IDENTITY AUTOMATION

GDPR Compliance for Higher Education

How Modern IAM Solutions Simplify the Process

Contents

The Stakes Are Real — And Higher Than You Might Think

The United States has long been the country of choice for international students looking for a quality higher education experience. In 2017, the US hosted about 1.1 million international students, more than any other country in the world.[1]

Hosting foreign students often means complying with rules and regulations that these students bring with them from their home countries. For students from the European Union (EU), US colleges and universities must now adhere to comprehensive and mandatory privacy rules put forth in the EU's General Data Protection Regulation (GDPR).

The GDPR, which went into effect on May 25, 2018, is designed to protect the privacy rights and personal data of every EU citizen, regardless of where they live in the world. The new regulation outlines the requirements for personal data handling, maintenance, and retention.[2]

Institutions of every size and stripe—private sector companies, nonprofit organizations, and educational institutions—need to consider these requirements when creating practices that are GDPR compliant. And if a breach is detected, the institution must file a report with the appropriate data protection authority (DPA, or the independent agency in each EU country charged with enforcing the GDPR) within 72 hours of discovery.

Failure to comply with GDPR is much more than a slap on the wrist. Regulators can impose fines of 4 percent of revenue from the previous year or up to 20 million euros ($23 million).

Failure to comply with GDPR is much more than a slap on the wrist. Regulators can impose fines of 4 percent of revenue from the previous year or up to 20 million euros ($23 million), whichever is greater, for violations.[3]

With the stakes for noncompliance so high, how prepared is your college or university for the GDPR? If you're uncertain of your school's GDPR responsibilities or how you'll meet them, we've got some good news: you're not alone, and Identity Automation can help.

This guide breaks down the GDPR for higher education and outlines clear, actionable steps to help you navigate the road to GDPR compliance. We'll explain the role Identity and Access Management (IAM) plays in ensuring GDPR compliance and the functionality your IAM solution must have to meet these needs. And finally, we'll review how a **GDPR Health Check** can help you assess your IT environment's current state of GDPR readiness and how our IAM platform, RapidIdentity can get you up to speed.

The Fundamentals of GDPR

Directly or indirectly, the vast majority of US-based higher education institutions have some relationship with countries in the EU. Whether it is a French student applying online for admission, an alumnus living in Germany who makes an online donation to the school, or a faculty member collaborating on a research project with colleagues in Italy, every routine digital interaction must adhere to the tenets put forth in the GDPR.

Even elementary and high schools need to be prepared for GDPR — particularly if they routinely host foreign exchange students or sponsor travel abroad programs.

At its essence, the GDPR dictates that university officials tasked with security and compliance, typically the chief security officer (CSO) or chief information officer (CIO), must have systems in place that thoroughly manage and track how and where the data they have on EU citizens is stored, shared, and used.

