A.D.

GDPR in the United States

What it means for nonprofits
What happened in the UK
What you can do to prepare

Amy Daultrey Krishnaswamy

June 2022

Contents

Introduction

Legislation in the United States to enhance the rights of individuals over their personal data is the **inevitable outcome of trends in data governance globally**. Recent enhancements by major technology companies to the privacy controls of individuals have added to this momentum. For nonprofits in particular the direction is toward **enhanced donor experience** and privacy preferences are an essential part of this. In future nonprofits will have to change their practices for contacting donors, sharing donor information and using wealth screening services.

What can be learned from a part of the world where this legilsation has already happened? What suggestions does it provide about how nonprofits in the US can prepare? The implementation of the General Data Protection Regulation (GDPR) in the European Union in 2018 had a dramatic impact on nonprofits and donors. As an example of legislation that affects nonprofits it provides a wealth of information. There was variation in how organizations prepared, responded and have operated since. This paper looks at the particular impact on nonprofits in the United Kingdom.

With GDPR-like legislation an inevitability in the US, preparations can be made in advance to minimize disruption. What can be done to face this evolution of data protection? **How can organizations future-proof their operations?** This paper looks at how a university in Georgia is addressing these challenges right now and what you can learn from their approach.

In thinking about GDPR in the US, there is scope to see it as **an opportunity**: to make data minimization standard practice, to demonstrate to donors how seriously you take their preferences, to scrutinize and enhance security, to improve your operations, increase data accuracy and in so doing achieve greater efficiency across your organization. At the end of this paper are action points you can take forward now to help you start embracing this opportunity at your organization.

Note: Throughout this paper donor data systems and fundraising practices are referred to in general terms. For resources about The Raiser's Edge 7 and NXT see links to downloadables at the end.

1.

The problem

GDPR-like legislation in the United States is an inevitability. The degree to which it applies to nonprofits, and the level of regulation at state vs. federal level remains to be seen. Based on the implementation of the GDPR across EU member states, preparation is key. Nonprofits that do not take the opportunity to change now may find adaptation a crippling challenge. Under pressure they may make hasty decisions that lead to loss of supporters and income. Additionally, failure to connect data handling to wider security responsibilities increases the vulnerability of nonprofits to digital attack and its associated problems, particularly loss of reputation. According to the Identity Theft Resource Center, nonprofits and NGOs reported 441 breaches from 2018 to 2022[1].

The General Data Protection Regulation came into effect in the European Union on May 25, 2018. The UK established a comparable set of rules to continue compliance after Brexit. Similar GDPR-like legislation has been enacted or is under way across the world, including in Canada, Malaysia, Argentina, Brazil and Switzerland.

In 2018, two US state bills were proposed on consumer privacy and business responsibility; by 2021 this had grown to 29 bills across 23 states. At the time of writing, five states have passed legislation on consumer privacy rights—Connecticut being the latest. At a federal level, numerous bills are in process. For example, the Consumer Data Privacy and Security Act, and Data Protection Act. The former of these would preempt state law if enacted.[2]

Meanwhile, Big Tech companies have been making dramatic changes. In 2021, Apple Inc. rolled out an enhancement to how iOS users can control the sharing of their data. Previously buried options became easier to access and control. In April 2021 CNN Business reported that small to medium-sized businesses would struggle with the impact on their advertising, with Facebook leading the charge in objecting to Apple’s actions.[3] Early in 2022 Google announced it would limit cross-app tracking, or the sharing of information between apps on Android devices. In February 2022 a LinkedIn editor wrote it “may be a death blow to the digital marketing practices of the last decade”.[4] Ongoing efforts in Europe to reign in the operations of Facebook and Google may have a wider impact on these companies’ activities across the globe.

[1] ITRC Notified, “Year-Over-Year Breach Trends” chart, notified.idtheftcenter.org/s/, accessed on May 2, 2022.
[2] Justin Brookman, “Consumer Reports Praises Passage of Privacy Bill in Connecticut Legislature”, Consumer Reports, April 28, 2022, advocacy.consumerreports.org/press_release/consumer-reports-praises-passage-of-privacy-bill-in-connecticut-legislature/; International Association of Privacy Professionals legislation trackers and iapp.org/resources/article/the-growth-of-state-privacy-legislation-infographic/, accessed on February 25, 2021.
[3] Samantha Murphy Kelly, "Apple's major privacy change is here. What you need to know", CNN Business, April 26, 2021, edition.cnn.com/2021/04/26/tech/apple-tracking-transparency-feature/index.html.
[4] Melissa Cantor, "Google plans big privacy changes", LinkedIn News, February 18, 2022, accessed on February 21, 2022.

