SINGAPORE
ACADEMY
OF LAW

Specialist Accreditation Scheme

Data and Digital Economy Law 2022

Recommendations from the Specialist Accreditation Scheme, Subcommittee on the specialist accreditation framework for Data and Digital Economy lawyers and inhouse counsel

Blank

Table of Contents

1. Executive summary

1.1. This paper sets out proposals for the implementation of a specialist accreditation scheme for Singapore lawyers and inhouse counsel ("legal practitioners") practising in the field of Data and Digital Economy ("D2E") in Singapore (the "D2E scheme").

1.2. While Telecommunications, Media and Technology ("TMT") is an established practice area that involves D2E competence, there is a growing recognition that the field of D2E warrants its own identity as a complex adaptive system for which unique legal industry competencies are needed. A key feature of this complexity is the way in which legal D2E issues can present across a range of traditional legal practice areas (e.g. insolvency, M&A and IP matters).

1.3. For this reason D2E resists framing as a subset of TMT practice or as a standalone practice area and is no longer exclusively the domain of the law firm lawyer. Instead, it may be more effectively articulated as a set of competencies required by professionals who are required to problem-solve D2E issues across a range of contexts. While the focus of the recommendations in this paper is legal practitioners, it is important to acknowledge that allied legal roles, such as legal knowledge engineers, are an emergent and important element of this space that may warrant the attention of a similar scheme in the future.

1.4. The recommendations of the D2E subcommittee,[1] set up under the Specialist Accreditation Board and chaired by Rajesh Sreenivasan of Rajah & Tann Singapore LLP and co-chaired by Joey Pang of DBS are geared towards:

a. recognising high levels of proficiency of legal practitioners in the D2E field by accrediting senior legal practitioners exhibiting D2E competence as D2E Senior Accredited Specialists;

b. incentivising younger legal practitioners to hone their skills and knowledge, and specialise in the D2E field by recognising their developing D2E competence as D2E Accredited Specialists, thus building a pool of talent to serve this dynamic industry;

c. providing consumers of legal services and legal industry stakeholders with a reliable means of identifying and accessing legal practitioners who have proven expertise in the D2E field by enabling accredited D2E specialists to use post-nominals referencing their accredited specialist status; and

d. promoting continued professional development and thought leadership of D2E capabilities amongst legal practitioners to maintain high standards of legal services in the D2E field.

2. What is the digital economy and the role of data in it?[2]

2.1 The "digital economy", the fourth industrial revolution, is a broad notion that defies clear and defined boundaries. Some useful frames of reference are provided by leading scholars and consulting firms studying the field which are set out below.

2.2 Don Tapscott, who has been credited with coining the term "digital economy", described it broadly as a new economy in which "information in all its forms becomes digital – reduced to bits stored in computers and racing at the speed of light across networks".[3]

2.3 Thomas Mesenbourg, in striving to develop a structured accounting framework for the digital economy, proposed that it be defined by three principal components: (a) e-business infrastructure (covering the hardware, software, information and human capital for information communication and computation technology ("ICCT") services, (b) e-business processes (processes business organisations conduct over computer-mediated networks), and (c) e-commerce transactions (the value of goods and services transacted over computer-mediated networks).[4]

2.4 The global management consulting firm, A.T. Kearney, applies a value-chain perspective, breaking down the internet ecosystem into five clusters: (a) content rights; (b) online services and search engines; (c) enabling technologies and services like web-hosting, billing and

[1] See Appendix D for members of the D2E subcommittee.

[2] Josh Lee Kok Thong, Chairperson, Asia Pacific Legal Innovation and Technology Association, private communication, 21 July 2020.

[3] Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (McGraw-Hill Education 1996), p. 6.

[4] Thomas L. Mesenbourg, "Measuring the digital economy", presentation at The Netcentric Economy Symposium, University of Maryland, 30 March 2001 <https://www.census.gov/content/dam/Census/library/working-papers/2001/econ/digitalecon.pdf> (accessed 10 December 2020).

payment and e-retail management; (d) connectivity infrastructure; and (e) web user interfaces and applications.[5]

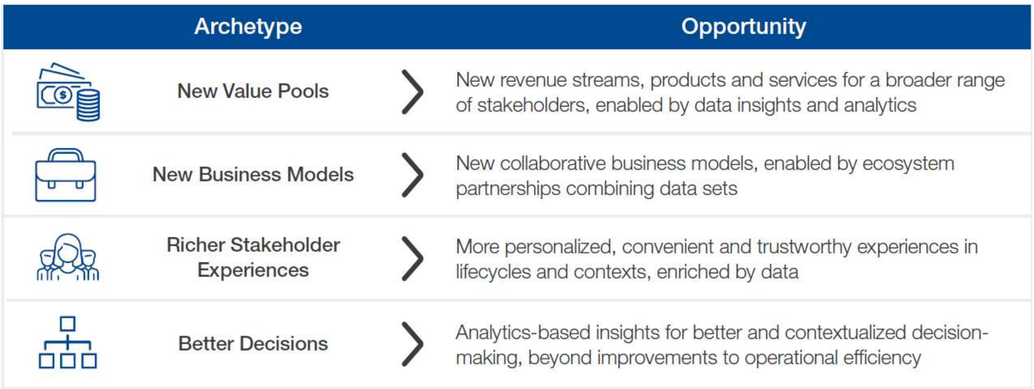
2.5 The lifeblood of the digital economy is, arguably, data. One estimate puts the amount of data created in 2021 at 79 zettabytes[6] with this figure set to rise to 180 zettabytes by 2025,[7] fuelled by more people coming online for the first time[8] and the proliferation of the Internet of Things ("IoT").

2.6 Data generally and the ability to collect, analyse and monetise massive amounts of it specifically has seen the evolution of the data value chain, comprising businesses that support data processing activities. These activities span from collection, production of insights from data, data storage, to analysis and modelling. These businesses employ data-driven business models and harness digital platforms to record and extract data derived from online activity and interaction of their users.[9]

2.7 More importantly, such businesses have used the advantages of data and digital channels to support their disruption of established sectors such as transportation (ride-hailing services), hospitality (holiday rentals), real estate (property listings) and entertainment (view on demand). The most popular and best-performing US – Facebook, Amazon, Apple, Netflix and Google (now under its parent Alphabet) ("FAANG") – and Chinese technology companies – Baidu, Bytedance, Alibaba and Tencent ("BAT") – increasingly demonstrate that the use of platforms as the core of their business model is one that brings vast rewards.[10]

2.8 Beyond platform services, businesses have also utilised data to generate top-line value and create new income streams by sharing and collaborating on sensitive data use, so as to (a) offer better engagement with and richer personalised experience for stakeholders, and (b) drive operational efficiency by enabling more contextualised decision-making, while at the same time

Box 3.1 Emerging opportunities for data-driven value creation.



Archetype	Opportunity
New Value Pools	New revenue streams, products and services for a broader range of stakeholders, enabled by data insights and analytics
New Business Models	New collaborative business models, enabled by ecosystem partnerships combining data sets
Richer Stakeholder Experiences	More personalized, convenient and trustworthy experiences in lifecycles and contexts, enriched by data
Better Decisions	Analytics-based insights for better and contextualized decision-making, beyond improvements to operational efficiency

World Economic Forum, "A new paradigm for business of data", Briefing Paper, July 2020, p 6.

[5] "Internet value chain economics: Gaining a deeper understanding of the Internet economy", A.T. Kearney, 2010, p. 6 <https://www.kearney.com/communications-media-technology/article?/a/internet-value-chain-economics> (accessed 15 December 2020).

[6] One zettabyte equals 1,000^7 bytes.

[7] "Data never sleeps 9.0", DOMO <https://web-assets.domo.com/blog/wp-content/uploads/2021/09/data-never-sleeps-9.0-1200px-1.png> (accessed 7 October 2021); "Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025", Statista <https://www.statista.com/statistics/871513/worldwide-data-created/> (accessed 7 October 2021.

[8] As of July 2021, 65% of the world's population, 5.17 billion people, now has access to the internet, a 10% increase from January 2021 ("Data never sleeps 9.0", DOMO <https://web-assets.domo.com/blog/wp-content/uploads/2021/09/data-never-sleeps-9.0-1200px-1.png> [accessed 7 October 2021]).