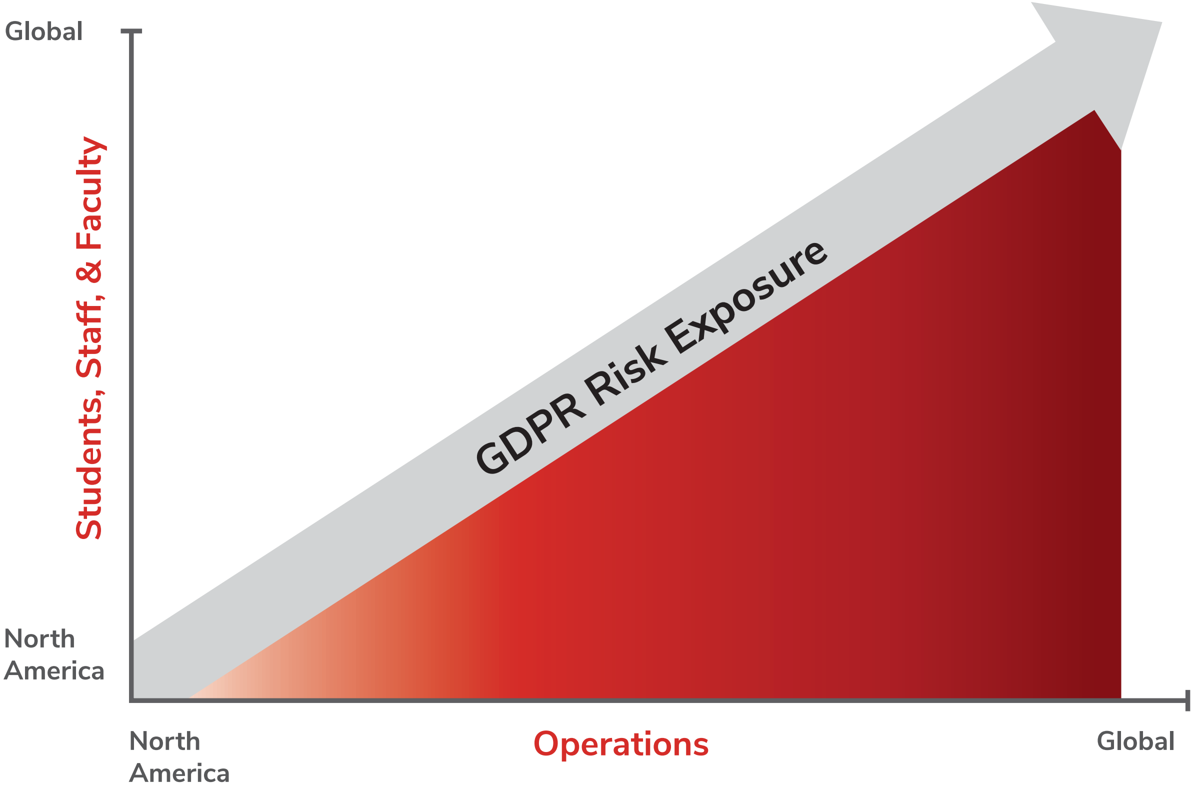
GDPR Core Principles

The controller or handler of the data must be responsible for, and be able to demonstrate, their compliance with the following principles:

- Ensuring lawful, fair, and transparent processing of individuals' data
- Limiting data usage solely to the purpose for which it was obtained
- Ensuring that data is adequate, relevant, and contains only the information necessary to accomplish its goal
- Maintaining data accuracy and keeping it up-to-date, while also properly removing or destroying data, without delay, when user has requested its removal
- Keeping data for a period of time specific to its intended use
- Processing data in a secure manner to protect the rights and privacy of individuals while preventing accidental loss or destruction of the same
- Strictly regulating the export of personal data outside of the GDPR
- Reporting any data loss or breach in a timely fashion

As many Information Security professionals have noted, the current context of the GDPR is somewhat left to interpretation, frequently using terms such as “reasonable” or “timely,” while never fully clarifying what they mean.[4] As more cases are reviewed, the GDPR will likely be amended to become less ambiguous and complicated. But for now, the lack of clear interpretation means that universities, and the vendors that provide them with software-as-a-service (SaaS) products, must take extra precautions when preparing themselves for compliance with this legislation.

DETERMINING YOUR GDPR RISK EXPOSURE



– Courtesy of Sophos, December 2017

A general breakdown of GDPR risk exposure by the breadth of a company’s (or university’s) operations and customer (student, faculty, staff) base. Organizations with the majority of their operations and people based in North America have minimal risk. The risk exposure grows as organizations go global, either today or in the future.

GDPR IS UNAVOIDABLE AND EXPANDING

While the GDPR is still quite new, many of its core tenets are already becoming a permanent fixture in the US's data security landscape. The recently passed California Privacy Act of 2018, which goes into effect on January 1, 2020, mirrors the EU law in that it gives California's 40 million residents the right to be informed about what kinds of personal data companies have collected on them, why it was collected, and how it is used.[5] It also gives customers the right to request deletion of personal information, opt out of the sale of their information, and access the information in a readily useable format.

