GDPR and Botany and Other Supported Conferences

I Awareness

Making sure that decision makers and key people are aware how important this is. Compliance is mandatory if you have clients in the European Union. For Botany 2016 we had 22 attendees from 10 countries, and in 2017 11 from 7 countries. So, we do have to protect their data.

II Information We Hold

The information we hold through the eTouches registration site is basic information; Name address, title, Institution, email, phone, name and phone in case of emergency, which society they are a member of, dietary needs, if they are presenting and what is their area of research interest. This is information WE keep. When they pay for the conference – they can use a credit card through eTouches and a gateway – which processes the card but does not keep the information. The information above is submitted by the attendee and is as accurate as they provide.

Who we share it with?

- We send out a list to exhibitors the month before the meeting of all attendees. List is name, title, institution and email. This is perk for exhibitors and allows them to do pre-conference marketing.
- New this year we will be partnering with a small company that will match poster presenters with attendees with similar research interests. That list will be name, interests and emails.
- Post Botany conference we provide Rob Brandt with a complete list of attendees. Again, names, titles, institution, addresses, emails, as submitted by attendee. He then imports the information into Civi.
- Workshops, field trips, ticketed events lists of attendees are provided to the organizers of those events, (names and emails) so that these attendees can receive pre-meeting materials or contact to prepare for the event. We will need to send lists as password protected documents..and can do this through eTouches. Lists are also printed onsite for check –in by volunteers – need to investigate doing all check in through scanners.

III Privacy Policy

We currently have a privacy policy on the registration site – describing how we use the collected information – This needs to be reviewed to be sure we meet compliance standards. It needs to be in basic, easy to understand language.

IV Individual's Rights

Under the GDPR individuals have the following rights:

- the right to be informed;
- the right of access; We can provide them with the data they have submitted
- the right to rectification; If it is wrong we can fix it – but we only have data they have submitted
- the right to erasure; We will work with eTouches to delete when necessary
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling. We don't do this…(double Check SEB/SoE)

V Subject Access Requests

If someone wants their information – we can't charge them for it. The new law provides a 30- day timetable to comply with the request. We have the right to refuse if request is unfounded or excessive, and if we refuse they have the right to question why.

VI Need a lawful basis for processing Data

We collect data as a way of registering for a conference – that is all.

VII Consent

Consent must be an opt-in option – not a passive option. Opt-in buttons need to be clear, specific, properly documented. Example – SEB/SoE asks if the attendee wants their information shared with other conference attendees…It is now a mandatory question they must answer before going on.

VIII Children

We don't collect information on children – unless they are also attendees – we ask ages for organizing purposes.

IX Data Breaches

The data breach for conferences would rest on the shoulders of eTouches and their ability to deal with them. Need to find out their policy and procedures.

X Data Protection

Privacy by design is now a legal requirement – refers to data collection systems – in our case another place where we rely on eTouches.

XI Data Protection Officers

Someone in the organization should be responsible for data protection. Under the regulations you must have a DPO If:

- You are a public authority (except for courts acting in their judicial capacity);
- an organization that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organization that carries out the largescale processing of special categories of data, such as health records, or information about criminal convictions.

For conferences – we should not need one – and will work with eTouches for data protection issues.

XII International

Applies if your organization operates in more than one EU Member state. Does not apply to us.

Action Items for Conferences

- Strengthen our privacy policies that currently exist on Botany and SEB sites
- Add opt-in buttons for data sharing questions as needed
- Double check with Mail Chimp and Survey Monkey as to their privacy policies – at very least delete the EU members from e-mailings - marketing and surveys. Current plan it to contact EU attendees for the past 3 years and get their permission to send them emails, surveys, etc. Before the end of April. If they don't respond we will remove there data from our lists.

DoubleDutch – Our Conference App

The App is GDPR compliant as of 12/31/17

- Analyzed PII transfer and storage flow, including where PII may have been included in back up and historical data.
- Standardized process to purge/anonymize PII data (Both at Event-level and Individual Attendee)
- Standardized process for purging entire Event data after event end date
- Reviewed data storage and security best practices to ensure our processes aligned
- Verified PII and non-PII are stored separated in our systems
- Updated Mobile App login Privacy Policy and Terms and Conditions

- Verified login screen, privacy policy checkbox will not be auto-checked for user
- Created better audit log of data redaction requests by users
- Created better audit log with timestamps of data purged for individuals and events
- Reviewed process for user to submit data requests
- Mobile App: Added more information to FAQs and Contact Us sections (final text pending) with support contact info (email address)
- Created script to provide report of processed PII to user upon request
- Coordinated data redaction process for any integration systems
- Align Engineering team with GDPR considerations when designing systems in the future

Process for Data Redaction:

- User must contact DD via customer support or email (contact email available in Privacy Policy)
- Ticket is logged, which issues a confirmation email to the user to verify their identity per the email address on file
- Customer is asked to confirm their identity and privacy request. User requests will be for one or more of the following:
    - 1) record of PII collected
    - 2) correction of PII
    - 3) PII deletion
    - 4) how PII is being used
- All GDPR customer requests will be executed within 30 days of receipt
- If the individual requests that their data be purged and that data was also shared with third parties (ex. Exhibitors), then those companies will also be notified of the deletion request.

Process for Event PII removal

To begin (May 25, 2018), event PII data will be purged at 60 days after an event end date (in the future, we will allow organizers to set their own date ranges, up to a max or 18 months)

- One week prior to the purge, an email will be sent to the organizer for the event, letting them know the data will be removed.
- Organizer data (including login credentials) will not be purged to allow them to continue to access the CMS account
- PII will be purged, but not event data - organizers will still be able to duplicate events in CMS, and pull reporting (but with PII redacted).