New Data Safeguards for APCO 2018

Why is APCO asking me to opt-in before providing any personal information?

As part of our ongoing effort to ensure the security of our members' personal data, and of the APCO networks and systems that support our members, APCO will be adding some additional requirements to the registration process for APCO 2018.

The European Union General Data Protection Regulation (GDPR)

As many of you may already know, the GDPR will be implemented on 25 May 2018. GDPR applies to any organization, whether or not it is based in the EU that collects, retains or processes the personal data of EU individuals. One key requirement for organizations is to ensure that personal data held is secure and to prevent data breaches through encryption measures. APCO wants to ensure not only compliance with the GDPR but even more importantly the security of your data as APCO members and supporters.

APCO's approach

The vast majority of organizations will be affected by GDPR. Organizations have two choices with regard to compliance. Either they can take measures to comply or they can decide to take the risk that a breach will not occur. APCO has decided that in the best interests of our members, and the Association, we will take proactive steps to comply with GDPR requirements, and that we will use this opportunity to increase our cybersecurity posture as well.

To this end, APCO has either already implemented, or will soon implement, the following:

- APCO has initiated an inventory of all hardware and software assets in order to ensure the visibility and security of those assets.
- APCO has reached out to all vendors who support our Association by collecting, processing, or maintaining data for us. We have requested their current cybersecurity and GDPR compliance status and have created a tracking sheet and compliance report based on this data.
- APCO will require proactive "opt-in" prior to collecting any personal information starting with registration for APCO 2018. The process will be applied to all events, and other data collection evolutions, moving forward.
- APCO is currently working on a plan that includes a requirement to track and account for all of the Association's data. This report will also include cybersecurity requirements and recommendations.
- As part of the overall technology, security, and compliance plan APCO will implement a data retention policy for events and a separate data retention policy for financial data.

APCO believes that taking these steps is important as part of our overall strategy to protect the Association and its members. As public safety communications professionals, and organizations who support the public safety mission worldwide, APCO knows that our members understand the importance of such measures. APCO thanks you for your continued support and understanding as we implement this new level of protection.