[9] "Digital economy report 2019: Value creation and capture: Implications for developing countries - Overview", UNCTAD, July 2019, pp 1, 2 <https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf> (accessed 19 August 2020).

[10] Seven of the world's top 10 companies by market capitalisation as at June 2020 employ the platform-based business model: Apple Inc, (no. 2), Microsoft Corp (no. 3), Amazon.com Inc (no. 4), Alphabet Inc (no. 5), Facebook, now Meta (no. 6), Tencent (no. 7), Alibaba (no. 8) ("Global Top 100 companies by market capitalisation", PWC, July 2020, p 11 <https://www.pwc.com/gx/en/audit-services/publications/assets/global-top-100-companies-june-2020-update.pdf> (accessed 19 August 2020).

managing privacy and security concerns. Box 3.1 illustrates this succinctly. Intangible assets which include data, make up US$21 trillion of S&P 500 company value.[11]

2.9 It has been estimated that the global open data[12] economy is worth US$3 trillion a year across seven domains.[13, 14] Pre-COVID forecasts anticipated that by 2021, 60% of the Asia Pacific's gross domestic product ("GDP") would be derived from digital products or services created through digital transformation ("DX"). Over the same period, DX is expected to add 0.8% annually to the region's GDP, or US$1.16 trillion.[15]

2.10 In 2019, 75% of organisations in the Asia Pacific saw data as valuable and these organisations were either currently extracting value from data or planning to do so in the future.[16] In Southeast Asia, the digital economy in five sectors[17] have also grown from strength to strength and hit US$100 billion in 2019 and is expected to triple by 2025.[18] In Singapore alone, the digital economy pre-COVID was set to add close to US$10 billion to its GDP by 2021, and this growth was forecasted to increase at a rate of 0.6% annually.[19]

2.11 The COVID-19 pandemic has accelerated the pace and scale of these developments and increased the stakes for ensuring that the way data is gathered, stored and delivered are carried out in a safe and trustworthy manner. Lockdowns and social distancing around the world have shifted the modalities of living, working and recreation, putting more of such activities online than ever before. Consequently, the pandemic has created increased dependence by individuals, governments and businesses on the technologies that drive daily activities and the resulting data that provide insights, intelligence and information.

2.12 For example, e-commerce saw a huge uptick in sales, making up 8.5% of total retail takings in March 2020 compared to 5.8% in January and 7.4% in February of the same year. This trend is set to continue even after the restrictions are eased.[20]

2.13 Subscriptions to virtual meeting platforms such as ZOOM and Webex increased exponentially and unintendedly exposed security issues that saw hackers ZOOM-bombing live-streamed school lessons in Singapore.[21]

2.14 Digital signatures and its associated software solutions, such as PandaDoc, Adobe Sign and DocuSign, now proliferate commercial contracts, where the authenticity and integrity of the signer can now be validated.

[11] Bruce Berman, "$21 Trillion in U.S. Intangible Assets is 84% of S&P 500 Value – IP Rights and Reputation Included", *IP CloseUp*, 4 June 2019 <https://ipcloseup.com/2019/06/04/21-trillion-in-u-s-intangible-asset-value-is-84-of-sp-500-valueip-rights-and-reputation-included/> (accessed 11 August 2020).

[12] Open data refers to public information and shared data from private sources.

[13] Education, transport, consumer products, electricity, oil and gas, healthcare and consumer finance.

[14] James Manyika, et al, "Open data: Unlocking innovation and performance with liquid information", McKinsey Global Institute, 1 October 2013 <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information> (accessed 15 July 2020).

[15] Daniel-Zoe Jimenez, et al, "Unlocking the economic impact of digital transformation in Asia Pacific", Microsoft-IDC White Paper, November 2018, p 1 <https://3er1viui9wo30pkxh1v2nh4w-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites /43/2018/11 /Unlocking-the-economic-impact-of-digital-transformation.pdf> (accessed 16 July 2020).

[16] The Dell Technologies' 2020 Global Data Protection Index (GDPI) Snapshot cited in "Thriving in a digital economy", The Business Times, 29 April 2020 <https://www.businesstimes.com.sg/technology/thriving-in-a-digital-economy> (accessed 16 July 2020).

[17] e-Commerce, media, ride-hailing, travel and financial services.

[18] Google, Temasek and Bain & Company, "e.Conomy SEA 2019: Swipe up and to the right: Southeast Asia's $100 billion Internet economy", <file:///C:/Users/gillianchee/Downloads/e-Conomy_SEA_2019 _deck_ulb8e2S.pdf> (accessed 16 July 2020).

[19] Tang See Kit, "The rise of the digital economy: What is it and why it matters for Singapore", ChannelNews Asia, 13 January 2020 <https://www.channelnewsasia.com/news/business/what-is-digital-economy-why-it-matters-mobile-app-12240630> (accessed 16 July 2020).

[20] Sue-Ann Tan, "Online shopping trend set to stay after curbs ease, say analysts", The Straits Times, 25 May 2020 <https://www.straitstimes.com/business/economy/online-shopping-trend-set-to-stay-after-curbs-ease-say-analysts> (accessed 5 August 2020).

[21] Hariz Baharudin, "Coronavirus: No more Zoom for home-based learning after hackers show obscene photos to Singapore students", *The Straits Times*, 9 April 2020 <https://www.straitstimes.com/singapore/hackers -hijack-home-based-lessons-on-zoom-to-allegedly-show-obscene-photos-to-children> (accessed 5 August 2020).

2.15 A major challenge faced by majority of businesses and the government is in keeping data safe. Consequently, individuals and society at large are now more conscious of data protection and privacy issues surrounding the collection of personal information and information about technology use, especially when that technology monitors individuals' movements, e.g. the Singapore government's implementation of the TraceTogether and SafeEntry applications.

3. Legal implications from data and the digital economy

Regulation and frameworks

3.1 Increased transborder data flows have resulted in novel legal implications that are often complicated by the fact that there is hitherto no global consensus on how such data flows and processing activities ought to be governed. Instead, what has emerged is a patchwork of regional and local regulations driven by the fact that governments are under increasing pressure to deal with such lacunas created by the borderless nature of data flows and online activities. It therefore comes as no surprise that in recent years, many countries have moved to update their regulations and introduce new approaches to cross-border data regulation.

3.2 For instance, in the area of personal data protection regulations, several international and regional organisations have attempted to harmonise national laws by the introduction of regional governing regimes.[22] Specifically, the EU has taken a leadership position by its enactment of the GDPR in 2018, a legislation which has been a catalyst for the rest of the world to relook at strengthening data protection laws and subsequently inspired legislation that will likely have global implications given their extraterritorial effect. Recognising the importance of having a comprehensive data protection regime, other jurisdictions have also formulated their own data protection laws having regards to their domestic social, economic, cultural and political conditions, such as the Personal Information Protection Law (China); Electronic Information Law, Government Regulation No. 71 of 2019 and Regulation No. 20 of 2016 (Indonesia); California Consumer Protection Act ("CCPA") (US); Consumer Online Privacy Rights Act ("COPRA") (US).

3.3 While international business has witnessed jurisdictional efforts to shore up data protection regulation, governments have conversely encouraged the growth of the digital economy by taking a softer stance in the form of regional and national frameworks that, while non-binding, provide an understanding on how data should be treated and shared.

3.4 Closer to home, the ASEAN Digital Integration Framework aims to achieve digital integration amongst the member states to coordinate and address obstacles and accelerate existing ASEAN platforms to facilitate seamless digital trade, protect data, expand the digital talent base and encourage entrepreneurship.[23]

3.5 More importantly, ASEAN introduced the Singapore-led Framework on Digital Data Governance with the view to facilitate the growth of the digital economy among member states by promoting trade and data flows within ASEAN, while strengthening digital data governance through enhanced data management and harmonisation of data regulations, acknowledging that member states are at various stages of maturity. The Framework, referencing the OECD

[22] EU General Data Protection Regime ("GDPR"); EU-US Privacy Shield; OECD Privacy Framework; APEC Cross-Border Privacy Rules ("CBPR"); Standards for Personal Data Protection for Ibero-American States; ASEAN Framework on Digital Data Governance

[23] ASEAN digital integration framework <https://asean.org/storage/2019/01/ASEAN-Digital-Integration-Framework.pdf> (accessed 11 August 2020).

