The Standards must be read in conjunction with the Rules Governing the State Bar of California Program for Certifying Legal Specialists, which govern the Program requirements.

THE STANDARDS FOR CERTIFICATION AND RECERTIFICATION IN PRIVACY LAW
(last revised effective [INSERT DATE])

1.0 DEFINITION

Privacy law is the practice of law dealing with: safeguarding an individual's personal information and data against unauthorized access, disclosure, or misuse; addressing the legal rights and responsibilities concerning data privacy, including compliance with applicable regulations and industry standards; advising clients on matters related to data collection, processing, and sharing practices; developing policies and frameworks for data protection; and representing clients in disputes or regulatory actions involving privacy violations or breaches. It encompasses areas such as consumer privacy, financial privacy, health information confidentiality, employee data rights, and emerging technology and digital privacy challenges.

2.0 TASK REQUIREMENT FOR CERTIFICATION

An applicant must demonstrate that, within the five years immediately preceding submission of the written application, he or she has been substantially involved in the practice of privacy law. A prima facie showing of substantial involvement in the practice of privacy law is made by the performance of the following tasks within the five-year period so as to accumulate 100 points. With respect to each task, the applicant must have performed the task personally, or had direct and primary responsibility for its performance under his or her close and ongoing supervision. For purposes of this showing, points may be accumulated from any of the tasks, subject to the maximums specified per task. However, each task may only be counted once

2.1 Provided substantive written legal advice or analysis regarding regulatory compliance with privacy laws. 5 points per matter. Maximum number of points in this category: 35

2.2 Reviewed, drafted or negotiated data privacy terms in contracts, including outsourcing/service provider agreements or other third party contracts. 5 points per matter or transaction. Maximum number of points in this category: 35

2.3 Provided substantive written legal advice or analysis regarding data sharing requests or counseling on cross-border data transfers and advised on privacy-related risks. 5 points per matter or transaction. Maximum number of points in this category: 35

2.4 Conducted data privacy due diligence involved in corporate transactions, including mergers and acquisitions, reorganization, bankruptcy, receivership, sale of assets, or transition of service to another provider. 5 points per matter or transaction. Maximum number of points in this category: 35

2.5 Advised on policies, procedures, or processes relating to physical, technical, and administrative privacy and information security controls. 5 points per policy, procedure or process. Maximum number of points in this category: 35

2.6 Represented a party in litigation as its principal attorney on privacy issues where matters of privacy law are among the main contested issues. 5 points per separate litigation matter; 10 points per litigation matter if at least 500 hours are billed by the attorney on the case on privacy issues; or 15 points per litigation matter if at least 750 hours are billed by the attorney on the case on privacy issues. Maximum number of points in this category: 65

2.7 Represented a party in a government investigation as its principal attorney where matters of privacy law are among the main contested issues. 5 points per investigations matter; 10 points per investigations matter if at least 500 hours are billed by the attorney on the case on privacy issues; or 15 points per investigations matter if at least 750 hours are billed by the attorney on the case on privacy issues. Maximum number of points in this category: 65

2.8 Acted as the principal attorney in devising and implementing the litigation strategy in connection with pending or threatened litigation where matters of privacy law are expected to be among the main contested issues. 5 points per litigation matter. Maximum number of points in this category: 35

2.9 Acted as the principal attorney in devising and implementing a formal compliance program for a client following the entry of a court order, consent order, settlement, or other binding order or award against the client in any litigation or investigations matter where matters of privacy laws are among the main issues. 5 points per litigation or investigations matter. Maximum number of points in this category: 35

2.10 Provided substantive written legal advice or analysis to conduct a data inventory or records of processing activities. 5 points per matter. Maximum number of points in this category: 35

2.11 Provided substantive written legal advice or analysis to develop or implement external-facing privacy notices, statements or reports as required by privacy laws. 5 points per matter. Maximum number of points in this category: 35

2.12 Provided substantive written legal advice or analysis on privacy issues for marketing, product, feature, or service delivery, such as implementing privacy by design or conducting privacy impact assessments. 5 points per matter. Maximum number of points in this category: 35

2.13 Provided substantive written legal advice or analysis regarding data subject or consumer rights matters (e.g., access, deletion, opt-ins/opt-outs). 5 points per matter. Maximum number of points in this category: 35

2.14 Led or participated in incident response or data breach investigations, including forensic analysis, root cause analysis, and remediation efforts, drafting and reviewing incident reports and communications to stakeholders. 5 points per matter. Maximum number of points in this category: 35

2.15 Assisted with breach notifications to regulators or affected individuals. 5 points per matter. Maximum number of points in this category: 35

3.0 EDUCATIONAL REQUIREMENT FOR CERTIFICATION

An applicant must show that, within the three years immediately preceding the application for certification, he or she has completed not less than 45 hours of educational activities specifically approved for privacy law.

4.0 ALTERNATIVE TO WRITTEN EXAM REQUIREMENT

As an alternative equivalent to the requirement of passing a written examination, an applicant may demonstrate the requisite knowledge of privacy law by fulfilling the following requirements within five years immediately preceding submission of the application for certification:

4.1 150% of the minimum practice requirement as set forth in section 2.0 (i.e., 150 points);

4.2 Supply evidence of at least 60 hours of continuing legal education or professional education from the topics in the Privacy Law Specialist exam specifications within the five years preceding the end of the two-year alternative exam period; and

4.3 Provide at least five peer references from attorneys, clients, or judges attesting to his or her privacy law qualifications.

5.0 TASK REQUIREMENT FOR RECERTIFICATION

An applicant for recertification must show that, during the current five-year certification period, he or she has had direct and substantial participation in the practice of privacy law. Such showing shall be made by compliance with the requirements set forth in section 2.0 or, at the discretion of the Commission, by sworn statement that the applicant has engaged in the practice of privacy law substantially to the same extent as described in the application for original certification.

6.0 EDUCATIONAL REQUIREMENT FOR RECERTIFICATION

An applicant for recertification must show that, during their current MCLE compliance reporting period, he or she has completed not less than 36 hours of educational activities specifically approved for privacy law.