Case Study: Future-proofing data handling at KSU

Excerpt from white paper, ***GDPR in the United States***,
Amy Daultrey Krishnaswamy, July 2022
available at amydaultrey.com/resources

Photo by Héctor J. Rivas unsplash.com/photos/1FxMET2U5dU

Case Study: Future-proofing data handling at KSU

Imagine a large university with a dozen or so departments, a few thousand staff, almost 130,000 alumni and a recent merge with another major institution. A lot of data being pulled in different directions. Myriad processes and hands on the wheel. Drop into this picture a new employee with a predisposition to get in front of data challenges and embrace innovation, who happens to be familiar with the EU GDPR.

This scenario has been playing out at Kennesaw State University (KSU, kennesaw.edu) in the metro Atlanta area. A public research university, KSU has 43,000 students and is part of the University System of Georgia. Founded in 1963, it grew into an accredited university in the early 90s and merged with Southern Polytechnic State University (SPSU) in 2015. With 12 colleges and an alumni association (plus various alumni societies, sports teams, interest groups) there are many demands on the use of its alumni data.

Matt Bain joined KSU at the start of 2020 as Executive Director of Advancement Services. What he found was processes for email marketing duplicated across departments with some working from duplicate data sets. Fuzzy data ownership was making consistency in communications difficult but also honoring constituent preferences a challenge (and anywhere data ownership and process duplication is an issue, security vulnerabilities may be found). The merge with SPSU in 2015 had combined two databases into one. Although great for consolidation of resources and effort, this presented its own backlog of clean up tasks and a pressing need to refine standards, define processes and refresh training.

Matt Bain, Executive Director of Advancement Services at KSU

This need to refine standards also presented an opportunity. As a higher education institution and part of a state system, KSU is used to complying with complex state and federal mandates and following legal guidance. **Could it go one step further than what was required for alumni data, and take this comfort with regulation, and desire for better standards, and make these the norm?** Doing so would prepare the institution for any future legislation that will specifically target data ownership, privacy and constituent rights and preferences.

As the pandemic rolled in, Matt took advantage of the downtime from usual activities to tackle cleanup and process improvement, with one eye on what could be done to consolidate, elevate and future-proof. He explained to me why this line of thought was even a possibility:

> I came from 18 years at Georgia Tech which is a forward-thinking organization. This had everything to do with my attitude to [EU] GDPR when it came along. Legal had to figure out how it applied to our alumni and we had to find a way to track consent. We also had to examine what data points were considered sensitive under GDPR and where these came from. [Although GDPR applied to a fraction of the alumni body] we embraced it as an opportunity to set standards and procedures for everyone.

For example, they started looking at how a long-view consent could be asked of students at the point of enrollment, rather than at graduation. It would grant permission for the student's information to be used beyond graduation and provide a seamless foundation for communications with them. Getting this in place would, for new alumni at least, minimize the impact of future legislation that demands constituent consent.

Stepping into his new role at KSU, Matt has taken many of the lessons learned at Georgia Tech. In taking on cleanup and the legacy of two databases, in trying to refine standards, what opportunities could be seized to future-proof KSU?

Tackling the silos of information, the advancement division assumed the role of centralized clearing house for email communications to alumni. Controlling the data set, branding and messaging, this takes a burden off individual departments and reduces the number of hands on the wheel. So far three departments have used this service and email communications as a tool is being opened up for self-service use—with oversight provided by the advancement division.

Meanwhile, Matt spearheaded a task force to analyze opt-outs and how each department was handling these. A separate task force looked at security and breach defense. Winning over staff across departments through these task forces is helping raise awareness, improve processes and open up further opportunities through cooperative effort.

Matt is hopeful the roll-out of the clearing house model will continue to other divisions. He also wants to keep the task force momentum going. These efforts are a work in progress but steps to get even this far have improved processes, security and data quality. Staff have more confidence in the data—in both alumni contact information and the accuracy of their preferences for communications. KSU is very well placed to respond to new legislation when it comes.

The KSU approach

- Compile a **data cookbook**. This maps systems, fields and metadata and identifies which of these are considered sensitive or personally identifiable information under GDPR. The cookbook also identifies ownership or stewards of the different pieces of information. It enables a place to track data sharing (and flag unnecessary data sharing) and documents a hierarchy of breach preparedness and reaction—lean on legal advice for defining your chain of command. The beauty of compiling a data cookbook is it prepares an organization not only for internal data handling issues, but also issues that arise when a third party is involved. Consider another breach of the nature of that at Blackbaud in 2020: with a cookbook in place, identifying potential sensitive data exposure is much faster and more accurate.

- Try and **win over staff across departments** to eliminate shadow systems and close security loopholes. Make sure everyone is using multi-factor authentication to access any and all data systems. Help staff understand that they should not hoard spreadsheets, paperwork or share sensitive data with external parties (like volunteers and donors). Have staff review your security policies every 6 to 12 months and take every opportunity to refresh their awareness.

- Set up a **task force** to analyze unsubscribes and opt-outs and how each department responds to them. The processes may be varied and problematic but you may also discover innovative approaches that would benefit everyone. Share best practices and try and achieve consistency in policies and procedures. Make sure everyone knows what to do with a “right to be forgotten” request (KSU uses a redact approach rather than deletion to avoid the risk of unintended re-acquisition). These efforts will also help present a cohesive front to your constituents as it enables bringing together branding and messaging decisions.

- Establish a **centralized clearing house** for all communications with alumni and donors. Spin it as taking a responsibility off the plate of individual departments and interest groups. Provide oversight for compiling data sets, branding and messaging of communications. For mailings, work directly with the mailing house that department is using to avoid the data set passing through unnecessary pairs of hands.

- Consider the best time and place to seek **consent** from your constituents, and what you’re asking them to consent to. For an educational organization where student records are shared with the alumni office, look at obtaining consent at the point of enrollment. When the data is transferred skip any information that the alumni did not consent to storing. Ensure retained information has both the consent and the date it was obtained.