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework, seeks to guide member states on their policy and regulatory approaches to personal and non-personal digital data governance in the digital economy.[24]

3.6 Beyond ASEAN, China also recently unveiled its global standard for data security amid a trade war with the US and the then Trump administration's hard-line stance against Chinese technology companies and its "Clean Network" programme. The framework's underlying aim is to preserve national security and interests as mounting data security risks pose new challenges to global digital governance. The framework proposes that states handle data security in a comprehensive, objective and evidence-based manner, where they should not ask domestic companies to transfer overseas data to their own governments in breach of another country's laws and opposes any form of surveillance of other states and requests to companies to store data generated and obtained overseas in their own jurisdiction.[25]

Technologies and policy considerations

3.7 There are also legal and policy implications arising from technologies that power the digital economy including AI, blockchain and more generally distributed ledger technology, 5G network, data analytics, and cybersecurity.

3.8 Singapore has been investing in information and communication technologies and infrastructure for the past 30 years, with the recent focus on the transformation of the society, government, and economy through digitalisation and automation. Specifically, the IMDA's Infocomm Media 2025 Industry Transformation Map ("ITM") seeks to build the infocomm media sector as an "enabler" of Singapore's digital economy by leveraging frontier technologies, of which the government has identified six technology areas that will propel and impact the digital economy, reflecting the disparate nature of and skillsets required to operate in this sector:[26]

a. Big data and analytics
b. IoT, e.g. remote patient health monitoring
c. Cognitive computing and advanced robotics, e.g. autonomous vehicles
d. Future Communication and Collaboration Technologies, e.g. fibre optics
e. Cybersecurity[27]
f. Immersive media, e.g. wearable tech with in-built augmented reality

3.9 This has been refreshed by IMDA's Services and Digital Economy Technology Roadmap (Services 4.0) that reflects the technology shifts that have since taken place and identifies nine trends that will have the greatest impact on the digital economy in the next three to five years

[24] "Framework on Digital Data Governance", ASEAN Telecommunications and Information Technology Ministers Meeting ("TelMin"), paras 2, 3 <https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf> (accessed 22 August 2020).

[25] Wang Wenwen and Zhang Hui, "China launches global data security initiative, respects data sovereignty", Global Times, 8 September 2020 <https://www.globaltimes.cn/content/1200228.shtml> (accessed 10 September 2020).

[26] "Infocomm Media 2025", Infocomm Media Development Authority, August 2015 <https://www.imda.gov.sg/-/media/Imda/Files/About/Resources/InfocommMedia2025Report.pdf?la=en> (accessed 27 July 2020).

[27] McAfee estimates that the impact of cybercrime on the global economy increased from US$445 billion in 2014 to US$600 billion a year in 2017 which is nearly 1% of the global GDP. An estimated two-thirds of the people online (more than two billion individuals) have had their personal information stolen or compromised ("Economic impact of cybercrime—No slowing down", Centre for Strategic & International Studies and McAfee, February 2018 <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact_cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email> (accessed 28 July 2020).

(2021–2023), with particular emphasis on services as it accounts for 70.4% of Singapore's GDP:[28, 29]

a. Artificial intelligence: adopt pervasively in commercial AI-based applications including products, processes and insights
b. Artificial intelligence: automate, augment and simulate human behaviour, thinking and engagement
c. Human-machine collaboration: narrow the gap between humans and machines, e.g. humanoids and cobots
d. Natural technology interfaces: integrate experiences through mixed reality, harnessing augmented and virtual reality and IoT
e. Codeless development tools: simplify previously complexed tasks, thereby making the creation of applications and solutions easier
f. Digital platforms and as-a-service architecture: harness convergence of emerging technologies to provide a seamless experience across the customer journey
g. Hybrid and Multi-Cloud: create a flexible cloud computing ecosystem
h. Blockchain: decentralise trust by utilising blockchain to act as gatekeeper of companies' assets and individuals' online identity and reputation
i. Application Programming Interface ("API") economy: reuse technology assets across and beyond a company's business

3.10 Another prong of the government's digital transformation drive is its ambitious Smart Nation plan to elevate every aspect of Singapore life by harnessing digital and smart technologies. Strides have already been made in this area: improvements in transport systems with autonomous vehicles and hands-free ticketing, establishment of seamless electronic payments in the form PayNow and the provision of secure transactions between individuals and business and the government via SingPass and MyInfo.[30] MyInfo, a database of citizens' and residents' vital information, is particularly interesting as the government has allowed commercial access to such personal information to promote operational efficiencies while establishing intuitive user experiences for customers. But this has posed the conundrum of balancing, on the one hand, the government's push for a smart nation on a macro level and business efficiencies and innovative solutions at a micro level, and the sensitivity of access to personal data and the risks involved in the responsible use of new technologies and data sharing on the other.[31]

3.11 The IMDA and the Personal Data Protection Commission ("PDPC") has attempted to address this issue when they introduced the Model AI Governance Framework ("Model Framework") and the Trusted Data Sharing Framework ("Trusted Framework") in 2019.

3.12 The purpose of the Trusted Framework is to recommend a set of baseline data sharing practices while recognising the confines of the Personal Data Protection Act ("PDPA") which, it is hoped, will increase consumers' trust in an organisation's ability to safeguard their personal data and

[28] "Nominal GDP 2019", Department of Statistics Singapore <https://www.singstat.gov.sg/modules/infographics/economy> (accessed 31 August 2020).

[29] "The future of services: Services and digital economy technology roadmap," Infocomm Media Development Authority, 22 November 2018 <https://www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/Technology/Technology-Roadmap/SDE-TRM-Main-Report.pdf> (accessed 30 August 2020).

[30] "Strategic national projects", Smart Nation Singapore <https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Strategic-National-Projects> (accessed 27 July 2020).

[31] Prateek Dayal, "New year, new regulations: where Singapore stands with privacy regulations", Singapore Business Review, 6 January 2020 <https://sbr.com.sg/information-technology/commentary/new-year-new-regulations-where-singapore-stands-privacy-regulation> (accessed 21 August 2020).

use it responsibly. This, in turn, may encourage them to share their data with organisations more willingly. This trust is the bedrock of a vibrant digital economy.[32]

3.13 The Model Framework encompasses practical ethical principles for organisations to adopt and adapt when deploying their AI solutions and to align their AI governance practices. It covers four key areas:

a. internal governance structures and measures
b. human involvement in AI-augmented decision-making
c. operations management
d. stakeholder interaction and communication[33]

3.14 Tied closely to this is MAS' general principles to promote FEAT to employ AI ethical principles in the financial sector:

a. Fairness – that individuals are not systematically treated unfairly or are disadvantaged through AI-driven decisions unless these can be justified
b. Ethics – that the use of AI and data analytics ("AIDA") is in line with a financial institutions' ethical standards, that AI-driven decisions are of similar ethical standards as those driven by humans
c. Accountability – that financial institutions using AIDA are accountable for internal and external AIDA models adopted
d. Transparency – that, as part of financial institutions' general communications, individuals (data subjects) are informed of the use of AIDA, including explanations of what data is used to make AIDA-driven decisions about them and how such data affects the decisions.

3.15 Financial institutions are to consider these principles, above and beyond existing laws, when using AIDA to create and provide financial products and services, and rolling out their own governance measures and frameworks relating to the use of AIDA in their business models.[34]

3.16 Beyond the FEAT principles, it is also worth noting that the MAS has embarked on Project Veritas in collaboration with financial institutions in Singapore, which is expected to provide a practical framework to operationalise the FEAT principles and to further elucidate how these principles may translate to meaningful outcomes for responsible AI deployment and data use.