The pace of GDPR-like regulation is expected only to accelerate, and other states have already begun working on their own privacy legislation.[6] The consensus within the IT industry is that e-privacy-as-human right will eventually become the law of the land throughout the US.

The consensus within the IT industry is that e-privacy-as-human right will eventually become the law of the land throughout the US.

But by October 2018—five months after the GDPR went into full effect—none of the EU's DPAs had levied any fines.[7] The common reason is that it is too early—both for the organizations violating the GDPR and for the DPAs themselves—to impose new fines under a regulation that has only been in effect for less than a year.

The GDPR is already making its presence felt, however. Rule enforcers in many EU countries have seen a spike in the number of complaints about violations, with France and Italy reporting a 53 percent jump in complaints from the previous year.[8] At least one DPA in Germany issued a ban on personal data processing from webcams that did not comply with the new regulations.[9] And in the UK, the Information Commissioner's Office reported more than 8,000 breach reports and 19,000 public complaints about data access and security since the GDPR's May 25th start.[10]

EU governments have recently started adding staff to review GDPR complaints, and DPAs are offering recommendations on how systems can be fixed to become GDPR compliant. The first set of major penalties, which will include admonishing the offenders, imposing temporary bans, issuing ultimatums, and finally, imposing punitive fines, is expected by early 2019.

What’s the Status?

With penalties and fines coming so soon, where is your school on the pathway to GDPR compliance? Are you just getting started or not sure where to begin?

If just thinking about these questions makes you nervous, you’re in good company. Most US colleges and universities have not done enough to beef up their security protocols and get compliant by the start date.

“Many US universities, the larger and more prominent ones in particular, think they have come a long way,” says Orville Wilson, the Lead Cybersecurity and Compliance expert with Moran Technology Consulting. This is evidenced in the recently released 2018 Campus Computing Survey, in which 48.6 percent of all higher education institutions reported that they currently comply with GDPR.[11] Private universities felt the most confident, with 69.2 percent reporting current GDPR compliance. Only 35.7 percent of community colleges reported being GDPR compliant.

Closer inspection of these stats suggests that more than 50 percent of all institutions do not consider themselves compliant. “And among the ones that feel confident in their compliance, all most of them have done is put a privacy statement on their website, and perhaps enacted one or two of the simpler policies around GDPR,” Wilson adds.

Closer inspection of the stats indicates that more than 50 percent of all institutions do not consider themselves compliant with GDPR.

According to Moran Technology Consulting, many universities have simply conducted a quick data review, changed up a few policies to move their data management closer to GDPR compliance, and then moved on. “I fear that many of these universities are not fully aware of the ramifications of non-compliance,” Wilson says. “They figure that they are showing some level of commitment to the GDPR, and that will buy them some time. And then, they will come back at some later date to shore up their data security and make sure that it is in line with GDPR regulations. But unless they are faced with a true non-compliance event and are hit with heavy fines, many of these universities may never get back to it. It’s quite a gamble.”

The more substantial work around data mapping—the mandatory documentation and the systems-in-place to ensure that EU data is handled, protected, and kept anonymous—is largely left undone. Even some institutions that have taken great pains and spent many months to comply with the GDPR—including identifying all data that might fall under GDPR protection and running various what-if scenarios for handling and removing European data—still have a long way to go to achieve full compliance.[12]

The lack of early enforcement has complicated the compliance picture. Many universities who felt an early sense of urgency around becoming GDPR compliant are now taking a "wait-and-see" approach—slowing their compliance efforts until they see fines levied against larger educational systems. Many US schools still do not understand the impact that the GDPR will have on their enrollment, research, and business dealings with students, faculty, and staff—who are either from the EU or doing work there.

