

附件



律师开展数据出境合规法律服务 业务指引

广州市律师协会第十一届
数据与数字经济专业委员会

广州数据交易所

编

二〇二六年五月

序 言

当前，数字经济纵深发展与高水平对外开放进程持续加速，广东省政府、广州市政府高度重视数字经济发展，相继出台《广东省数字经济促进条例》《广州市数字经济促进条例》等法规，并印发《关于以高水平开放推动数字贸易和服务贸易高质量发展的实施意见》等政策文件，聚焦大力发展数字贸易、推进服务贸易创新发展、拓展国际市场布局、强化保障支撑体系四大方面，提出 18 项举措。《广东省国家数字经济创新发展试验区建设方案(2025—2027 年)》明确提出，计划到 2027 年，数字经济发展水平稳居全国首位，并要构建数据基础制度新范式，完善数据要素市场化配置制度规则体系。

在此背景下，数据出境已成为广州企业参与国际竞争、融入全球产业链供应链的必然要求。广州作为国家中心城市与“一带一路”重要枢纽，数据跨境流动需求日益旺盛且场景不断丰富。与此同时，《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《规范和促进数据跨境流动规定》《数据出境安全评估办法》等法律法规相继出台并持续细化，构建起日趋完善的企业数据出境监管框架，企业“出海”过程中面临的境内外双重合规压力显著提升。

习近平总书记强调，“要维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济”、“要加快形成系统完备的涉外法律法规体系，提升涉外执法司法效能”。党的二十届三中全会也明确指出，要“提升数据安全治理监管能力，建立高效便利安全的数据跨境流动机制”。因此，必须深入贯彻习近平涉外法治思想，坚持建设中国特色社会主义法治体系，加强重点领域、新兴领域、涉外领域立法，统筹推进国内法治和涉外法治，加快涉外法治工

作战略布局，在数据跨境流动中更好维护国家主权、安全、发展利益，协调推进国内治理和国际治理，切实保障企业和公民的合法权益。

《关于构建数据基础制度推进数据要素市场高质量发展的实施意见》（即广东省“数据二十条”），明确提出要构建数据安全合规有序跨境流通机制，大力推动粤港澳三地数据协同与流动规则机制联通，支持在科技、医疗、金融、教育、文旅、交通、电子商务等领域，探索建立科学规范认证制度、数据出境标准合同规则、安全评估标准等。探索建立数据出境安全评估便捷机制，构建多渠道、便利化的数据跨境流动监管机制，确保数据跨境安全。

由此可见，律师开展数据出境合规法律服务，既是助力广州企业防范合规风险、保障跨境业务平稳有序开展的关键支撑，也是积极贯彻习近平涉外法治思想、响应广东省、广州市等省市重大战略部署，落实广东省“数据二十条”关于构建便利化数据跨境流动监管机制、广州市推进数据跨境安全有序流动相关政策要求的重要途径。

为指导和规范律师开展此类业务，广州市律师协会数据与数字经济专业委员会结合国家法律法规、粤港澳大湾区及广州地方政策，参考数据跨境合规实务经验，制定本指引，为广州市广大律师同行们提供借鉴与参考。

目 录

第一章 总则.....	1
第二章 律师开展数据出境法律服务业务流程.....	2
第三章 数据出境安全风险自评估与个人信息保护影响评估.....	7
第四章 数据出境安全评估申报专项法律服务.....	10
第五章 个人信息标准合同备案专项法律服务.....	11
第六章 数据出境保护认证专项法律服务.....	13
第七章 数据出境合规管理体系建设.....	15
第八章 律师从事数据出境合规法律服务业务的执业规范与风险防范.....	16
第九章 附则.....	19

广州市律师协会数字经济专业委员会
广州数据交易所

第一章 总则

第一条 为深入贯彻落实习近平总书记关于“统筹推进国内法治和涉外法治、更好维护国家主权、安全、发展利益，加快形成系统完备的涉外法律法规体系，提升涉外执法司法效能”的重要论述及指示精神，引导广州律师规范开展数据出境合规法律服务，推动企业依法合规开展数据跨境活动，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《数据出境安全评估办法》《个人信息出境标准合同办法》《律师执业管理办法》等法律法规，制定本指引。