3.17 While advancements have been made in building Singapore's digital economy and digitisation has become more ubiquitous, the flipside of the Singapore government's digital transformation initiatives is that cybersecurity is now a real vulnerability that requires serious attention. To this end, Singapore has enhanced the country's cyber and data security capabilities through the establishment of the Cyber Security Agency of Singapore and the passing of the Cybersecurity Act 2018. One billion dollars of public funds has been dedicated in Budget 2020 to further safeguard personal and public data and critical information infrastructure.

[32] "Enabling data-driven innovation through trusted data sharing in a digital economy", Infocomm Media Development Authority, 28 June 2019, updated 16 July 2020 <https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2019/Enabling-Data-Driven-Innovation-Through-Trusted-Data-Sharing-In-A-Digital-Economy> (accessed 22 August 2020).

[33] Info-communications Media Development Authority and Personal Data Protection Commission, Model Artificial Intelligence Govenance Framework, (2nd Ed, 2020) p 20 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf> (accessed 1 October 2021).

[34] "Principles to promote fairness, ethics, accountability and transparency in the use of artificial intelligence and data analytics in Singapore's financial sector", Monetary Authority of Singapore, 12 November 2018 updated 7 February 2019 < https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf> (accessed 28 August 2020).

3.18 This is especially timely on the back of high-profile cybersecurity breaches in the commercial and public sectors, which makes Singapore a key target for cybercriminals. There were 7.24 million local incidents in 2019 for Singapore, as compared to 6.75 million in the previous year:

a. cyberattacks on a number of local websites by a member of the hacktivist organisation Anonymous, "The Messiah", partly in response to Singapore's web censorship regulations
b. the cyberattack on Singapore General Hospital's database in 2017 where personal particulars of close to 1.5 million SingHealth patients were accessed and copied
c. leakage of personal data of 2,400 Ministry of Defence personnel in 2019

3.19 It is estimated that, in 2017, the economic loss in Singapore due to cybersecurity incidents amounted to US$17.7 billion,[35] with 80% of Singapore organisations having suffered a data breach as a result of a cyberattack in the past 12 months (April 2019–March 2020)[36] and risk managers in 2019 citing cyber threats as the second top business risk, followed by changes in legislation and regulation.[37]

3.20 The spate of data breaches has warranted the introduction and stricter enforcement of laws and penalties. The PDPC enforces the provisions of the PDPA and has the power to give directions, ranging from destruction of illegally collected personal data to hefty penalties of up to S$1 million levied on entities which it finds has breached any of those provisions. Since its inception in January 2013, it has released 146 decisions[38] resulting in "not in breach", warnings, directions and penalties. It saw a record number of reported PDPA breaches in the first 8 months of 2019 alone, with 26 organisations having either been fined or warned, up from 23 for the whole of 2018, with S$1.28 million[39] in fines issued compared to $339,000 from 2016 to 2018.[40]

3.21 To keep pace with the ever-changing landscape, the PDPC has taken steps to update the PDPA. In June 2020, it released a consultation paper on the Personal Data Protection (Amendment) Bill where the proposed amendments aim to "strengthen public trust, enhance business competitiveness, and provide greater organisational accountability and assurance to consumers, in support of Singapore's Digital Economy"[41] including enhancing the PDPA's framework for the collection, use and disclosure of personal data to enable "meaningful consent where necessary", and the new Data Portability Obligation which gives individuals greater autonomy over their data. On 2 November 2020, the amendment bill was formally passed and introduced not only the aforementioned data portability obligations, but also new bases to legitimise data processing, enhanced penalty and enforcement powers and breach reporting notifications in the event of data breaches involving personal data.

[35] "Understanding the cybersecurity threat landscape in Asia Pacific: Securing the modern enterprise in a digital world", Frost & Sullivan and Microsoft, 18 May 2018 <https://news.microsoft.com/en-sg/2018/05/18/cybersecurity-threats-to-cost-organisations-in-singapore-us17-7-billion-in-economic-losses/#_ftn1> (accessed 28 July 2020).

[36] "Singapore Threat Report: Extended enterprise under threat", Carbon Black, June 2020, p. 13 <https://www.carbonblack.com/wp-content/uploads/VMWCB-Report-GTR-Extended-Enterprise-Under-Threat-Singapore.pdf> (accessed 29 July 2020).

[37] "Allianz Risk Barometer: Identifying the major business risks for 2020", Allianz Global Corporate & Specialty, January 2020, Results Appendix 2020, p. 21 <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020-Appendix.pdf> (accessed 29 July 2020).

[38] Manual count

[39] Of the S$1.28m in fines, S$1m was attributed to the SingHealth breach.

[40] Data Protection Excellence Centre ("DPEX") and Straits Interactive, "Number of organisations breaching the Personal Data Protection Act rise significantly in Singapore", media release, 17 September 2019 <https://www.dpexnetwork.org/media-releases/the-data-protection-excellence-dpex-centre-releases-research-on-the-number-of-organisations-breaching-singapores-personal-data-protection-act/> (accessed 7 August 2020).

[41] "Public Consultation on Personal Data Protection (Amendment Bill)" Personal Data Protection Commission, 14 May 2020 <https://www.pdpc.gov.sg/news-and-events/announcements/2020/05/public-consultation-on-personal-data-protection-(amendment)-bill#:~:text=PDPC%20%7C%20Public%20Consultation%20on%20Personal%20Data%20Protection%20(Amendment)%20Bill&text=Organisations%20registered%20with%20ACRA%20can,information%20via%20ACRA%20BizFile%E2%81%BA.&text=Should%20you%20urgently%20require%20to,sg%20to%20make%20an%20appointment> (accessed 5 August 2020).

4. Proposed D2E Specialist Accreditation Scheme

Developing and recognising legal D2E competence

4.1 The developments observed in Section 3 above have driven demand for and elevated the importance of legal professionals with capabilities to address legal issues involving data protection, data breaches, data management/governance, technology policy advocacy, AI governance and cybersecurity/cybercrime. The unique competencies emerging from these changes extend beyond the ones defined in "TMT" practices - the ubiquitous and market-established naming convention adopted by most law firms for their technology practices. At its inception, TMT as a practice area was dominated by analogue technologies – print, media and telecommunications – each governed by individual sets of regulations. However, these platforms have since moved online, been digitised, and are driven by data where multiple governing laws and/or sector regulations may apply.

4.2 While "TMT" captures the horizontals of the digital economy, it does not do the same for the vertical emerging segments such as social media and blockchain. D2E therefore seeks to recognise this shift by focusing on what drives this industry which is data. "Data" is an inclusive term which covers AI, data analytics, cybersecurity, data protection, IP in terms of ownership and the right to use data, transactional work and infrastructure, e.g. telecommunications work and building pipes for transmission.

4.3 At the professional level, "TMT" does not recognise the disparate D2E ecosystem of stakeholders – inhouse counsel, legal technologists and engineers – and the work that they do where each plays an important part in the D2E legal space.

4.4 Beyond innovation in technology, new business models have also challenged how legal services may be provided. Apart from TMT practice areas in large firms, boutique law firms dedicating much of their practice to digital law are now commonplace on the legal services landscape. For example, Collyer Law (whose tagline is "Legal Engineering") offer legal services focussing on "emerging tech and the innovation economy" in sectors such as "Fintech", "Digital Commerce & Platforms" and "Digital Currency & Blockchain".

4.5 Joyce A. Tan & Partners deal with technology matters specifically Information Technology, Data Protection & Privacy and Cybersecurity, while Consigclear LLC delves in gaming law specifically social, mobile and cloud gaming and operational contracts such as software licences, non-disclosure agreements and service and level agreements.