And while university IT leaders have been told not to panic about GDPR enforcement at recent national education conferences and seminars, they have also been advised not to get complacent.[13] The smart move is to start taking steps now, at a reasonable and measured pace, to come into compliance. The other option, waiting and rushing, raises the risk of making mistakes and spending more on a data protection solution that does not fully address every GDPR requirement.

The smart move is to start taking steps now, at a reasonable and measured pace, to come into compliance.

Getting Compliant: Where to Begin?

GDPR changes the entire concept of privacy for many US institutions. While it is largely treated as a fundamental human right in Europe, privacy is considered more of a consumer right in the US. As a result, the requirements put forth by the GDPR are jarring for many US-based institutions who are not accustomed to thinking this way. This begs the question: If the GDPR is mandatory, and the concept of privacy is changing at a fundamental level throughout the US, what steps should schools take to get GDPR compliant?

Regardless of how far along your school is on the GDPR compliance path, there are several steps that can make the process manageable and straightforward:

1) ESTABLISH ACCOUNTABILITY AND THE GOVERNANCE FRAMEWORK

This vital first step requires your school's CIO (or other manager leading the GDPR compliance effort) to get administrative support for starting the project and seeing it through to completion. This will require a careful and candid discussion about the benefits and risks of GDPR compliance (or non-compliance). At this point, your institution should appoint a GDPR project manager who reports to the CIO and is responsible for keeping the different groups on track with their specific contribution to the compliance effort.

2) SCOPE THE PROJECT LIST

Working with your school's IT department, the project manager identifies the college departments, administrative offices, and other departments that are within scope—anyone who will be impacted by (or who will impact) the data management and security process, and whose day-to-day activities directly or indirectly influence GDPR compliance.

This step also identifies all standards and/or management systems that might provide a framework to ensure GDPR compliance. There may be some overlap with other best practices and procedures, such as ISO 27001 (the information technologies security best practice).[14]

3) CONDUCT A DATA INVENTORY AND DATA FLOW

This process maps out how European data moves through the university—where and how it is stored and processed, who sees it, how much is shared, how it is transmitted, and so on.

4) ASSESS THE RISK IMPACTS ON THE DATA

This step calls for determining how easily the data can be breached, siphoned, lost, deleted, or stolen as it moves through the university system. This is commonly done through penetration testing, which uses ethical or "white hat" hacking to test your system for security vulnerabilities that an attacker could exploit.[15] (Moran Technology Consulting offers a range of vulnerability scans and penetration testing services specifically for this type of need.) With this assessment, you can better understand your current compliance position.

While it is largely treated as a fundamental human right in Europe, privacy is considered more of a consumer right in the US.

