KCBA KING COUNTY BAR ASSOCIATION

Justice... Professionalism... Service... Since 1886

1.0 Law & Legal CLE Credit – A/V Approval #1065370

Recording Date – January 4, 2018
Recording Availability – March 6, 2018

Meeting Location	Date	Time	Topic
King County Bar Association 1200 Fifth Avenue - Suite 700 Seattle, WA	**Thursday, January 4, 2018**	12:00 PM to 1:15 PM	Overview of New EU GDPR: Privacy by Design

AGENDA

12:00 PM Introduction

12:10 PM Presentation: 'Overview of New EU GDPR: Privacy by Design', by Barb Rhoads-Weaver, Focal Law PLLC

- Overview of 1995 EU Directive regarding Data Protection
- Overview of US Safe Harbor and Privacy Shield regarding EU data subjects
- A look-forward to EU General Data Protection Regulation (GDPR), implementation on May 25, 2018

1:15 PM Adjourn

SPEAKER BIOGRAPHY

Barb Rhoads-Weaver, Focal Law PLLC - Barb is an attorney with Focal Law PLLC in Seattle Washington. She represents businesses, non-profits and individuals with a wide range of transactional and civil litigation matters.

In state and federal courts, Barb has successfully represented clients through trial and on appeal. Early on in her legal career, Barb clerked for The Honorable Tom Chambers of the Washington State Supreme Court. Before joining Focal, she worked as an associate at a mid-sized law firm in Seattle. With this experience under her belt, she had the pleasure of starting and running her own general practice firm on Vashon Island.

She has served as a Governor on the Washington State Bar Association Board of Governors and as an officer and director of QLaw. Barb is a volunteer attorney with the King County Bar Association's

Vashon-Maury Neighborhood Legal Clinic. Early efforts to secure marriage equality inspired Barb to attend law school, and she was fortunate to spend a summer during law school as an Equal Justice Works fellow clerking at the National Center for Lesbian Rights.

She graduated *Summa Cum Laude* in 2003 from Seattle University School of Law. Before she began her law career, Barb worked as a research assistant at Chesapeake Biological Laboratory where she spent most of each year on a research vessel. She is barred in Washington State and Federal Courts, the U.S. Supreme Court, and Puyallup Tribal Court.

HOW DO I EARN CREDIT FOR SELF-STUDY OR AUDIO/VISUAL (A/V) COURSES?

For pre-recorded A/V (self-study) programs, although the sponsor should apply for accreditation, **lawyers need to report the credits earned for taking the course.**

To add an approved course to your roster, follow the procedures below:

- Go to the "mywsba" website at www.mywsba.org/.
- Log in.
- Click on the "Access MCLE" link in the "MCLE Info" box on your home profile page.
- Click on "Add Activity." Search to find the approved course in our system. (See search suggestions on the screen.)

Adding a Recorded Course

Select Recorded Course from the Add New Activity screen.

This will prompt you to search for the activity in case the activity has already been accredited in the MCLE system.

You can search by Activity ID or by specific Activity Details. For the Activity Details search, you can use keywords for the title, sponsor name and date.

After entering your search criteria and selecting Search at the bottom of the screen, a list of possible activities will be provided.

You can select the correct one by clicking the Activity ID. This will take you to the specific activity. Entered the date(s) on which you began and ending viewing this recorded activity.

Then claim the correct credits for which you attended this activity in the Credits Claimed fields and click the Submit button at the bottom of the page.

You will receive a confirmation message at the top of your screen stating, “The activity has been added to your roster.

Overview of EU GDPR: Privacy by Design

focal PLLC

The European Union
General Data Protection Regulation (GDPR)
(Regulation (EU) 2016/679)
Enforcement Begins May 25, 2018

Presented to King County Bar Association
Noontime CLE January 4, 2018

By Barb Rhoads-Weaver

focal PLLC

The 1995 EU Data Protection Directive

- Directive 95/46/EC focus is on processing and transferring “personal data”

- Personal Data
  - Similar to personally identifiable information (PII)
  - Defined as “any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his physical, physical, physiological, mental, economic, cultural or social identity.”

- Processing
  - EU Member States required to protect data subject rights, especially to privacy, with respect to processing of Personal Data.

- Transferring
  - EU Member States can't restrict or prohibit free flow of personal data in the European Economic Area (28 EU members plus Iceland, Liechtenstein and Norway)
  - Need adequate protection of data subject rights, especially to privacy, to transfer outside EEA
  - Standard Contractual Clauses (SCC), Binding Corporate Rules, and Safe Harbor (initially) are mechanisms deemed to provide adequate protection

EU-US Safe Harbor Framework

- US Department of Commerce program
  - Businesses self-certify
  - Intended as a mechanism to comply with the Directive to provide adequate protection when transferring Personal Data from EU to the US

- European Court of Justice declared Safe Harbor invalid (10/6/2015)
  - 2013 following Snowden and other revelations of US surveillance programs, German DPAs issue concern and EU Commission makes recommendations
  - 2015 German DPAs pass resolution that Safe Harbor self-certification does not provide sufficient safeguards and adequate protection for transfers of Personal Data from EU to US
  - Max Schrems (Austrian Facebook user) case regarding NSA program.

EU-US Privacy Shield

- February 2016 new agreement reached called Privacy Shield
- Requires annual reviews (first annual review working but needs improvement)
- EU can suspend program at any time if finds inadequate protection
- Can self-assess and verify or hire third party, but still self-certify compliance
- Challenges to the adequacy of Privacy Shield and SCCs are working their way through the EU courts.

- Framework is based on 7 Principles and 16 Supplemental Principles

1. Notice (generally an online privacy policy with required links)
2. Choice (opt out and mechanism to exercise)
3. Accountability for Onward Transfer (contracts)
4. Security (reasonable & appropriate given risks and nature of personal data)
5. Data Integrity and Purpose Limitation (reliable & accurate for purpose)
6. Access (correct or delete inaccurate info or when violation of Principles)
7. Recourse, Enforcement and Liability (independent mechanism free for individuals or subject to DPAs)

GDPR

- Effective May 25 2018 – replaces the 1995 EU Data Protection Directive
- Regulation vs Directive
- Jurisdiction expanded if offer goods or services, or monitor behavior
- Penalties expanded
  - Up to €20 million or 4 percent gross annual global revenue, whichever is greater
  - 2 percent for not having required records in order
  - Max Schrems NOYB (Article 80 Representation)
  - Processors subject to penalties for breach and non-compliance as well as Controllers

- Privacy by Design – not added on, but included in design from beginning
- Data Protection Officer – appoint independent DPO for large scale systemic monitoring or special categories of data
- Audits, impact assessments, record keeping
- Consent in plain language and easy to withdraw
  - Clear affirmative action or statement
  - Opt-out or implicit (silent, pre-ticked boxes, inactivity) is inadequate
- Data Subject rights expanded

- Right to Access
  - Free copy of data in electronic format
  - What data processed, where and for what purpose

- Right to be Forgotten
  - Data erasure
  - To stop processing or limit processing

- Data Portability
  - Commonly used machine readable format
  - Right to transfer to another controller

- Breach Notification
  - Mandatory within 3 days to supervisory authority
  - Breach of security leading to accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data
  - To data subject if “high risk” to rights and freedoms of data subjects

- Sensitive Data
  - Definition expanded to include genetic, biometric, and sexual orientation data

- Parental Consent
  - 16 years old, but member states can set lower to 13 years old

Questions?