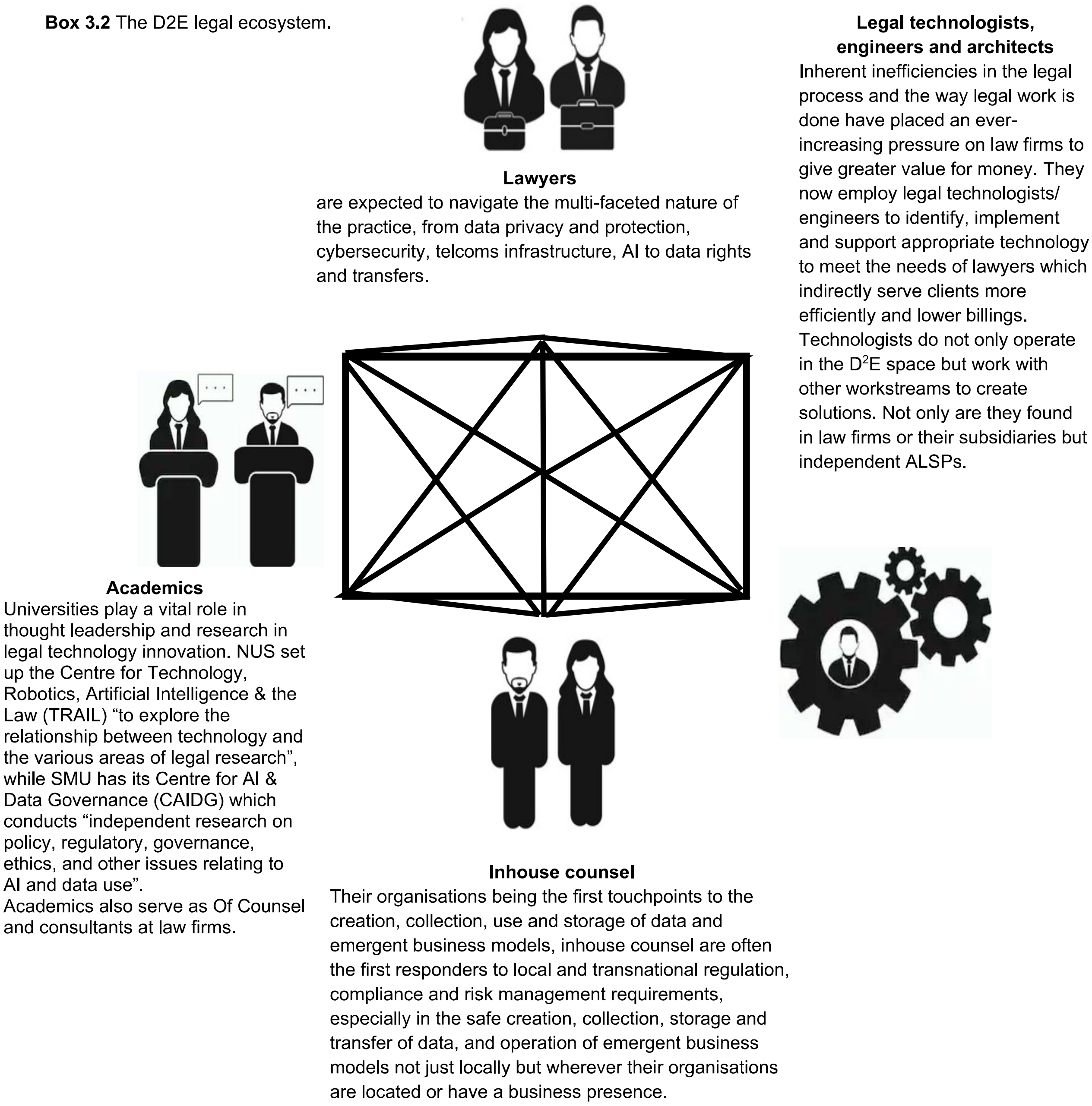
4.6 Alternative Legal Service Providers ("ALSPs") in some jurisdictions are now providing online legal advice at a fraction of lawyers' fees. It is estimated that ALSPs' revenues have soared from US$8.4 billion in 2015 to US$10.7 billion in 2017 globally. Where once ALSPs served mainly big corporations with solutions like eDiscovery, the COVID-19 pandemic has seen them make inroads in the SME and private citizen markets.[42]

4.7 Each stakeholder in this disparate group undertakes a range of tasks that require dedicated skillsets (see Box 3.2). Section 2 highlights the expansive nature of the D2E domain which conversely demands the legal community to possess skills and knowledge that are vast and agile to serve in an increasingly complex area.

[42] Stefanie Santana, "Covid-19: Three less obvious ways it is influencing the legal tech revolution", *The Legal Technologist*, July 2020 <http://www.legaltechnologist.co.uk/TheLegalTechnologistJul20.pdf> (accessed 12 August 2020).

4.8 Broadly speaking, while adopting the term “D2E” may be defining a new genre of specialisation, this also presents an opportunity for Singapore to be recognised as the thought leader in this domain of competence, especially if this classification is accepted by the public and catches on in other jurisdictions.

Box 3.2 The D2E legal ecosystem.



Lawyers
are expected to navigate the multi-faceted nature of the practice, from data privacy and protection, cybersecurity, telcoms infrastructure, AI to data rights and transfers.

Legal technologists, engineers and architects
Inherent inefficiencies in the legal process and the way legal work is done have placed an ever-increasing pressure on law firms to give greater value for money. They now employ legal technologists/ engineers to identify, implement and support appropriate technology to meet the needs of lawyers which indirectly serve clients more efficiently and lower billings. Technologists do not only operate in the D^{2}E space but work with other workstreams to create solutions. Not only are they found in law firms or their subsidiaries but independent ALSPs.

Academics
Universities play a vital role in thought leadership and research in legal technology innovation. NUS set up the Centre for Technology, Robotics, Artificial Intelligence & the Law (TRAIL) “to explore the relationship between technology and the various areas of legal research”, while SMU has its Centre for AI & Data Governance (CAIDG) which conducts “independent research on policy, regulatory, governance, ethics, and other issues relating to AI and data use”.
Academics also serve as Of Counsel and consultants at law firms.

Inhouse counsel
Their organisations being the first touchpoints to the creation, collection, use and storage of data and emergent business models, inhouse counsel are often the first responders to local and transnational regulation, compliance and risk management requirements, especially in the safe creation, collection, storage and transfer of data, and operation of emergent business models not just locally but wherever their organisations are located or have a business presence.

Approaches in recognising legal technology competence in other jurisdictions

4.9 Accreditation schemes in other jurisdictions have sought to recognise the expertise of legal practitioners in substratas of TMT, e.g. Bar Association of North Carolina’s Privacy and Info

Security Law certification and Die Rechtsanwältinnen und Rechtsanwälte in der Bundesrepublik Deutschland's Informationstechnologierecht (information technology law), or to identify lawyers and paralegals with proficiency in legaltech, e.g. the Law Society of Scotland's Accredited Legal Technologist.[43]

4.10 The D2E Scheme, as explained in the preceding section, attempts to highlight the nature and expansiveness of the skillsets that are grounded in data, which are relevant, necessary and in demand for today's legal practice in this field.

Defining D2E specialist competence

4.11 In recognising the expansive nature of the D2E practice, the subcommittee proposes an accreditation framework that would reflect the attributes, experiences, and range of work to which legal practitioners in this domain are expected to be exposed to and undertake in the course of their professional career, while being mindful to not stray too far from existing accreditation programmes.

4.12 Because the field of D2E is wide, the subcommittee was cognisant of the need to strike a balance between showing evidence of practice across a broad spectrum of topics (which may make accreditation limiting and under-inclusive), and the danger of over-specialising fragmentation if accreditation is readily given to those who specialise in only one specific field.

4.13 Thus, the subcommittee's recommended accreditation framework requires individuals to be substantially involved in core areas, while recognising their unique specialisations in the form of specialisms. This will lend to the creation of specialists with shared expertise, while allowing some flexibility to build upon expertise in their own dedicated field.

4.14 This is reflected in the topics for assessment and in turn the syllabus for the examination preparatory course (see Appendix B). The subcommittee has devised requirements for each tier of specialist that encompasses the competencies expected of a D2E legal specialist (see Appendix A).

Who can be accredited?

4.15 Unlike the current practice areas offered under the Specialist Accredited Scheme (the "Scheme"), the D2E accreditation programme will be open to legal practitioners comprising:

a. Singapore-called lawyers
b. Singapore-called inhouse counsel

4.16 The D2E subcommittee was of the opinion that the role of inhouse counsel has changed. They are now driving the practice on both the legal and technical fronts. As inhouse counsel are heavily involved in their organisations' data collection and security governance and best practices, it is logical to open the accreditation programme to this group of practitioners.