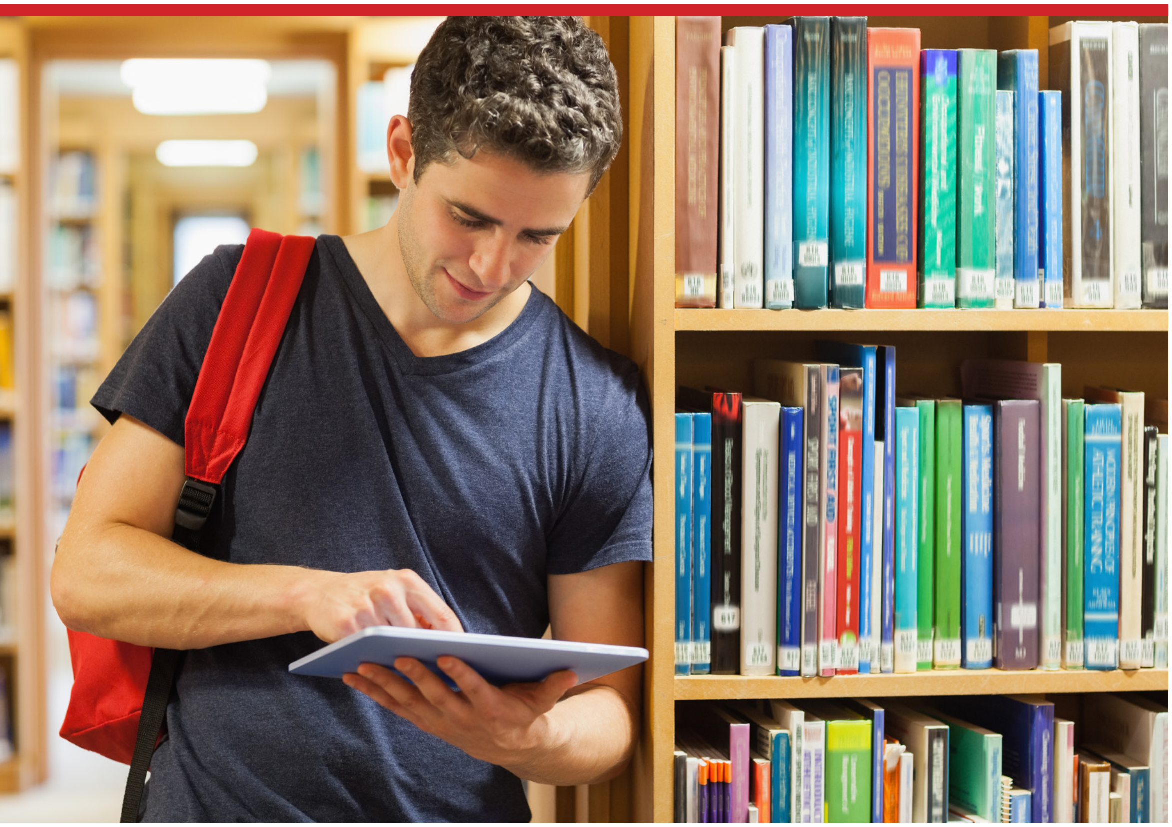
5) CONDUCT A GAP ANALYSIS

A gap analysis compares what is in place today with what should be in place for GDPR compliance. It identifies areas for improvement—where security and processes need to be tightened up—to achieve compliance.

Common questions to ask during this gap analysis include: Is the data encrypted when it comes into the university system? Is it stored in clear text? Is it shared with all the right departments? Asking these questions will help you understand what kind of protection and tech controls are required and then guide how you can tighten up the security to get compliant.

6) DEVELOP OPERATIONAL PROCEDURES

With the previous steps as your guide, put the processes, policies, and systems in place to close the gaps and get compliant.



> "Among the [colleges and universities] that feel confident in their compliance, all most of them have done is put a privacy statement on their website, and perhaps enacted one or two of the simpler policies around GDPR."

Orville Wilson
Lead Cybersecurity and Compliance Expert
Moran Technology Consulting

Still Not Sure How to Start? A Health Check Can Help

Even using the general roadmap from the previous section as a guide, understanding the complexities of GDPR requirements and the potential risks facing your institution is difficult. Moran Technology Consulting, an Identity Automation partner and IT management consultancy serving higher education and business clients, offers a **GDPR Health Check** that quickly identifies how GDPR applies to your institution and what efforts might be required to mitigate those risks.

The GDPR Health Check is an all-encompassing assessment of your total IT environment as it relates to GDPR.

For a low fixed fee, the **GDPR Health Check** provides valuable insight and direction in several key ways:

- Identifies required stakeholders and participants across your institution that may transmit, process, and store EU data, such as: Admissions, Financial Aid, Bursar, Registrar, Housing, Advancement, Human Resources, Finance, Student Health Center, and Public Safety/Police Department.

- Conducts a joint kick-off meeting with all participants to explain GDPR and the Health Check objectives, scope, and approach.

- Conducts individual interviews/workshops with each of the participating stakeholder groups.

- Reviews existing documented policies, standards, procedures, processes, and mechanisms to protect, anonymize, and/or pseudonymize the data.

