Society for Pediatric Interventional Radiology

This **Privacy Notice** sets out how The Society for Pediatric Interventional Radiology (SPIR) uses your personal data:

- SPIR may collect your data in a variety of ways, including through your registration process, correspondence, membership renewal and annual meeting registration
- We store your application documents, such as your CV, in secure systems online including the Wild Apricot platform and Dropbox (see below)
- We will use your personal data to contact you with general SPIR communications and for communications and record-keeping specific to you, such as membership renewals.

We process your personal data in keeping with Article 6 (1) and Article 9 (2) of the General Data Protection Regulations (GDPR).

Your rights under applicable data protection law are as follows (noting that these rights do not apply in all circumstances):

- The right to be informed about processing of your personal data
- The right to have your personal data corrected if it is inaccurate and to have incomplete personal data completed
- The right to object to processing of your personal data
- The right to restrict processing of your personal data
- The right to have your personal data erased (the 'right to be forgotten')
- The right to request access to your personal data and information about how we process it

You may exercise these rights by contacting us at spir.secretary@gmail.com

Wild Apricot Security: To ensure security and privacy of your data, Wild Apricot provides traffic encryption (https) capability. Traffic encryption ensures that data entered into the online forms (e.g. membership application, event registration) as well as data transferred from Wild Apricot servers back to users is protected from snooping, for example if you access internet over an insecure WiFi connection.

Wild Apricot's hosting provider is Amazon Web Services (AWS). AWS is a secure, durable technology platform with industry-recognized certifications and audits: PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and/or SSAE 16), SOC 2 and SOC 3 audit reports.

The AWS infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure AWS data centers.

AWS storage solutions deliver highly scalable, durable, and reliable cloud storage with robust data protection.

Currently, the main Wild Apricot solution is distributed over one AWS Region with at least three Availability Zones (data centres). All backups are delivered to separate regions. Wild Apricot uses a set of high reliable services/solutions provided by AWS.

Updates on Wild Apricot's security can be found on their website.

Dropbox Security: Dropbox have a team dedicated to keeping your information secure and testing for vulnerabilities. Security features to protect how they store, process and transmit data include two-factor authentication, encryption of files at rest, and alerts when new devices and apps are linked to the account.

When transferring data from the European Union, the European Economic Area and Switzerland, Dropbox relies on a variety of legal mechanisms, including contracts with our customers and affiliates. Dropbox complies with the EU-US and Swiss-US Privacy Shield Frameworks as set forth by the US Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union, the European Economic Area and Switzerland to the United States. Dropbox is overseen by the US Federal Trade Commission.

Updates on DropBox's security can be found on their website.

If you have any queries about how your data is protected, please contact spir.secretary@gmail.com

Created 8/7/2018