4.17 Furthermore, the D2E scheme seeks to enhance the portability of skillsets by recognising these skills of ex-lawyers who once plied their D2E trade in law firms but have now ported their practice inhouse, and also those who return to practice thereafter.

[43] Interestingly, the Counseil National de Barreaux (France) offered specialist accreditation in *Droit des Nouvelles Technologies, de l'Informatique et de la Communication* (roughly translated as law of new technologies, computer science and communication) until 2021 (Counseil National de Barreaux, "Guide Pratique Candidat: Obtenir un certificat de spécialisation 2019"; "Liste de qaulifications spécifiques", 21 October 2021 <https://www.cnb.avocat.fr/fr/liste-des-qualifications-specifiques> [accessed 19 November 2021]).

4.18 They were also cognisant that the other accreditation programmes of Building and Construction Law and Maritime and Shipping Law are not open to inhouse counsel. The inclusion for the D2E scheme will be a testbed for a similar approach in the future for these two practice areas.

4.15 The D2E subcommittee also recognises that technology and data flows are borderless, and D2E legal practitioners are often required to be involved in cross-border and cross-jurisdictional matters. The D2E accreditation would lend larger credence if foreign practitioners can be accredited under this Scheme, which can in turn lead to recognition of the D2E accreditation in other jurisdictions. Hence, while admission to the Singapore Bar is a core requirement for legal practitioners, the subcommittee leaves open the possibility of expanding the Scheme to include both foreign practitioners and foreign-qualified inhouse counsel in the future.

4.16 The subcommittee also considered the inclusion of academics and allied legal professionals who are responsible for legal technology initiatives and thought leadership at their educational institutions, firms and government/private organisations. While these professionals contribute substantially to the D2E ecosystem, the subcommittee opined that in light of the Scheme's objective of recognising the expertise of legal practitioners, the Scheme would for the moment not include this group but leaves open the possibility of expanding the Scheme to additional segments of the D2E legal ecosystem in the future.

5. Conclusion

5.1 After much deliberation, the subcommittee has presented a proposed framework for the accreditation of Singapore-based D2E legal practitioners.

5.2 The Scheme will relook at whether the D2E accreditation programme should be open to foreign legal practitioners, academics and allied legal professionals after it has run for a few years and if there is demand for accreditation from professionals in that sector.

6. Pro tempore selection panel

6.1 As with the other accreditation programmes, a pro tempore selection panel ("panel") will be constituted for the first year that the D2E accreditation programme is offered under the Scheme.

6.2 The panel will be responsible for reviewing applications, interviewing candidates and recommending to the Specialist Accreditation Board ("SAB") candidates for accreditation.

6.3 This five-member panel is expected to be headed by a judge, and includes professionals from relevant government, industry, and/or academic institutions to ensure that the selection process is fair.

6.4 For proceeding runs of the accreditation programme after the first year, the selection panel will comprise professionals from the aforementioned bodies and D2E accredited specialists.

7. Timelines

7.1 The following is the <u>tentative</u> schedule for the D2E law specialist accreditation programme for 2022:

Date	Event
Opening of Legal Year	Accredited Specialist applications open
30 March	Accredited Specialist applications close 5pm
30 April	Accredited Specialist candidature confirmed
1 May	Exam preparatory course registration opens Exam registration opens
1 July	Senior Accredited Specialist applications open
One week prior to start of course	Exam preparatory course registration closes
July/August	Exam preparatory course
One week prior to examination date	Exam registration closes
31 August	Senior Accredited Specialist applications close 5pm
August/September	Examination
30 September	Senior Accredited Specialist candidature confirmed
October/November	Selection panel interview
Opening of Legal Year 2023	Results released to all candidates

Appendix A. Specialist accreditation and reaccreditation framework for Singapore Data and Digital Economy Law[44]

A.1 The accreditation programme will be in Data and Digital Economy Law.

A.2 The accreditation programme for D2E law will be open to Singapore-qualified lawyers and Singapore-qualified inhouse counsel.

Accreditation framework

Baseline criteria for all applicants

A.3 Applicants must satisfy the following baseline eligibility criteria to have their candidature confirmed:

a. Admitted to the Singapore Bar as an Advocate and Solicitor of the Supreme Court of Singapore
b. For practising lawyers, hold a currently valid practising certificate
c. Have a minimum full-time post-qualification experience (PQE)
d. Have not been subject to professional disciplinary proceedings or charged and convicted of a serious crime
e. Have been substantially involved in the full-time practice of D2E law
f. Have been engaged in continuing professional development (CPD) in this area of practice
g. Provide favourable reference statements

Accredited Specialist

Baseline criteria explained

A.4 **Post-qualification experience (baseline criterion (c))**
Legal practitioners should have at least **5 years** of full-time PQE.

A.5 **Substantial involvement (baseline criterion (e))**
For lawyers, applicants must show that, in the immediate **3 years** prior to application, they have been engaged in full-time practice and have dedicated **per year** a **minimum 450 hours** to **1 core and 1 specialism**.

For inhouse counsel, applicants must show that, in the immediate **3 years** prior to application, they have been engaged in full-time legal work, i.e. work that is a permanent and ongoing feature of their role, in **1 core and 1 specialism**[45] within their organisation(s) **a year**.

Core areas
Data Privacy and Protection
Digital Trade[46]
Technology Procurement[47]
Intellectual Property

[44] For an illustration of the framework, see Box A.1.
[45] Recognising the dynamic nature of the D2E space, the Core areas and Specialisms will be reviewed periodically by the selection panel.
[46] Topics include e-commerce, markets and platforms, payment systems and electronic contracting.
[47] Topics include technology contracting and vendor legal risk management.

Specialisms
Artificial Intelligence
Digital Asset Management and Protection
Fintech and Regtech Regulation
Internet-of-Things and Computing
Cybersecurity
Media
Telecommunications

A.6 **Continuing professional development (baseline criterion (f))**
For lawyers, in the immediate **3 years** prior to application, applicants must have accumulated at least **6 public and/or private SILE CPD points a year** in this specialisation.

For inhouse counsel, in the immediate **3 years** prior to application, applicants must have **undertaken the equivalent of at least 6 public and/or private SILE CPD points a year** in this specialisation, e.g. by:

a. attaining a relevant educational graduate qualification or professional certification, e.g. certification from IAPP;
b. attending and/or conducting workshops, webinars, seminars and training courses, CPD events
c. contributing to journals, articles, books, consultation papers, and other forms of publications, etc

A.7 **References (baseline criterion (g))**
Lawyers shall be required to submit two favourable reference statements from D2E legal practitioners (lawyers and/or in-house counsel) and/or non-D2E legal practitioners who can attest to the applicants' involvement and competence in the specialisation who can attest to the applicants' involvement and competence in the specialisation, and character.

Inhouse counsel shall be required to submit two favourable reference statements from D2E legal practitioners (lawyers and/or in-house counsel) and/or non-D2E legal practitioners who can attest to the applicants' involvement and competence in the specialisation, and character.

Assessment criteria

A.8 **Examination**
Candidates must sit for and pass an open-book examination which shall test their knowledge on aspects of D2E law and processes (see Appendix B).

A.9 **Selection panel interview**
Candidates, who achieve a satisfactory examination grade, are required to undergo a selection panel interview (see Appendix B).

A.10 The interview will be conducted by a panel of three assessors with expertise in the area of D2E.

Senior Accredited Specialist

Baseline criteria explained

A.11 **Post-qualification experience (PQE) (baseline criterion (c))**
Legal practitioners should have at least **10 years** of full-time PQE.

A.12 **Substantial involvement (baseline criterion (e))**
For lawyers, applicants must show that, in the immediate **5 years** prior to application, they have been engaged in full-time practice and have dedicated **per year** a **minimum 650 hours** to **1 core and 1 specialism**.

A.13 For inhouse counsel, applicants must show that, in the immediate **5 years** prior to application, they have been engaged in full-time legal work (i.e. work that is a permanent and ongoing feature of their role) in **1 core and 1 specialism**[48] within their organisation(s) **a year.**

Core areas
Data Privacy and Protection
Digital Trade[49]
Technology Procurement[50]
Intellectual Property

Specialisms
Artificial Intelligence
Digital Asset Management and Protection
Fintech and Regtech Regulation
Internet-of-Things and Computing
Cybersecurity
Media
Telecommunications

A.14 **Continuing professional development (baseline criterion (f))**
For lawyers, in the immediate **5 years** prior to application, applicants must have accumulated at least **6 public and/or private CPD points a year** in this specialisation.