- Delivers the **GDPR Health Check Report**, which identifies and prioritizes risks associated with GDPR, as well as a plan for addressing each of the identified medium and high risks.

The **GDPR Health Check** is an all-encompassing assessment of your total IT environment as it relates to GDPR. It helps you assess your starting point and guides you along the steps you need to follow to get compliant. This includes a review of your current Identity and Access Management (IAM) solution. Depending on the IAM system that you currently have in place, the assessment might find that its features and functionality are not robust or flexible enough to facilitate your journey to GDPR compliance.

A Modern IAM Solution Clears a Path to Compliance

Here is where a modern IAM solution can help. Today's IAM systems give universities a highly-available, centralized, and flexible identity management infrastructure that incorporates the principles of GDPR and other data security legislation into their day-to-day business processes, and in an automated fashion. This ensures consistent, reportable, and auditable controls that can be utilized to demonstrate organizational compliance, while freeing up IT staff to focus on other business objectives.

During provisioning, IAM solutions quickly identify whether the person in question is European. If they are, the solution workflow ensures that the person's data is stored in another location or undergoes pseudonymity, anonymity, or encryption to protect the user's identity.

IAM solutions also ensure that, per GDPR requirements, the European user's data has a finite lifetime in the university system. During deprovisioning or anytime the user requests it, the data is carefully and completely deleted—without risk of being lost, leaked, or stolen.

During provisioning, IAM solutions quickly identify whether the person in question is European. If they are, the solution workflow ensures that the person's data is stored in another location or undergoes pseudonymity, anonymity, or encryption to protect the user's identity.

While a number of IAM solutions provide some level of data protection and security in line with the GDPR mandates, Identity Automation's RapidIdentity offers several unique features. The platform delivers maximum flexibility to adhere to existing compliance regulations and adopt new policies as they arise—but without the expense and complexity of other IAM solutions that must be customized before you can use them.

RapidIdentity offers a great deal of functionality right out of the box. And as new security threats emerge, the platform can be easily configured to adapt to new ad-hoc rules and requirements.

RapidIdentity also affords flexibility in hosting. It may be locally hosted within the university to maintain complete, in-house or in-network data flow. Or, RapidIdentity may be implemented and hosted within a cloud service, such as Amazon Web Services (AWS), where compliance with regulations like GDPR are a priority for implementation in the cloud.[16]

Assure GDPR Compliance with a Complete IAM Solution

While much of the focus on GDPR compliance has centered on US companies in the private sector, US universities with some foothold in Europe and/or with EU citizens as students, faculty, alumni, or staff are also in the regulators' sights. And whether your university is dealing with one European or 100,000, the result is the same: GDPR compliance is mandatory, and the time to comply is now.

Regulatory authorities in the EU will soon start issuing penalties for non-compliance. No matter how far along your school is on the GDPR compliance journey, you need to get moving. A reasoned, stepwise approach—one directed by a dedicated GDPR manager—should be adopted and include establishing a governance framework, scoping which departments and administrative functions impact data security, conducting a data inventory, assessing data breach risks, and identifying and closing compliance gaps. Taking these steps now will make the compliance process more orderly and efficient, while helping you to avoid rushing through a solution that is too expensive, poorly executed, and not adaptable to future regulatory requirements.

Having the right technology in place is another critical factor for ensuring that your school can meet its GDPR requirements.

Having the right technology in place is another critical factor for ensuring that your school can meet its GDPR requirements. Your current IAM solution may not offer the flexibility or capabilities to correctly manage and maintain European identity data or adapt as data privacy regulations continue to evolve and gain traction in the United States.

Switching to a modern IAM solution, like RapidIdentity, gives you a cradle-to-grave identity management solution that addresses all of your school's governance, risk, and compliance needs, while aligning your data management protocols with GDPR's requirements. With RapidIdentity, you can ensure that European identity data is correctly handled through all stages of the identity lifecycle for every user, regardless of the nature of their relationship with your institution.

