GDPR
General Data Protection Regulation

May 25, 2018
May 25, 2018
May 25, 2018
Before we get started:

1. Yes, we are recording this webinar and will post the webinar & slides in the Post Resource Center.  [https://www.same.org/Get-Connected/Post-Resource-Center](https://www.same.org/Get-Connected/Post-Resource-Center)

2. To ask a question, please use the chat box and we will respond to all questions at the end.

3. Follow up questions may be sent to [nroch@same.org](mailto:nroch@same.org) or [jmurphy@same.org](mailto:jmurphy@same.org)
General Data Protection Regulation

Provides a new framework for the way Associations (businesses, and any other organizations) collect, process and protect the personal data of people in the European Union.

It’s a matter of time before something similar comes to the U.S.
What’s Considered Personal Data?

Any information that can be used to directly or indirectly identify an individual. This includes but is not limited to:

• Name
• Address
• Email Phone
• Date of Birth*** sensitive information
• Race, religion, health, biometric information, political association, criminal history.
What Countries are in the European Union?

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom*

*Countries in red are where SAME currently has members regardless of Brexit.
Who GDPR Applies to:

- **Customers**: all our members who live/work in the EU
- **Employees**: all SAME staff
- **Third Parties**: Posts, Events, Committees who have EU participants
  - Rhein-Main, Kaiserslautern, Dolomiti Posts AND any OTHER Posts or Field Chapters that have members living/working in the EU
  - European events and workshops AND any other events that have attendees in/from the EU
  - International Committee AND any other committees with members in the EU
  - Exhibitors, Sponsors, or Attendees who get a list of attendees that contains information with members in/from the EU
Rules for GDPR

• **#1 Legitimate Basis for Data**
  
  – Data is used in a transparent, fair, appropriate and permitted way.

  **Example:**

  – **Birthdate**: needed to determine if member is eligible to receive special rate and participate in young-member-only events

  – **Political Affiliation**: no legal or any other basis to collect this
• #2 Data Storage
  – Personal data is kept safe and secure
  – Appropriate data management processes and controls are in place
  – Standard procedures are followed to minimize errors, correct inaccuracies and delete data
  – Data no longer needed has been archived or deleted
• #3 Individuals’ Rights

  – Anyone who you collect data from has the right to:
    • Ask what you’re collecting about them and why
    • Receive a copy of the all data you collect on them
    • Update their data at any time
    • Restrict how and why you use their data and who we share it with (except where it’s business essential- i.e. sending and processing invoices)
    • Have all their data deleted from your database
• #4 Explicit and Clear Consent
SAME must obtain **active, affirmative** consent by any individuals stored in their database in order to use their data for any purposes other than those directly related to their membership.

Consent cannot be obtained through passive acceptance such as pre-ticked boxes or opt-outs.
#4 Explicit and Clear Consent (continued)

**Actions that require consent:**
- Newsletter distribution
- Marketing emails
- Event notifications (both at the Post and National Level)
- Post-level communications and notifications
- Membership surveys and questionnaires

**Actions that do not require consent:**
- Renewal notices
- Individualized communications directly related to membership processing or event registrations (**legitimate purpose**).
#4 Explicit and Clear Consent (continued)

– Consent form link now available in everyone’s Member Dashboard at www.same.org.
– Consent form will be added to applications and event registrations.
– GDPR Information is only editable by the user.
– All reports, including Committee and Post rosters and event attendee lists must include Consent data.
#4 Explicit and Clear Consent SAME Actions (continued)

- Consent request email sent to all members, non-members, and event attendees in Europe, April 25, May 2, and May 9.
- Consent request letters will be sent on May 9.
- Consent request phone calls MAY be made before May 25 deadline
- No response = no consent
- ALL lists, rosters, reports will be refreshed with consent data on May 25.
• #5 Children’s Data
  – “Child” is defined as anyone under 16
  – Children cannot be sent any information or contacted without explicit consent from Parent or Guardian
  – Children at SAME are Camp Applicants (14-15 year olds)
  – Camp Application forms will be modified to include Consent and Privacy Statement
• #6 Privacy Notices
  – Must be transparent and easily accessible
  – Must explain what information we have, what we do with it and who we share it with
  – SAME Privacy Act statement is available:

  https://www.same.org/Discover-SAME/SAME-Privacy-Policy
• #7 Data Breaches
  – Data breaches must be reported to both users and data protection authorities within 72 hours of the breach
  – SAME does NOT store any credit card or other financial information in CV
  – Only SAME Staff can access records in the database
  – CLAS is under modification to enact tighter controls on Post Roster distributions
• #8 - #9 - #10

These three items are more theoretical in nature and SAME needs to be aware of them but they currently do not require direct action.

#8 – Privacy by Design – new systems must incorporate privacy and protection mechanisms

#9 – Privacy Impact Assessment – new projects, campaigns or products must be reviewed to determine the impact and possible risks to privacy.

#10 – Data Protection Officer – required for

  (a) public authorities
  (b) organizations that engage in large scale systematic monitoring, or
  (c) organizations that engage in large scale processing of sensitive personal data (Art. 37)
• #11 Third Party Management
  – Vendors who manage our membership database and event registrations
  – Councils and Committees
  – Posts
  – Anyone we give our mailing lists

SAME bears the responsibility to prove that third parties are properly following the guidelines and regulations regarding the acquisition and management of personal data. SAME must have confidence that the third-party services used to manage data are properly secured. If our third-party provider causes a breach, SAME will remain liable.
• #12 Awareness
  – Staff Training
  – Monitoring of data in database
  – Post Officer training
  – Council and Committee Chair training
What is **NOT** allowed under GDPR

- Using pre-ticked or opt-out forms for Consent data
- Not having the proper processes and systems to store Consent data
- Sharing lists freely with venues, speakers, members, attendees
- Not paying attention to the data that non-SAME staff have access to
- Emailing unsecure spreadsheets or posting public lists
- Leaving printed registration lists on-site at events
- Letting non-SAME staff have access to data at events
What does this mean?
Committees & Councils

• Committee & Council emails will only be sent by SAME staff.
• Chairs will send their announcements, newsletters and event information to the SAME Staff POC for distribution to committee/council members
• Any existing lists on personal computers, storage devices, Google Drive, Dropbox etc. are to be deleted
• Any use of an Email Service Provider (ESP) such as MailChimp, Constant Contact, Event Brite etc. will cease
What does this mean?

Posts

• Post rosters from CLAS will only include the names of any EU residents who have NOT opted-in.
• Posts will be required to pull a new roster any time they send an email communication to their members.
• Any existing lists on personal computers, Google Drive, Dropbox etc. are to be deleted.
Conclusion

• “I didn’t know” is not a defense.
• Penalties for non-compliance are severe
  (€20,000,000 severe!)

QUESTIONS?

Follow up: nroch@same.org or jmurphy@same.org