A.15 For inhouse counsel, in the immediate **5 years** prior to application, applicants must have **undertaken the equivalent of at least 6 public and/or private SILE CPD points a year** in this specialisation, e.g. by:

a. attaining a relevant educational graduate qualification or professional certification, e.g. certification from IAPP
b. conducting workshops, webinars, seminars and training courses, CPD events
c. contributing to journals, articles, books, consultation papers, and other forms of publications, etc

[48] Recognising the dynamic nature of the D2E space, the Core areas and Specialisms will be reviewed periodically by the selection panel.
[49] Topics include e-commerce, markets and platforms, payment systems and electronic contracting.
[50] Topics include technology contracting and vendor legal risk management.

A.16 **References (baseline criterion (g))**

Lawyers shall be required to submit two favourable reference statements from D2E legal practitioners (lawyers and/or in-house counsel) and/or non-D2E legal practitioners who can attest to the applicants' involvement and competence in the specialisation, and character.

Inhouse counsel shall be required to submit two favourable reference statements from D2E legal practitioners (lawyers and/or in-house counsel) and/or non-D2E legal practitioners who can attest to the applicants' involvement and competence in the specialisation, and character.

Assessment criteria

A.17 **Selection panel interview**

The interview will be conducted by a panel of three assessors with expertise in the area of D2E (see Appendix B).

Accreditation post-nominals and validity

A.18 Candidates who are accredited may include the following post-nominals:

Acc. Spec. (Data & Digital Economy), Singapore Academy of Law
or
Snr. Acc. Spec. (Data & Digital Economy), Singapore Academy of Law

A.19 The validity of specialist accreditation for D2E law is two years, after which specialists must apply for reaccreditation.

Reaccreditation framework

Accredited Specialist

A.20 **Substantial involvement and continuing professional development**
To be reaccredited, Accredited Specialists must show that, in the two years as specialists, they have been engaged in full-time practice in D2E law by fulfilling the same substantial involvement and CPD criteria as for accreditation. Additionally, Accredited Specialists must complete at least one D2E skills module within their first year of accreditation and reaccreditation (see paras A.22–A.25).

A.21 **Panel interview**
If the selection panel deems it necessary, Accredited Specialists may be required to attend a panel interview.

Mandatory completion of skills modules

A.22 Accredited Specialists must complete one D2E skills module from a list of curated and SAL-approved programme which will be identified in consultation with the D2E selection panel and the SAB.

A.23 The D2E skills module must be completed within the first year of accreditation and re-accreditation. If a module is CPD accredited, then completion of the module may also count towards accumulation of CPD points for that year.

A.24 A D2E skills module may not be taken more than once by the same Accredited Specialist.

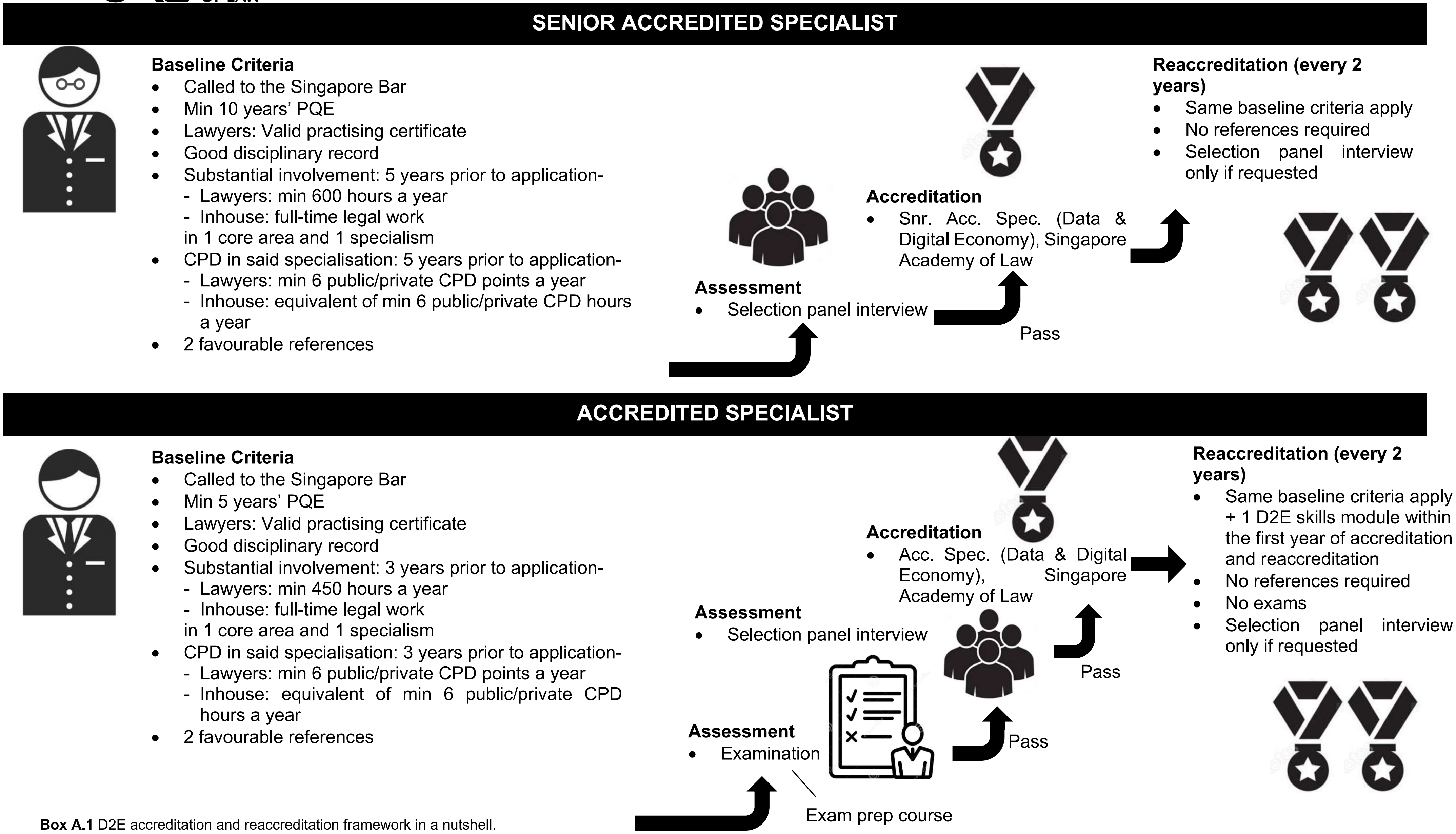
A.25 Topics covered by D2E skills modules can include:

a. Data and design-based problem solving
b. Computational thinking
c. Data analytics and visualisation
d. Digital transformation
e. Complexity and systems thinking
f. Change management

Senior Accredited Specialist

A.26 **Substantial involvement and continuing professional development**
Specialists must show that, in the 2 years as specialists, they have been engaged in full-time practice in D2E law by fulfilling the same substantial involvement and CPD criteria as for accreditation.

A.27 **Panel interview**
If the selection panel deems it necessary, Senior Accredited Specialists may be required to attend a panel interview.



