *why* they collect any piece of personal information from EU data subjects, *what* they do with it, and to *whom* it is disclosed — even if the organization did not collect the information in the first place (i.e., it was provided by other organizations). Many U.S. institutions may have legacy information-management practices that may struggle to achieve common needs, let alone GDPR requirements: limited or missing authorizations for information; non-standardized information collection and handling processes; mixed file formats that make data searches inefficient or impossible, etc.

Institutions capturing and holding personal data of EU data subjects should know what data is collected; why data is being collected; where data is held and processed; and who has access.

Even worse, some colleges and universities may have complex, siloed information workstreams with cumbersome processes and incomplete documentation. Mapping information workstreams can be a good first step for institutions to track the collection and processing of personal information, as well as adherence to GDPR compliance requirements.

While there is no specific GDPR requirement for data mapping itself, data mapping can be regarded as a key component of compliance efforts.[13] Why? Because mapping can help to identify *where* personal information is kept (e.g., systems, contact lists, email addresses) and to optimize *how* this information is managed in ways consistent with GDPR efforts. For example, do the location and access provisions for a specific type of data make it easy to find and revise or delete records upon request? Can the institution identify and remove unnecessary personal information — across all functions and departments?

Just as important, data mapping can identify delays and waste in document management processes — which can lead to enhancing collaboration and productivity, and more time to focus on learning outcomes.

Accommodating customized data requirements

The GDPR's right of information and access to personal data grants EU data subjects the right to information about data collected about them, and gives data subjects information necessary to ensure fair and transparent processing.[14] To do this, institutions may consider the implementation of personal-data workflows that can improve compliance with GDPR requirements; automating these new processes can help administrators in meeting EU data subject requests.

Developing consistent, institution-wide, information-governance strategies

All actions involving personal data — collecting, hosting, managing contacts, removing data, working with support vendors, etc. — can be aligned with institution-wide GDPR strategies, policies, and technologies, from main campuses out to regional branches. For example, even if the institution may be viewed solely as a data controller for a given data set (i.e., it collected and defined how the data is to be used and processed), it should ensure that its data processor(s) are GDPR compliant too.

Some institutions began taking steps to become GDPR-compliant long before May 2018. For example:

- *Stanford University:* — In August 2017, Stanford's University Privacy Office convened a multi-disciplinary task force to review and assess GDPR and its impact on the university. The GDPR Task Force and seven working groups engaged in data mapping; conducted a gap assessment; prioritized compliance efforts; developed new privacy notices and policies; amended consent language in admissions, financial aid, human resources, and research; updated contractual language; and developed a training video for the university. The university is approaching GDPR as an ongoing effort that requires continuous review.[15]

[13] Alison Cregeen, "A practical guide to data mapping for GDPR compliance," PWC, March 6, 2018.

[14] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

[15] Kate Chesley, "Stanford readies for new EU privacy regulations," *Stanford News,* May 23, 2018.

- *The Ohio State University:* A working group at Ohio State — including representatives from University Compliance and Integrity, Office of Academic Affairs, Enterprise Security, the Wexner Medical Center, the Office of Research, and the Office of Legal Affairs — created a plan to meet GDPR requirements; established governance around GDPR data management; and began implementation of a GDPR program using pilot offices with the highest exposures to EU residents. The group also developed a GDPR FAQ for the university's website to improve awareness of GDPR and the university's compliance efforts: "Ohio State is implementing a GDPR compliance program. We are piloting our compliance efforts with offices that are most likely to work with, collect, and store information about EU residents."[16]

[16] The Ohio State University.

Leverage Opportunities in GDPR Compliance

Some improvement-minded institutions are changing their data processes, workflows, and document-management systems to help improve data security — but with other gains in mind, too. Indeed, for some, GDPR compliance can be a vehicle to leverage data workflow improvements that can enhance day-to-day operations and bring greater value to students, staff, administrators, and other stakeholders. This can be done by implementing best practices, new work models, and new technologies that impact:

- *Data workflows:* Lean organizations — those seeking to continuously remove waste and costs and add value for customers and clients — have used process mapping for decades to identify bottlenecks and wastes that drain profits even as they frustrate customers, partners, and staff. Mapping can not only define new document workflows that can help with some GDPR requirements but can also help to streamline document workflows. For example, moving from paper or mixed-media information formats to all-digital data workflows can improve the overall efficiency of office operations.

  Mapping can also identify gaps in security and information controls, which can help lead businesses to remediate potential security liabilities and establish a log of activities through which personal information travels, from handling to authorized access.

- *Data security:* Institutions can implement new personal data workflows with security controls by establishing automated tracking mechanisms to document the collection and management of information. Data protection technologies can be integrated into processes to help minimize the risk of security breaches, such as incorporating protected and/or sensitive content into a regulated workflow as soon as data is received; limiting unauthorized access to office devices; and ensuring that digital communications leverage classification tools to accurately catalog, store, and protect information.

GDPR compliance can be a vehicle to leverage data workflow improvements that can enhance day-to-day operations and bring greater value to students, staff, administrators, and other stakeholders.

- *Data-breach response:* GDPR may drive many institutions to limit data access (including printers, copiers, scanners, smart phones, and other touchpoints) in order to limit breaches. And because GDPR requires that a breach be reported to the supervisory authority without undue delay but not later than 72 hours of discovery — along with identifying, among other things, both the cause and likely consequences[17] — automated GDPR-alert capabilities and proactive procedures can help. New technologies that alert administrators automatically of breaches help to compile an investigative trail, by capturing log-in information, data, and images from office devices, etc. These plans and technologies may also help institutions in contacting other authorities, business partners, and individuals regarding security breaches that may not involve GDPR and EU data subjects.

- *Deploy and model new best practices and technologies:* Higher education institutions can embrace the GDPR as a means to prepare themselves for a new era of personal-information management. Protecting personal information privacy by establishing new infrastructure and policies may not only improve data security but also enhance efficiency across the institution. This can also provide a template to share with those supporting the institution for managing the personal information within their organizations — involving EU data subjects and others.

Higher education institutions are often on the leading edge of social, cultural, and technological issues; GDPR encapsulates all these elements in a digital context. Is your institution ready for a brave new world of risk — and opportunity?

[17] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Canon U.S.A. is not engaged in the rendering of professional advice or services including, without limitation, legal or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the suggestions discussed in this white paper. Canon USA does not make any warranties concerning the accuracy or completeness of the opinions, data and other information contained in this content and, as such, assumes no liability for any errors, omissions or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data or other information.

Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, GDPR, Sarbanes-Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

Prepared as of 2.8.19. Rules and regulations may change from time to time. As stated above, please have your own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.