I was asked to consider the legal issues involved in the proposed AUSKF website and its immediate implementation by a member of the AUSKF Board of Directors. While I am a lawyer in Texas, I have only analyzed this issue in brief. There are many other state and local laws being developed and implemented on almost a daily basis that could impact this decision. Also, this is not a complete picture of the potential legal problems and issues involved. I am simply highlighting a few of the major issues. I am not counsel for the AUSKF or any other party involved. I was asked to do this personally because of my concern for Kendo and the national federation. Under the present state of the law, if I were to offer a legal opinion to anyone on this issue, I would strongly argue against implementing the website until a competent legal team has reviewed all of these issues and the board of directors have acted on that team's recommendations and national policies and procedures have been written and enacted. For the record, I am not the type of lawyer that cries wolf, I was first a businessman who hired and fired lawyers. The issues I have presented are very real considerations and should not be dismissed.

Set forth herein are several serious legal issues that need to be considered and dealt with prior to the AUSKF going on line with the proposed website registration system. To date, I have not seen anything addressing any of these issues. Further, as I stated the law in this area continues to develop at a very rapid rate with changes being instituted on a state by state basis almost monthly.

Among the major legal considerations is compliance with the cyber security/data protection laws of all fifty states as well as general internal organizational steps designed to limit potential data breaches, limit liability and damages in the event of a breach.

State by state compliance.

The AUSKF website will be electronically available to members and potential members in all 50 states, therefore, the website must adhere to each states legal requirements for data storage and access. The national standards set forth in U.S. law are merely starting points and compliance with these laws does not ensure conformance with the various state laws covering the retention and distribution of Personal Identification Information (known in the industry as "PII"). PII includes but is not limited to: names, addresses, dates of birth date, social security numbers, health information and any financial information including credit card numbers. It is important to note that paying something such as AUSKF dues via an online transaction whereby the website has for even a limited time an individuals credit card number is considered sufficient retention to be covered by certain state and federal statutes.

By way of examples, US privacy laws generally do not limit the retention of PII to certain specified grounds. There are, however, laws that may indirectly affect an organization's ability to retain PII. For example, organizations that are collecting personal information online from California residents must comply with the California Online Privacy Protection Act. Pursuant to this law, and general consumer expectations in the US, the organization must provide a privacy notice detailing the PII the company collects and how it is used. If the organization uses the PII in materially different ways than those set forth in the privacy notice without providing notice and obtaining consent for such uses from the relevant consumers, these uses would likely be considered a deceptive trade practice under federal and state unfair competition laws.

Therefore to be in compliance with California law the AUSKF must have a written and published privacy notice on the website that has been vetted and approved by the AUSKF Board of Directors/officers.

Further, California's Online Privacy Protection Act requires organizations to specify in the notice: 1) the categories of PII collected through the website; 2) the categories of third-party persons or entities with whom the operator may share the PII; 3) the process an individual must follow to review and request changes to any of his or her PII collected online, to the extent such a process exists; 4) the process by which consumers who visit the website or online service are notified of material changes to the privacy notice for that website; and 5) the privacy notice's effective date.

To my knowledge none of California's state requirements have been addressed.

In addition to this California law, other federal and state laws require a privacy notice to be provided in certain circumstances. Has any vendor been engaged to ensure compliance, has the Board taken those steps necessary to undertake a through comprehensive review of the training and implementation process?

Further from a liability and negligence viewpoint, I do not believe the AUSKF has adopted appropriate security policies and procedures, including written policies as necessary to create a culture of security, a plan to enforce its security procedures, or has created appropriate incident response and business continuity data recovery/breach plans. I do not believe the AUSKF has ever tested its response plan or created program to manage compliance with applicable federal and state, laws on an ongoing basis.

For example, what are the written procedures for issuing administrative passwords, what are the criteria for revoking password access, what officer(s) has been empowered to make these decisions and what written policy, adopted by the Board of Directors does this officer need to operate under?

California's Privacy Act is rather generic and allows the user, such as the AUSKF, design its own safe guards and policies to meet the laws requirements. However, unlike the California law, a Massachusetts cyber security law contains certain specific data security standards, including required technical safeguards, on all private entities with Massachusetts consumers or employees. Any AUSKF member from Massachusetts would be covered by this law. Has this been reviewed and addressed from the technical, policy and legal view points?

Nevada law requires that organizations doing business in Nevada and that accept payment cards must comply with the Payment Card Industry Data Security Standard. It requires that other organizations doing business in Nevada use encryption when transferring any personal information through an electronic, non-voice transmission other than a facsimile to a person outside of the secure system of the data collector, and moving any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor.

This statute has been interpreted by Nevada state and federal courts to mean that data shared going into or out of Nevada must be encrypted. This would cover the PII of any AUSKF member such that if someone in Nevada is given an administrative access code whereby they can look at any member's information in another federation (as in to confirm AUSKF membership for participation in a seminar or Taikai) the the data must be encrypted. Based on this law, most national websites now have all of their data encrypted or are moving to have it encrypted. Has the AUSKF undertaken the steps necessary to encrypt the data such as engaging a vendor to provide this service, maintain the process and ensure compliance?

To give those reading this short memo an understanding of the extent of the monetary liability issues involved. Recently suit was brought against a California based entity that lost, due to a data breach, the names, addresses and birth dates of six adult (6) individuals. This case was settled for $100,000. If minors had been involved the cost would probably have been double.

Fortunately the entity involved had a cyber/data breach insurance policy in place. Has the AUSKF such an insurance policy. I know the answer has to be, no. Without the written privacy policy and other administrative rules having been considered adopted and implemented as discussed above, obtaining such a policy would be impossible, no insurance company would issue it.

Until these significant issues are addressed, until the proper policies and procedures are in place, the use of the proposed website, regardless of the technical issues involved, is a major risk and not one the board should approve. I would caution that it could be considered a breach of the fiduciary duty the directors owe to AUSKF and would most certainly be considered negligent conduct by a court in the event of a breach and data loss.

There are other significant issues, such as those involving who has access to child PII, that I have not addressed but that need to be throughly vetted. For example, will all administrators be vetted to ensure that no one who has access to child PII is a registered sex offender? Regardless of how unlikely this may be, if the AUSKF does not have a policy in place to address this issue, even if its only access to the data, liability could be incurred.

The website may be a great idea designed to save lots of time and effort, as to that I have no comment, however those in charge of approving this project must recognize that as a national organization it must ensure it plays by rules set for it by others in this area.

Mark A. Kerstein
THE LAW OFFICE OF MARK A. KERSTEIN
9801 Wsteheimer, Suite 302
Houston, Texas 77042
(713) 917-6890
kersteinlaw@gmail.com