FOR PURPOSE LAW GROUP
A Professional Law Corporation

NONPROFIT

Donor Data: The New Hostage?

03.06.19 | Linda J. Rosenthal, JD

In the immortal words of Saturday Night Live's Roseane Roseannadanna aka Gilda Radner: "**It's always something.** If it's not one thing, it's another…."

Now you may have to worry about paying a ransom for your nonprofit's data.

The New Data Scam

Imagine an organization that has worked hard – for months and even years – to attract and retain donors. It's signed up 20,000 people who have each pledged monthly donations of $50. The group takes in about $100,000 from these recurring donations. That adds up to a total of some $1.2 million a year. That's a big chunk of change.

Of course, in addition to this money, the organization has acquired another valuable asset: the donor data itself. "Even seemingly **simple pieces of data** can have a high value for your organization. This is especially true if that data is tied to recurring donors, who are **over five times more valuable than one-time donors**."

Many nonprofits use DRM database vendors as well as credit card payment processing firms. For a variety of reasons, a nonprofit may want to switch providers. Recently, though, some organizations have faced an unwelcome surprise: Certain vendors are **refusing to transfer the data.**

In ***Can Your Monthly Donors Be Held Hostage?*** (May 2018), Donor Voice's Roger Craver was among those raising the alarm at "The Agitator" blog. They had "encountered many frightening examples of hostage-taking by vendors," including situations in which "large, sophisticated organizations with thousands of monthly donors have been blocked or grossly delayed in transferring their data." An organization may have forked over huge sums to build a new sustainer program, only to learn that a CRM or payment processor won't cooperate when the group decides to switch providers.

Wanting to determine – more than anecdotally – how often this happens in the nonprofit sector, Craver asked readers to fill out a short survey about their own experiences.

Just one week later, 98 organizations had responded. In ***Freeing Monthly Donor Hostages: Survey Results*****,** Craver revealed the results to that point: While 52% of the organizations had never tried to transfer their data (and 5% weren't sure if any attempt had been made), 31.2% had – indeed – tried to transfer their data and had met with resistance from the vendor.

Of this 31.2%, 4% "never solved the problem," while 5% "solved it by 'persistently badgering the vendor.'" Another 1% retained legal counsel. Some 9% "solved it only by changing vendors and then individually contacting each donor to ask for their credit card or EFT information and then placing them on a new system."

Precautions to Safeguard Data

More recently, in ***Do You Truly Own Your Nonprofit Donor Data?*** (January 2019), the folks at Classy, the innovative online fundraising platform, took up this issue as well. "Your donor **data is the lifeblood of your nonprofit**, fueling your acquisition, retention, and stewardship efforts. So, **who owns it**?"

An organization, of course, owns its data, but a complication arises because the data "**lives inside the different technologies** you use to support your online fundraising efforts, tied to the different tech vendors you partner with." Some vendors "can make it very difficult or flat out refuse, to release your data" or even attempt to claim ownership of it.

"The vendor may make this process **sound impossible**, or like it's the first time they've ever had to do this." But they have, indeed, done it before and **it's done with a "simple query"**: by pressing a single button, up pops your file with all of your data. "Very rarely," according to the Classy people, " would it actually take longer than one or two days to complete."

What's the solution?

First, be aware of and understand this danger. Second, head it off at the pass. Make sure you address these issues "**at the very beginning** of your vendor partnership, in **your contract negotiation**." Then insist that the contract for services spell out clearly that: (1) you own your data; (2); it comes with you in all circumstances including when you switch providers; and (3) the provider will turn over the data in a reasonable time and with no hassles or demands. In particular, make sure that ownership is explicitly spelled out – even in a standalone section of the agreement.

Conclusion

Organizations in the European Union that are subject to the **General Data Protection Regulation (GDRP)** don't have to deal with the specific issue of vendor refusal; the GDRP **requires vendors to transfer data** when the data-owner makes a request. In the United States, at least so far, there is no such protection. While the GDRP applies to many U.S. nonprofits, it's an indirect link only.