SENIOR ACCREDITED SPECIALIST

Baseline Criteria

- Called to the Singapore Bar
- Min 10 years' PQE
- Lawyers: Valid practising certificate
- Good disciplinary record
- Substantial involvement: 5 years prior to application-
  - Lawyers: min 600 hours a year
  - Inhouse: full-time legal work

  in 1 core area and 1 specialism
- CPD in said specialisation: 5 years prior to application-
  - Lawyers: min 6 public/private CPD points a year
  - Inhouse: equivalent of min 6 public/private CPD hours a year
- 2 favourable references

Assessment

- Selection panel interview

Pass

Accreditation

- Snr. Acc. Spec. (Data & Digital Economy), Singapore Academy of Law

Reaccreditation (every 2 years)

- Same baseline criteria apply
- No references required
- Selection panel interview only if requested

ACCREDITED SPECIALIST

Baseline Criteria

- Called to the Singapore Bar
- Min 5 years' PQE
- Lawyers: Valid practising certificate
- Good disciplinary record
- Substantial involvement: 3 years prior to application-
  - Lawyers: min 450 hours a year
  - Inhouse: full-time legal work

  in 1 core area and 1 specialism
- CPD in said specialisation: 3 years prior to application-
  - Lawyers: min 6 public/private CPD points a year
  - Inhouse: equivalent of min 6 public/private CPD hours a year
- 2 favourable references

Assessment

- Examination

Exam prep course

Pass

Assessment

- Selection panel interview

Pass

Accreditation

- Acc. Spec. (Data & Digital Economy), Singapore Academy of Law

Reaccreditation (every 2 years)

- Same baseline criteria apply + 1 D2E skills module within the first year of accreditation and reaccreditation
- No references required
- No exams
- Selection panel interview only if requested

Box A.1 D2E accreditation and reaccreditation framework in a nutshell.

Appendix B. Examination and selection panel interview

Examination

B.1 Candidates who have applied to be Accredited Specialists must sit for a written examination.

B.2 They will be examined on a selection of the following topics. The selection of topics will depend on topical areas in a given year, and subject to periodic updates over a two- to three-year cycle to keep pace with developments in the field.

B.3 Due to the expansive nature of D2E law, the format of the examination is expected to allow candidates to choose from a selection of Core Area questions and Specialism questions. For example, candidates may be required to answer 2 out of 4 Core Area questions and 3 out of 5 Specialism questions.

Technical knowledge

Core areas

a. **Data Privacy and Protection**
Digital consumer protection

b. **Digital Trade**
Markets and platforms
Payment systems
Electronic contracting

c. **Intellectual Property**

d. **Technology Procurement**
Technology contracting
Vendor **legal** risk management

Specialisms (structured around interconnectedness of the various areas)

e. **Artificial Intelligence**
Liability and negligence

f. **Cybersecurity**
Computer misuse
Technology risk management

g. **Digital Asset Management and Protection**

h. **Fintech and Regtech Regulation**
Blockchain and cryptocurrency
Distributed ledger technology

i. **Internet-of-Things and Computing**
Platforms and systems including cloud computing
Quantum computing

j. **Media**
Mainstream and social media

Online gaming
Content regulation

k. **Telecommunications**
Connectivity technologies
Software layer
Regulatory issues

B.4 Recognising the borderless nature of the digital economy and data flows, some examination questions should be made jurisdiction-agnostic so as to assess the candidate's grasp and understanding of universally applicable concepts. For instance, while the exam could include a case study on data protection specific to Singapore laws, it can also include essay questions that test and recognise candidates' awareness of D2E issues, which are not confined to Singapore. Examples of questions may include:

a. A case study on data protection compliance in an international organisation
b. Describe the application of design thinking in a digital transformation project in which the candidate was involved
c. The candidate has been given the task of creating a solution to automate a complicated internal work process within their organisation. Using design and/or computational thinking, briefly describe how they would approach this challenge.
d. Questions on change management

B.5 The overall pass mark is **60%**. If the examination consists of parts, the candidates must pass (50%) all parts and must attain the overall pass mark of 60% before they are considered to have passed the examination.

Examination preparatory course

B.6 SAL may offer an examination preparatory course (EPC) for candidates required to sit for the examination.

B.7 EPC attendance is not compulsory.

B.8 The EPC comprises 21 to 28 contact hours of classroom instruction. It may be conducted in-person, asynchronously and/or synchronously online or blended.

B.9 It is assumed that candidates who undertake the EPC have knowledge in D2E law expected of a 5-year PQE legal professional.

B.10 The D2E subcommittee is aware of existing technology law courses[51] that address some of the examination topics but not all. SAL will work with the subcommittee to review these courses and determine if they may be leveraged for the purposes of the D2E scheme, e.g. curating from or adapting modules to be part of the EPC.

Selection panel interview

B.11 Accredited Specialist candidates who pass the examination and Senior Accredited Specialist candidates must attend a selection panel interview.

[51] See Appendix C.

B.12 The interview will surround the candidates' practice experience and their practical and industry knowledge on the said subject matter.

B.13 Similar to the examination, the interview will assess the candidate's grasp and understanding of locally and universally applicable D2E concepts and issues.

B.14 Other topics can include:

Contextual knowledge

a. Geopolitics and Regulation
b. Technology Law and Economics
c. Society and Ethics

Appendix C. Data and Digital Economy Law related courses in Singapore

National University of Singapore

LLM in Intellectual Property and Technology Law

C.1 The LLM in Intellectual Property and Technology Law is a 12-month programme and focussed on intellectual property (IP) law – copyright, trademarks, patents, design and confidential information – in the areas of science and technology such as biomedical law, telecommunications law and internet law.

C.2 The following are the programme's modules:

a. Law of Intellectual Property
b. Singapore Common Law of Contract
c. Artificial Intelligence, Information Science & Law
d. Biotechnology Law
e. Chinese Intellectual Property Law
f. Electronic Evidence
g. Entertainment Law: Pop Iconography & Celebrity
h. Foundations of IP Law
i. Global Data Privacy Law
j. Intellectual Property in Body, Persona & Art
k. International Copyright Law and Policy
l. International Patent Law, Policy and Practice
m. International Trademark Law and Policy
n. IT Law I
o. IT Law II
p. Privacy & Data Protection Law
q. Protection Overlaps in Intellectual Property Law
r. Regulation of Digital Platforms

Singapore Management University

Graduate Certificate in Law and Technology

C.3 The programme's learning objective and approach is to give learners an understanding of the difference between legaltech and technology law, specifically the current state of legaltech and how to implement it in practice.

C.4 There are nine modules, lasting two days each, grouped into four categories relating to foundational knowledge, legal technology, technology law and impact of technology law, to address the learning needs of three specific groups of learners: the innovator (legal technologist), researcher (paralegal) and practitioner (lawyer and legal service officer).

C.5 Foundation Knowledge
a. Understanding Law and Technology

Legal Technology
b. The 21st Century Office
c. Applications of Data and AI in LegalTech
d. Legal Innovation

Technology Law
e. Blockchain, Cryptocurrencies and Smart Contracts

f. Legal issues in AI and Machine Learning
g. Personal Data and Data Protection

Impact of Technology on Law
h. Cybercrime
i. Digital Assets and IP Disputes

Appendix D. Specialist Accreditation Scheme Data and Digital Law Subcommittee

Ken Chia
Associate Principal
Baker McKenzie.Wong Leow LLC

Joey Pang
Joey Pang (Jan 24, 2022 23:46 GMT+8)

Joey Pang (Co-Chair)
Senior Vice President (Legal & Compliance)
DBS Bank Ltd

Vice-Chair, Cybersecurity and Data Protection Committee
Law Society of Singapore

Josh Lee Kok Thong
Chairperson
Asia Pacific Legal Innovation and Technology Association

Co-Founder
LawTech.Asia

Legal Policy Manager (AI Governance)
Infocomm Media Development Authority

Ivan Rawtaer
Ivan Rawtaer (Jan 25, 2022 03:18 GMT+8)

Ivan Rawtaer
Co-founder
Pactly

How Khang Lim
How Khang Lim (Jan 24, 2022 14:04 GMT+8)

Lim How Khang
Assistant Professor of Law and Computer Science (Practice)
Yong Pung How School of Law
Singapore Management University

Director
Centre for Computational Law
Singapore Management University

Rajesh Sreenivasan (Jan 25, 2022 13:35 GMT+8)

Rajesh Sreenivasan (Chair)
Partner
Rajah & Tann Singapore LLP

Director
Rajah & Tann Technologies Pte Ltd

Lim Seng Siew
Advocate and Solicitor
OTP Law Corporation

Council Member
Law Society of Singapore

Michael Tan (Jan 28, 2022 09:45 GMT+8)

Michael Tan
Head of Legal
Google Cloud APAC

With contribution from
Paven Sharma
Managing Legal Engineer
Pinsent Masons MPillay

END