Assuming the success of one or more state and federal bills in the coming years, organizations may have to adjust their data acquisition and storage practices, switch from an "opt-out" approach to opt-in, make minimization the norm and enable constituents to request data removal in an easy way. Although legislation may target corporations (and possibly weakly in the first instance) it cannot be assumed that it will not apply to nonprofits eventually: these are organizations that handle personal data and therefore are at risk of data breaches and privacy violations. Ultimately rules will likely apply to most organizations processing personal data.

When might something happen?

State and federal legislation is an inevitability but may take years to come into effect. It is also unknown the extent to which legislation will apply to nonprofits. For example, only healthcare and higher education may be affected initially or just nonprofit corporations. Healthcare foundations and state funded universities might not find it much of a leap as they are already familiar with data protection practices through HIPAA and FERPA.

To imagine the impact on nonprofits and the steps they'd have to take to prepare, there are at least three scenarios:

1. New legislation is stalled, status quo continues for the next 5+ years.
2. New legislation passes within the next 5 years but nonprofits are exempt except higher education, healthcare and nonprofit corporations.
3. New legislation passes within the next 5 years and all types and sizes of nonprofits are affected.

It's hard to imagine the third scenario at this time but developments are heavily influenced by efforts to reign in the data handling activities of Big Tech. Also recalling that efforts to legislate are active in many states, we can safely assume that the second scenario is likely, evolving to the third scenario over a longer period of time.

Why should you care?

If most nonprofits might be exempt from legislation (at least initially), why bother worrying about this? The question is not why you should care but when. The trajectory of data management is leaning towards consumer consent and a more open understanding of how the data of individuals is used, with greater consequences for organizations that do not take the security of their data and rights of data subjects seriously. **We can expect more rules and restrictions to arrive, but it is highly unlikely that there will be *less*.**

2.

Key elements of the EU GDPR

The EU General Data Protection Regulation became law on May 25, 2018. An understanding of its key terms helps us to imagine what similar legislation in the United States might look like. In general terms, the Regulation is about securing data that can be used to identify someone in the European Union. As a region-wide set of rules it aimed to remove inconsistencies between data protection laws in different member states. It improved the controls that individuals have over their data and set out rules and procedures for organizations that acquire and process that data. It affected millions of people and organizations of all kinds - from small community groups to multinational corporations. The Regulation also has teeth - financial penalties for organizations that fail to comply can be huge.[5]

For nonprofit organizations, the GDPR can be boiled down to this: **collecting only the data you need, using it in only the way you need to, storing it only as long as necessary and removing it when requested**. Read on for a primer on the key terms that impact nonprofits.

The GDPR defines the ways in which organizations can collect and use personal data - known as the **lawful basis** for processing. There are eight types, of which two are used by the majority of nonprofits:

Consent requires organizations to obtain the agreement of individuals to having their data collected and used. It has to be explicit - you cannot rely on assumption, pre-checked boxes or silence as consent. Organizations have to record when the consent was received (so they can determine recency at any time) and provide an easy way for individuals to withdraw their consent. If an organization finds it is not compliant at any time they have to seek new consent or stop processing the data - essentially, delete it.

Legitimate Interests leans on expectations of individuals - it enables the use of data by organizations so long as it is in a way that individuals would reasonably expect, where there is a need to do so, and a minimal impact on privacy.

This is the basis that charities use to contact donors who would reasonably expect to receive communications - such as thank you letters to new donors and mailings to existing donors who haven't opted out.

[5] "25 Biggest GDPR Fines So Far", Tessian, last updated May 5, 2022, https://www.tessian.com/blog/biggest-gdpr-fines-2020/

Personally Identifiable Information (PII) is any data that can be used, directly or indirectly, to identify someone. It includes the obvious (contact details, birth dates, employment) and things like social media activity, IP addresses, browser cookies, mobile IDs and geographic locators, affiliations and memberships. It includes electronic and paper records and anywhere these are stored. The key to handling this mountain of PII and avoiding storing surplus data is to use a **relevant and necessary** rule: only collecting data for specific and legitimate purposes. If you won't use it and don't need it, don't collect it. This approach also aims to discourage the widespread harvesting and retention of data for vague and non-consented purposes.

