Policy on Protection of Personal Information

From our perspective, and from the perspective of most of our clients, the mission of The Conference Exchange is to collect and disseminate information about the identities, activities, discoveries, opinions, plans, and policies of conference participants. A small fraction of that information is considered sensitive by the individuals or organizations involved, or by the governments or standard-setting organizations that rule them. For example:

- Hackers should never to be able to lift individuals' social security numbers from our systems.
- We should not make it easy for mailing list vendors to harvest the email addresses of presenting authors, attendees, etc. from our site.
- Whenever we handle credit card payments we must be PCI compliant.
- The EU's General Data Protection Regulation (GDPR), which goes into effect in May of 2018, requires us to protect the privacy of EU customers. Since the majority of the conferences we support do attract speakers and attendees from Europe, and since we don't want to have to enforce geographically-specific policies, we will protect the privacy of all individuals in our system in the same way regardless of their geographic or national origin.
- GDPR gives citizens of EU countries the right to access their personal data, the right to rectify incomplete or inaccurate data, the right to be forgotten, and the right to restrict the processing of their data. Confex will provide those protections to all users.

Confex policies regarding security of sensitive data aim to be at least as stringent as our clients' own principles. Our obligations to protect personal information must be balanced against our contractual responsibility to provide a user-friendly data-entry experience and to ensure the accuracy of the information we collect.

Standard Data Security Policies

We never store complete credit card numbers or security codes anywhere in our system. We comply in all ways with PCI standards and our systems are regularly monitored by an independent expert to ensure that we remain in compliance.

As a general rule, we will not store social security numbers, W-9 forms, and similarly sensitive personal data in our system. In rare situations where there is no other way for our client to meet their accounting obligations, and only when personally approved by our company president, Confex will store a limited quantity of sensitive data. This data will be encrypted at rest, using highly secure encryption algorithms. The private key to the encrypted data will be very tightly controlled and will not be stored in our code.

In the absence of client directions to the contrary, these standard policies apply to the protection of email addresses and other personal information:

- Starting in 2018, with rare exceptions, we will not display email addresses in conference programs published online. The major exception to this rule is the display of email contact information for exhibitors.
- Conference programs published prior to 2018, being part of the historic record of our client and likely available from many sources, will continue to display email addresses. However, we will pull email

addresses or other information from old programs when the owner of that information specifically asks us to remove it.

- When a regular user searches for someone by name or email address, e.g. to add someone as a co-author on an abstract, any email address shown in the search results will be masked. For example, instead of showing Kevin O'Neill's full email address along with his name, we will show "O'Neill, Kevin, k*****@confex.com". We will always show five asterisks in the masked email address, regardless of the actual length of the username in the email address. So, kevin@confex.com and koneill@confex.com and ko@confex.com and k@confex.com will all be rendered in the search results as k*****@confex.com. *NOTE: Confex staff, and client staff who have logged in as such, will still see unmasked email addresses.*
- If a regular user is only allowed to search for someone by email address, we will not show any email address in the search results -- not even a masked email address.
- When a regular user searches for someone by name or email address we will show institutional affiliation (when we have it) in addition to a masked email address in the search results. The objective of showing the masked email address and affiliation is to help a user select the right person from a list of similar names in the search results. We know that it is rare to encounter multiple people with the same name at the same institution. It is more common to encounter multiple people with the same masked email address.
- We may still show the person's full, unmasked email address on the form offered for editing personal information. We might not even show the unmasked email address there if:
    - all modifications of name and email address are to occur in our client's association management system, OR
    - the email address has been specially validated and extra protection has been requested.
- If a meeting participant (author, session organizer, etc.) asks us to remove them from the publicly accessible record of an old meeting, i.e. from webprogram or meetingapp, we will first obtain permission from our client to do so. If our client grants permission, we will remove that person from the appropriate page(s). Otherwise, we will refer that person directly to our client.
- Whenever possible, we tend to avoid collecting information from people about their health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, criminal history, etc. If an exception arises, we will:
    - ascertain whether collecting this information in the abstract system is truly necessary
    - ensure that access to this information is password-protected
    - never display this information publicly (unless it is intended to be revealed in an abstract or a bio, and the person providing that information is explicitly made aware that it is intended for display in the online program or app)

Any exception to these standard policies must be approved in advance by the president or a vice-president of Confex. Unless otherwise noted, references to the "display" of data refer to both the normal view of web pages and to the source code or publicly accessible API feeds.