Ready to take the next steps? Contact us today to discuss your GDPR compliance challenges, learn more about RapidIdentity, or to schedule your GDPR Health Check!

Sources

1. Zong, Jie and Batalova, Jeanne. "International Students in the United States," Migration Information Source, a publication of the Migration Policy Institute, 9 May 2018, https://www.migrationpolicy.org/article/international-students-united-states#CountryOrigin, Accessed 14 Nov 2018.

2. "Implications of the General Data Protection Regulation: An Interassociation Guide," May 2018.

3. McKenzie, Lindsay. "European Rules (and Big Fines) for American Colleges," Inside Higher Ed, 13 March 2018, https://www.insidehighered.com/news/2018/03/13/colleges-are-still-trying-grasp-meaning-europes-new-digital-privacy-law, Accessed 12 July 2018.

4. Nadeau, Michael. "General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant," CSO, 23 April 2018, https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html, Accessed 10 August 2018.

5. Ghosh, Dipayan. 'What You Need to Know About California's New Data Privacy Law," Harvard Business Review, 11 July 2018, https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law, Accessed 23 October 2018.

6. Locklear, Mallory. "Georgia Congressman Is the Latest to Introduce Data Privacy Bills," Engadget, 26 July 2018, https://www.engadget.com/2018/07/26/georgia-congressman-introduces-data-privacy-bills/, Accessed 29 October 2018.

7. Nohe, Patrick. "GDPR: The Fines Are Coming—Likely by Year-End," Hashed Out, 11 Oct 2018, https://www.thesslstore.com/blog/gdpr-fines-are-coming/, Accessed 14 Nov 2018.

8. Chee, Foo Yun. "Exclusive: EU Privacy Chief Expects First Round of Fines Under New Law by Year-End," Reuters, 9 October 2018, https://www.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUSKCN1MJ2AY, Accessed 14 Nov 2018.

9. Meyer, David. "Here's Why the First GDPR Fines Could Still Be Months Away," IAPP, 28 Aug 2018, https://iapp.org/news/a/heres-why-the-first-gdpr-fines-could-still-be-months-away/, Accessed 14 Nov 2018.

10. Schwartz, Mathew J. "GDPR: 8,000 Data Breach Reports Filed So Far in UK," Data Breach Today, 10 Dec 2018, https://www.databreachtoday.com/gdpr-8000-data-breach-reports-filed-so-far-in-uk-a-11828, Accessed 14 Dec 2018.

11. Green, Kenneth. 2018 Campus Computing: The 29th National Survey of Computing and Information Technology in American Higher Education, p 22, October 2018, www.campuscomputing.net.

12. Clark, Dan. "With GDPR in Place, US Higher Education Institutions Face Their Own Challenges," Corporate Counsel, 20 June 2018, https://www.law.com/corpcounsel/2018/06/20/with-gdpr-in-place-u-s-higher-education-institutions-face-their-own-challenges/?printer-friendly, Accessed 7 Sept 2018.

13. McKenzie, Lindsay. "Don't Panic About GDPR, Colleges Are Told," Inside Higher Ed, 1 November 2018, https://www.insidehighered.com/news/2018/11/01/eu-slow-enforce-new-data-privacy-rules-colleges-told-not-panic-about-lack-compliance, Accessed 3 November 2018.

14. ISO/IEC 27000 family - Information security management systems, International Organization for Standardization, https://www.iso.org/isoiec-27001-information-security.html.

15. "Pen Test (Penetration Testing)," TechTarget, https://searchsoftwarequality.techtarget.com/definition/penetration-testing, Accessed 14 Dec 2018.

16. https://aws.amazon.com/compliance/gdpr-center/

IDENTITY AUTOMATION

7102 N Sam Houston Pkwy W, Ste 300
Houston, TX 77064, USA

Phone: +1 281-220-0021
Email: info@identityautomation.com
www.identityautomation.com

IDENTITY
AUTOMATION™