Under GDPR, a nonprofit is a **controller** of personal data. Controllers are organizations and individuals that acquire and manage data and decide what is done with it. Third parties that store data, such as a database provider, are **processors** of personal data. They are organizations and individuals that process the data on behalf of the controller. In order to legally acquire and use PII, controllers must determine whether they need the consent of individuals, and what form that consent should take; how they will store the data; how they will respond to requests from individuals to view or delete their data; and how they will handle secure passing of data to other organizations if necessary for their operations. Controllers must also have a procedure for responding to a **data breach**, notifying the regulator in their country within 72 hours and all affected individuals without delay.

Charities also have to appoint a **data protection officer,** if they do not already have one, to be the main contact for GDPR queries, to monitor compliance, advise staff of obligations and stay on top of legal requirements. It's good practice for compliance to be reviewed at least annually and whenever new staff join.

The EU GDPR enables compliant organizations to **transfer data** between member states and European Economic Area countries. Transferring data beyond these borders gets tricky: some countries have been formally recognized as having sufficient laws in place for safe data transfer. For countries that have not been recognized (this includes the US), there are terms and conditions that must be met, known as **Model Clauses** or **Standard Contractual Clauses**.

How organizations make it work

With all this regulation, how do organizations operate? Besides understanding the lawful bases under which they can function (and regularly testing this), they try and follow a rule of data minimization: only acquiring and storing information that is necessary for the organization to carry out the operations that its constituents would reasonably expect it to. This applies to existing and new records, and all places that personal data is stored. As well as databases this could be an email platform, payment platform, social media messaging, event software, membership platforms. It includes cloud storage and digital files, printed lists, paperwork and notes on desks. Here’s three examples:

EXAMPLE: Cancer charity operating a helpline and funding research

Calls to the helpline are stored if the caller consents to this. Minimal information is taken to enable categorization and analysis of conditions most/least often called about. The charity shares summary data in its work with medical professionals engaged in funded research - no PII is shared with these professionals. If an individual requests details of research programs and trials the charity provides it but does not contact the program on their behalf or provide the program with any information about them. Donors can opt in to newsletters, campaign updates and information about legacy giving. These opt-ins cannot be used for any other purpose.

EXAMPLE: College alumni society

On graduation students are asked if they would like contact from the alumni society. Since this includes careers networking most students agree and the society stores their graduation year and degree, and later their employment information. Those that opt-in to fundraising contact also receive appeals and campaign updates. Alumni are assisted in contacting classmates with the society acting as an intermediary so personal information is not shared. Reunion event hosts are required to process all attendee information through an event platform and if they wish to email alumni this is done by the society – they do not keep their own contact lists.

EXAMPLE: Wildlife rescue and conservation center

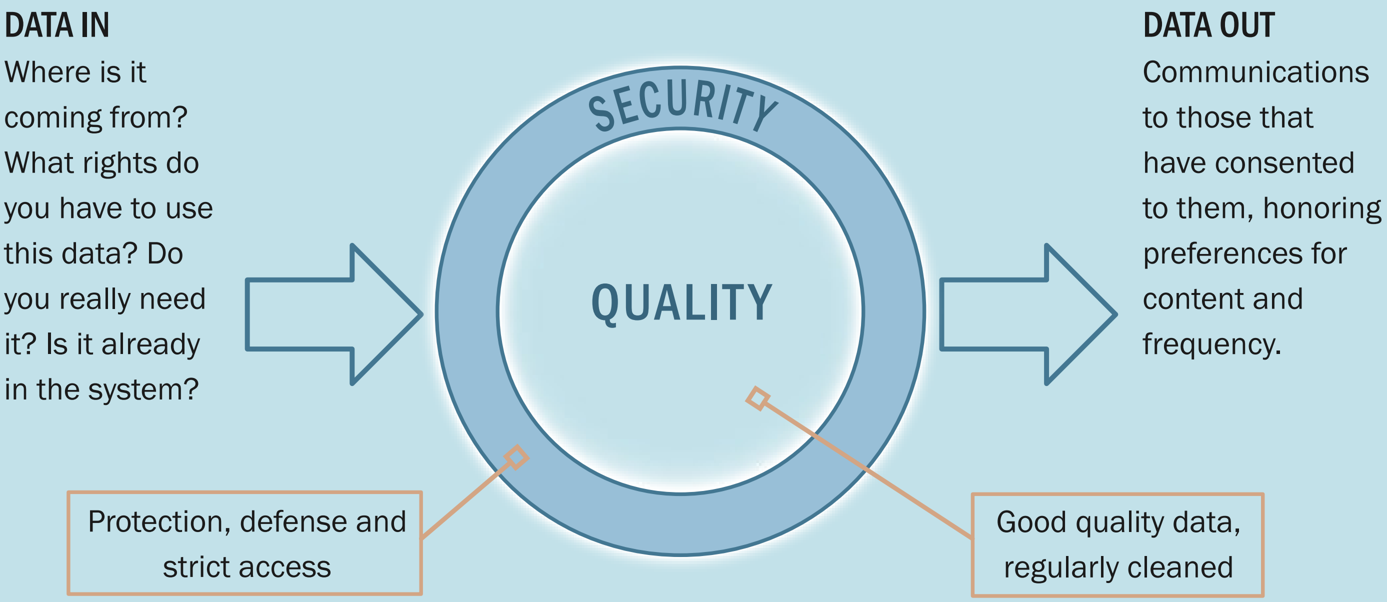
Visitors are encouraged to sign up for newsletters and campaign updates. Those that become members receive email invitations to member events and news about animals they have sponsored. Major gift officers contact repeat members who have opted in to receive fundraising updates, cultivating them for named gifts and event sponsorship. Besides event software, mailing house and payment platforms, data is not shared with any third parties and no mass screening or list acquisition is performed.

