GDPR and the Botanical Society of America

The European Union has legislated a new regulation called the General Data Protection Regulation (GDPR) that **will** affect the way the BSA works, but to what extent we haven't yet determined. GDPR is scheduled to be enforceable on May 1 of this year.

What is GDPR?

The GDPR is a regulation intended to protect the privacy of EU citizens and provide data transparency for them. Key provisions:

1. Consent. An EU citizen must consent to their data being processed. This means they need to opt in to pretty much any usage of their data.
2. Many organizations will require the designation of a Data Protection Officer (DPO), someone who is an expert on data privacy and security. The DPO may need to reside in the EU . It is anticipated that many smaller organizations will contract out this responsibility.
3. In some circumstances "pseudonymisation" is required. If data is being analyzed to track behavior, a particular person shouldn't be identifiable.
4. Data breaches. A organizational plan would need to be developed to handle notification of data breaches.
5. Right of access. An EU citizen has the right to see on request what data on them is being processed. Basically, a "portal" application to login and see their data and what's being done with it.
6. The Right to be Forgotten. On request, their data would need to be either deleted or any identifiable reference to them removed. Certain limitations to this, such as financial records can't be deleted without ruining accounting systems.
7. Data portability. An EU citizen has the right to require that their data be migrated to another organization's systems.
8. Data protection by design. Basically, everything has to be VERY secure.

Who does GDPR apply to?

This is the hardest question to get answered. MANY sources say that it applies to anyone who does business with EU citizens living in the EU. However most of those sources have compliance services to sell. I found one source on a law blog, written by lawyers who sounded knowledgeable, that it applies to any organization who *targets* EU citizens **or** "*monitors*" them. "Monitoring" is somewhat ill-defined but seems to indicate anything that tracks their behavior. In other words, if a simple US based ecommerce company simply completed a sale to an EU citizen who happened to find them on the internet and did nothing more with the data, they wouldn't be

liable under the regulation. Apparently, the US has signed certain treaties with the EU that guarantee their authority regarding their own citizens.

What this means is that if the BSA decides to try and avoid being regulated by this law, we cannot *target* EU citizens in any way, nor do anything that would consist of tracking their behavior. I have come up with a list of things we might do that would be problematic. We should probably get the advice of an attorney that knows the law well to confirm this.

- Membership or Journal advertisements geographically, nationally, ethnically or politically targeting EU citizens.
- Solicitation of Journal articles from EU citizens.
- Solicitation of conference participation by EU citizens (authors, special speakers, presiders, etc.)
- The only activities we do that clearly track behaviors is the Botany Conference "custom schedule" and the schedule and gamification in the conference mobile app. We could do these things for EU citizens while they are on US soil, but not when they are physically in the EU.
- We couldn't hold a conference in the EU.
- We couldn't have a booth in someone else's conference in the EU.
- We might not be able to support EU teachers, students and mentors in PlantingScience.
- There are probably other scenarios I haven't thought of yet.

What options do we have?

The penalties for required non-compliance are substantial, €20 million or 4% of annual worldwide revenue, per infringement, whichever is greater. So we should take this seriously. We could take the following approaches:

- Do nothing and hope for the best. The best outcome if we take this option is that many others will do the same, the law will be seen as unreasonable, and there will be a diplomatic solution for non-EU organization (seriously, there are a lot of small US companies that are irate over this regulation. It seems to be designed to regulate small organizations OUT of business). The worst outcome would be very bad indeed.
- Go "full compliance". It will probably be my main project for the rest of the year to deal with all of the security requirements, create a "see my data" portal, make personal data downloadable and portable, create "right to be forgotten" functions for all of our web sites (including past Botany Conferences, PlantingScience, etc.).
- Do what's easy and watch to see how things develop. There will likely be software solutions available soon that help to address the requirements. There is already a CiviCRM extension that implements many of the

requirements such as consent, pseudonymization, and right to be forgotten. There will likely soon be portals that can be used to gather data from various sources for display. There will also likely be more documentation – and court cases – that clarify not only best practices but also what can be done to avoid coming under the regulation at all.

- Be very intentional about not targeting or monitoring EU citizens, at least until the GDPR is better understood, best practices are standardized and software tools for it are updated or created.