The importance of security

A fundamental tenet of the EU GDPR is the joint importance of data security and data protection, the latter encompassing how data is acquired, used, stored, shared and deleted. So to successfully rise to the GDPR challenge, organizations had to examine data security as well. In 2020, 26% of UK charities reported a breach[6]: the issue of security is ongoing and very real.

Caring for data acquired means organizations have to ensure their systems are secure, both in how data is stored and how it is used. This includes strong security settings to access systems (such as multi-factor authentication) and defined processes for users to follow.

The volume and type of data acquired is also crucial. A focus on maximizing quality, rather than volume, goes hand in glove with reducing risk. Moving away from the idea that to get results you have to send mass communications to as big a list of contacts as possible, produces better outcomes in the long run. Data that is more accurate is better quality, no matter the volume. Sending appropriate communications to good quality records produces better results and, in turn, more useful analysis of those responses. As you'll see on the following pages, although many charities in the UK saw their donor databases shrink as a result of GDPR compliance, they are now operating with cleaner, leaner and more secure systems.



DATA IN
Where is it coming from? What rights do you have to use this data? Do you really need it? Is it already in the system?

DATA OUT
Communications to those that have consented to them, honoring preferences for content and frequency.

Protection, defense and strict access

Good quality data, regularly cleaned

[5] Kirsty Weakley, "26% of charities had a cyber attack last year", Civil Society, March 30, 2021, https://www.civilsociety.co.uk/news/26-of-charities-had-a-cyber-attack-last-year.html

3.

Lessons learned: GDPR was a challenge

The implementation of the EU GDPR was a massive event that affected millions of people. The impact on charities in the UK provides some useful lessons on how to respond to this kind of legislation.

Late, confusing guidance

Although there was a two-year preparation period before the GDPR became law, this didn't mean that everyone knew what to do. Guidance was late to arrive, confusing and open to interpretation: lacking specific instructions, charities had to determine for themselves what they needed to do to comply. Since 2018 more sector-specific guidance has been published but the very nature of the legislation means it's the responsibility of organizations to figure out how to comply. Those that lacked legal advice were heavily influenced by what others were doing, which led to overly cautious responses. In the rush to follow the trend, small charities in particular struggled[8]. This was a major shortcoming of the GDPR: it was legislation aimed at large corporations but everyone was affected. It was not sophisticated enough to recognize the challenges and needs of nonprofits, especially small ones with limited resources (and in the UK the majority of nonprofits are small[6]). The guidance they needed arrived too late to be of practical use - just two weeks before the May 25 deadline[9].

An excess of caution

In the absence of sector-specific guidance an overly cautious reaction was common. Nonprofits misunderstood the bases under which they could handle data, especially for mail vs. email. This led to wholesale removal of constituents from communications and from databases. In some cases this will have been the only option where the organization had not routinely noted when and how it got consent. Other organizations hadn't been consistent about consent so could not rely on the accuracy of large chunks of their records. Nonprofits that saw their contact lists dramatically reduced had to determine what they could legally do with these "inactive" contacts: could they re-approach them to ask for fresh consent? The winners in this challenge were those who had already been on top of recording donor preferences (specific, dated) and those with the legal resources to navigate the legislation.

[7] Rebecca Cooney, "If donations fall 'don't blame the GDPR'", says academic, Third Sector, May 21, 2018, thirdsector.co.uk/donations-fall-dont-blame-gdpr-says-academic/fundraising/article/1465294; Shamal Faily, "Small charities face bankruptcy for not complying with GDPR, but put clients at risk if they do", The Conversation, May 21, 2018, theconversation.com/small-charities-face-bankruptcy-for-not-complying-with-gdpr-but-put-clients-at-risk-if-they-do-95463.

Strained resources

Appointing a data protection officer, allocating staff time to understanding the GDPR, communicating with donors and inspecting records for consent was a major demand on resources. In an NFP Synergy survey of 176 staff at various UK charities in 2018, 89% reported that it had taken a lot of time to comply with the regulation and 75% reported a hit on money and other resources.[10]

Lack of testing

In the rush to send notices to constituents about how they could amend their preferences, some organizations didn't test these for usability. It's impossible to estimate how many potential opt-ins were lost simply because the mechanism for responding didn't work, couldn't cope with the volume of traffic or hadn't been optimized to work in other languages, on mobiles, tablets or with screen readers.

Donor fatigue

In the weeks leading to May 25, 2018, consumers were receiving increasing numbers of emails containing "GDPR notices" or "farewell unless you want to hear from us" messages from every single organization they'd ever given their email address to, from small community groups to large retailers. Nonprofits were included in this deluge and the closer to the deadline, the more likely the recipient was to ignore or delete the email. For many people this was an opportunity to reduce the number of emails they received - especially for communications they could not recall signing up for. The messaging was also mixed: some companies told consumers there was nothing they needed to do and this was just a legal notice; others required recipients to click a button to opt-in to future email communications; others required them to do this for mail too, or even to log in to update their preferences. Many of these messages took the "farewell" approach: an email stating that if the recipient did not respond within a given timeframe the organization would assume they no longer wished to receive communications and would be taken off a list.

[8] Charity Commission, "Recent charity register statistics", UK Government, October 18, 2018 gov.uk/government/statistics/charity-register-statistics.

[9] Hugh Radojev, "ICO publishes guidance on consent ahead of this month's GDPR deadline", Civil Society, May 10, 2018, civilsociety.co.uk/news/organisations-not-required-to-automatically-refresh-old-consents-under-gdpr.html.

[10] Debbie Hazleton, Evelyne Kemunto and Joe Saxton, "Key things our 'Life after GDPR' surveys tell us", nfpResearch (formerly nfpSynergy), October 17, 2018, nfpsynergy.net/blog/key-things-our-%E2%80%98life-after-gdpr%E2%80%99-surveys-tell-us.

Not following up - a lost opportunity

Some organizations that asked all their constituents to opt-in to future communications had not planned what to do next. This was a massive opportunity to follow up and keep or refresh a relationship with constituents. With a strain on resources, a “fix and forget” attitude focused on compliance, not engagement. Opting in required an act on the part of the constituent and deserved a follow-up: a later thanks email or, to avoid inbox swamping, a notice of thanks in a regular newsletter. The impact of not following up is subtle and hard to quantify, but arguably the failure to address the GDPR elephant in the room had a negative impact over the long term. For some constituents, being asked to update preferences may have been a mild irritant they thought nothing further of. For others the way organizations responded to GDPR demonstrated their professionalism, commitment to security and respect for supporters. Including a note of thanks or other message about security at the very next opportunity was an easy win to demonstrate that GDPR was more than a box-ticking exercise.

Inconsistency

Numerous organizations made changes to comply and meet the GDPR deadline, but did not follow through on all aspects of their interactions with consumers. It is a requirement of the legislation that filling in a form for communications requires an opt-in, not an opt-out. To this day, some organizations are still not following this requirement, “silently” opting people in to communications, or using opt-out or pre-checked boxes (persistent offenders tend to be for-profit companies, not charities). The experience for the consumer is obvious: they were not expecting to hear anything further, so when they do this is can be a negative experience. Additionally, some organizations took a narrow approach, making minimal changes to meet the legislation but missing the wider need to inspect and rectify the security of *all* their systems and handling of data. They may have tightened up their website forms but overlooked paperwork, email accounts, volunteer lists, spreadsheets on staff laptops and wholesale storing of information they did not need.

Changing course

Some organizations, having taken an overly cautious approach, changed course after they better understood their obligations under GDPR. Having sent "farewell" notices to constituents requesting an opt-in to continue contact, organizations realized the impact on their active supporter base and explored how they could use the Legitimate Interests basis to continue mailing those who hadn't opted out or who had donated since GDPR came into effect. An illustrative example is the RNLI (Royal National Lifeboat Institution - a major UK charity funding search and rescue services). With a database of around 2 million supporters with an estimated 900,000 actively engaged[11], they announced in 2015 that they would be taking a cautious approach to GDPR and seeking opt-in consent from constituents. Their database shrank to 500,000 opted-in and a drop in financial resources followed. In 2019 the RNLI announced a switch to use the Legitimate Interests basis[12]. At that time their fundraising director emphasized that the 500,000 records were of engaged supporters and a good place to grow from. The impact on their fundraising was not solely because of their reaction to GDPR - there were several other factors influencing their income at the time - so it is difficult to say what outcome a less cautious approach would produced, but the change in direction certainly impacted the size of their supporter database. This no doubt also had an impact on staff who were managing the changes.

Scams

Naturally some unscrupulous individuals saw the GDPR - and the glaring lack of simple instructions - as an opportunity. Bogus "GDPR certification" programs were advertised and "GDPR experts" abounded. It can be assumed that those organizations that lacked legal resources, had a panicked response, or left their response until too late were more likely to fall victim to these scams. Since 2018, a "non-compliance register" scam has been common, accusing organizations of not complying with the GDPR. Because the legislation itself contains mechanisms for penalizing organizations that don't comply these scams can be very convincing[13].

[11] David Ainsworth, "More than 500,000 supporters opt in to RNLI communications", Civil Society, February 9, 2018, civilsociety.co.uk/news/more-than-500-000-supporters-opt-in-to-rnli-communcations.html.

[12] Priya Kantaria, "RNLI reverses 'opt-in' marketing policy to stem income fall", Civil Society, October 1, 2019, civilsociety.co.uk/news/rnli-reverses-opt-in-marketing-policy-after-income-fall.html.

[13] Mike Puglia, "Don't get hooked by GDPR compliance phishing scams", ITProPortal, December 7, 2020, itproportal.com/features/dont-get-hooked-by-gdpr-compliance-phishing-scams/

4.

Lessons learned: GDPR was an opportunity

It wasn't all bad. In among the hard work to achieve compliance was an opportunity to improve data and processes, enhance relationships with donors and a moment for the whole charity sector to evolve in the right direction.

Better policies, protection against attack

GDPR enhanced and reinforced legislation that was already in place in the UK (such as the Data Protection Act 1998). It set expectations for consumers on how they could expect their data to be treated. The policy "refresh" that the GDPR triggered has been seen as a positive. In a survey of nonprofits in 2018, 70% agreed that GDPR had "helped us get our data protection house in order"[14]. Those that realized GDPR was an opportunity to improve the security of their data helped future-proof themselves against attack. In an article in early 2018, academics from Coventry University summed it up:[15]

> **Remember GDPR is not a choice between privacy or innovation: it's about privacy and innovation. See it as an opportunity to stop storing data for future use and to better understand what data you need to retain. GDPR is an opportunity to reduce the risk of being the victim of a data scandal caused by poor privacy practices.**

Higher quality, more reliable data

Many nonprofits took the opportunity to clean and purge their data, working with less records but of better quality. This included addressing backlogs of duplicates, removing redundant records, deleting unnecessary spreadsheets and surplus contact lists. Setting in place improved procedures for responding to constituent requests (to view or remove their information, or complain about how it was handled) gave gravitas to the need for accuracy - especially as organizations are required by law to respond promptly to these requests. Ensuring ongoing compliance with the legislation by keeping on top of these procedures helps maintain data quality over the long term. The improved quality of data also led to more useful analysis and reporting.

[14] Debbie Hazleton, Evelyne Kemunto and Joe Saxton, "Key things our 'Life after GDPR' surveys tell us", nfpResearch (formerly nfpSynergy), October 17, 2018, nfpsynergy.net/blog/key-things-our-%E2%80%98life-after-gdpr%E2%80%99-surveys-tell-us.

[15] Sara Degli-Esposti and Maureen Meadows, "GDPR: ten easy steps all organisations should follow", The Conversation, February 20, 2018, theconversation.com/gdpr-ten-easy-steps-all-organisations-should-follow-90651.

Increased engagement

GDPR came on the back of several years of scrutiny of fundraising practices, and media reports of cold-calling, spamming and other unethical approaches that smacked of desperation. Getting away from harvesting and acquisition at any cost, and instead focusing on data quality, stewardship and messaging improved engagement and lifted the charity sector as a whole. A change from relying on supporters to opt out, and instead asking them to opt in, means that those that do sign up are more likely to be engaged with the organization from the start. These are people that really do want to hear from you. With more engaged supporters, click rates and conversions improve, even though the volume of active records may be less than before.

Pride in privacy practices

Charities that embraced the changes harnessed messaging around data privacy and donor rights. Rather than a nice-to-have, organizations that championed what they were doing demonstrated how much they cared. In turn, supporters felt they could trust that organization more. When supporters and donors believe their privacy is taken seriously they are more likely not only to donate, but to share information with the charity that is useful and helps to further build a relationship. They are also more likely to speak positively about the charity to others.

Reduced costs

Over the long term some organizations are spending less money on data storage because the volume of records has reduced and they are maintaining data in less places. Those that really embraced data security are also more likely to be aligning with new and robust technologies rather than using outdated, risky or suspiciously cheap systems.

5.

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 after they left KSU. 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 e-comms 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 and 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.

6.

Preparing for the future: What might happen?

With the assumption that some form of GDPR-like legislation in the US is an inevitability, the following might be required:

- You may need to **keep a history of when your constituents opted in** to receive communications from you. Don't assume that no opt-in means you can't communicate with them – it will depend on the legislation. Keeping a history with dates of opt-in and opt-out will help prepare you for whatever legislation demands.

- You'll need to ensure you're **only keeping information about your constituents that you really need** and could demonstrate a use for if challenged.

- You'll need to have a procedure in place for fulfilling **requests from constituents to be removed from a mailing list**, to see data held about them, or to be deleted altogether. A common approach is to remove if possible (for example if the record has no gifts and is unlikely to be re-acquired) or otherwise redact all personally identifying information.

- As part of wider data security measures at your organization, you will need to have a **process for assessing new software and services** to avoid unintended retention of personal information by them. You may also need to demonstrate you've assessed existing software and services.

- If your organization operates across state lines or has donors, employees or volunteers in other states you will need to **conform to legislation in all applicable states**. Federal legislation may take precedence over state law and it may be your responsibility to determine what applies to you and where.

- As now, if your organization operates internationally **with a presence or constituents in countries with active data protection law**, you must adhere to the rules within that country.

What can you do now?

With so much unknown, the when and what yet to be determined, what can you do now to mitigate the impact of future legislation on your organization?

- **Familiarize yourself with potential legislation** and what is means for your organization. Be sure to check all states in which you operate or have constituents. Look for what the draft legislation says about what you can store about donors and for how long, and what you must not store. See links at the end of this paper to state and federal legislation trackers you can follow.

- Start **making data minimization an everyday practice**. This includes in plugins, apps and other systems besides your donor database. See links at the end of this paper for a downloadable guide to getting started with minimization.

- **Review your policies**, your public notices about how you handle constituent data, procedures that your staff must follow and the guidelines, training and support you're giving them.

- Start exploring **how best you can track constituent preferences and opt-in/opt-out history**. The standard ways to do this in your data system may not meet your organization's needs, but try to avoid workarounds that require a lot of steps or are easy to get wrong.

- **Look at your procedures for responding to constituent requests** to opt-out, view or remove their information. **Discuss with stakeholders** how best to handle these and document what everyone should be doing.

- **Get involved** with data security decision making at your organization. Look for opportunities to consolidate systems, remove surplus records and improve data accuracy. Educate users about email security, not maintaining external lists, not sharing information and keeping on top of data hygiene.

- **Get board/trustee buy-in**. Educate them about what's in the legal pipeline and why it's important. If you're recruiting a new board member, consider seeking out someone with experience in the field.

- **Train staff on what's happening but above all explain *why*** you are asking them to make changes. If users can embrace this themselves they will be more invested in protecting donor records, keeping on top of data quality and alerting you to issues when they find them. Identify staff that can be subject-matter champions for their team and help their colleagues embrace changes.

- Make sure you have a procedure in place to follow when staff leave. **Avoid knowledge drain and security gaps** by capturing day-to-day processes and knowing what to do to close a user in your system. Keep super-users of your systems to an absolute minimum - this is especially important at small nonprofits who do not have a dedicated IT team managing this.

- Require users to **enable multi-factor authentication** for all systems you use that have this feature.

- **Incorporate donor preferences into your marketing now**. When the time comes that you have to email constituents about GDPR, **use it as an opportunity** to demonstrate to them that their information is stored and used with care and respect. Avoid coming across as panicky, unprepared or reluctant to take ownership of your responsibilities.

- Finally, **keep at it**! None of this will be a one-time fix. Data protection, security and donor preferences are ongoing, dynamic, and everyone's responsibility.

7.

Conclusion

Uncertainty abounds as to when GDPR-like legislation will impact nonprofits in the United States, but it is arguably an inevitability. The trend in data handling practices, particularly influenced by the actions of Big Tech, is increasingly demanding more controls for consumers, scrutiny of security and protection against sensitive data loss.

With the assumption that legislation will happen there will inevitably be challenges for nonprofits of all sizes. Drawing on the experiences of organizations in parts of the world that already have such legislation, we can see that advance preparation, implementing changes early on and embracing privacy messaging with constituents are all essential for mitigating the impact on operations. Smaller nonprofits will need assistance and would benefit from networking with colleagues at similar organizations to share ideas and advice. It would not be wise to wait for authorities to provide guidance and support.

Some organizations in the US are already a step ahead. Healthcare foundations and universities that receive state funding are likely to adapt more quickly to potential legislation as they are already familiar with concepts and terminology through their adherence to HIPAA and FERPA. Organizations of all sizes can learn from what some of these nonprofits are doing. Kennesaw State University is an excellent example of one such organization going above and beyond what is required to prepare it for the future and minimize the impact of new legislation.

The running theme throughout this paper is that preparation is key and the aims of data protection legislation should be seen as an opportunity. Future-proofing your organization is a win-win: cleaner, leaner data systems, reduced security vulnerabilities, staff on board with changes and a constituent body that knows you are on their side. Nonprofits that do the work to prepare them for this future can expect better engagement rates, more useful analytics and reduced risk of data breaches and fines.

Resources, links & further information

Recommended websites, blogs and thought leaders to follow:

- **IAPP State Legislation tracker**: iapp.org/resources/article/us-state-privacy-legislation-tracker/
- **IAPP Federal Legislation tracker**: iapp.org/resources/article/us-federal-privacy-legislation-tracker/
- **Center on Privacy & Technology at Georgetown Law**: law.georgetown.edu/privacy-technology-center/
- **IData blog** - data management concepts and tips: blog.idatainc.com/
- **IT Governance blog**: itgovernanceusa.com/blog/category/data-protection
- **National Institute of Standards and Technology blog** - cybersecurity and privacy topics: www.nist.gov/privacy-0
- **Grant Fritchey, "GDPR in the USA"**, Redgate Hub, March 28, 2019, red-gate.com/simple-talk/devops/data-privacy-and-protection/gdpr-in-the-usa/
- **Kirk Schmidt** on LinkedIn - look out for his posts on predictive analytics and privacy in fundraising, an area to watch if you want to engage in advanced analytics using personal data: ca.linkedin.com/in/kirkschmidtcalgary
- **Nonprofits are Messy**: blog.joangarry.com/nonprofits-are-messy-podcast/. Joan Garry's brilliant podcast has useful episodes on winning over board members.
- **Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)"**, New York Times, September 6, 2021, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/amp/

Free downloadable resources available on the author's website at amydaultrey.com/resources:

- **Consents in The Raiser's Edge**: challenges and shortcomings of this feature.
- **Consents in The Raiser's Edge**: a sample setup to help you make use of this feature.
- **Info Source Options in The Raiser's Edge**: where you can track where you got information from.
- **Annual Reports and Honor Walls**: can donor names ever be listed under GDPR?
- **Sharing Donor Names**: can you share donor lists with third parties under GDPR?
- **Letting Data Go**: embracing data minimization and identifying data for deletion.

About

Amy D. Krishnaswamy is a software services consultant in the UK helping nonprofits in the UK and US improve their donor and supporter data systems and unlock their fundraising potential. Find out more at amydaultrey.com and connect with Amy at linkedin.com/in/amydkrishnaswamy/.

Photo by Nikki Van Der Molen Photography

Image credits

Tiles by Andrew Ridley unsplash.com/photos/jR4Zf-riEjI
Person using devices by Christina Morillo of WOCinTechChat.com unsplash.com/photos/UTw3j_aoIKM
Museum of Pop Culture, Seattle by Ryan Stone unsplash.com/photos/U3cctUBucn0
Reunion Tower, Dallas by Ash Edmonds unsplash.com/photos/azkczZ4r0gk
Forum Building, Barcelona by Héctor J. Rivas unsplash.com/photos/1FxMET2U5dU
Network cables by Jordan Harrison unsplash.com/photos/40XgDxBfYXM
Padlock by Muhammad Zaqy Al Fattah unsplash.com/photos/Lexcm-6FHRU