第二条 本指引适用于广州市执业律师（以下简称律师）办理数据出境法律业务，包括但不限于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证和其他与数据出境相关的活动。

第三条 数据出境安全评估与合规管理涉及的数据，主要为重要数据和个人信息。

重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。仅影响组织自身或公民个体的数据一般不作为重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

第四条 数据处理器是指在数据出境活动中，自主决定数据处理目的和处理方式的主体，如为企业集团且涉及多个关联公司，则需明确一个作为数据处理器具体承担数据出境申报合规责任的主体。

第二章 律师开展数据出境法律服务业务流程

第五条 律师开展数据出境法律服务业务流程

（一）指导数据处理器盘点数据资产，梳理境内数据收集涉及的业务场景，并确定数据处理器；

（二）识别数据出境的必要性，是否存在数据出境安全评估、个人信息出境标准合同备案及个人信息保护认证的豁免情形，是否为自由贸易试验区制定的区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单（以下简称负面清单）外的数据；

（三）识别数据处理器是否属于关键信息基础设施运营者或自由贸易试验区内数据处理器，及出境数据的类型、规模和敏感度，有无重要数据及敏感个人信息等，关于重要数据的识别，可参考 GB/T 43697-2024《数据安全技术 数据分类分级规则》附录 G；

（四）协助明确数据出境的接收方及有无再转移、出境目的、处理方式、出境链路及相关安全保障能力与技术措施等；

（五）查明并协助更新数据处理器现有的数据安全及个人信息保护政策，如有无信息安全政策、信息分类政策、个人信息保护政策、数据记录管理政策、访问控制及加密政策、应急管理指南、个人信息保护影响评估报告等；

(六) 根据数据出境的目的、数据处理者的类型、出境数据的类型和规模、是否存在豁免情形等因素，为数据处理者提供数据出境合规路径选择的法律建议；

(七) 协助数据处理者拟定及修改境内数据处理者与境外接收方订立的数据出境合同等相关法律文件；

(八) 协助数据处理者开展数据安全风险评估或个人信息保护影响评估，并针对评估中发现的法律风险提出整改建议；

(九) 协助数据处理者申报数据出境安全评估，或申请个人信息出境标准合同备案，或开展个人信息保护认证。

第六条 律师梳理数据出境行为及个人信息跨境处理场景

(一) 数据出境行为

1. 数据处理者将在中华人民共和国境内收集和产生的数据传输至境外；

2. 数据处理者收集和产生的数据存储在国内，境外的机构、组织或者个人可以查询、调取、下载、导出；

3. 符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他数据处理活动。

(二) 典型的个人信息跨境处理场景

1. 跨国公司或同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动；

2. 境内个人信息处理者委托境外服务提供商处理数据；

3. 境内个人信息处理者向境外接收方提供个人信息；

4. 境内个人信息处理者与境外接收方共同处理个人信息；
5. 境外个人信息处理者在境外收集分析境内自然人个人信息。

第七条 律师提供数据出境的合规路径选择的法律建议

（一）数据出境安全评估申报适用范围

数据处理者向境外提供数据，符合下列条件之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

1. 关键信息基础设施运营者向境外提供重要数据或者个人信息；
2. 关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息。

（二）个人信息出境标准合同或者通过个人信息保护认证适用范围

关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。

个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同或个人信息出境认证的方式向境外提供。

第八条 律师审查是否具有豁免情形

符合下列情形之一的，免于申报数据出境安全评估、申请个人信息出境标准合同备案或提交个人信息保护认证：

（一）国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的；

（二）数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的；

（三）为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的；

（四）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的（不包括应聘者简历及信息）；

（五）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

（六）关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的。

第九条 律师审查是否属于自由贸易区内数据出境负面清单外的申报

自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免于申报数据出境安全评估、申请个人信息出境标准合同备案或提交个人信息保护认证。但数据处理者仍需遵守《个人信息保护法》等

法律法规的基本义务，如获得个人信息时应履行单独告知义务并获得同意，数据处理者应每年进行个人信息保护影响评估并形成年度报告。

第十条 律师协助审查及加强出境数据中个人信息权益的法律保障

律师应当协助数据处理者审查出境数据中涉及的个人信息的收集及处理，是否符合“合法、正当、必要”原则，是否具有出境必要性，是否已采取对个人权益影响最小的方式。数据处理者是否已履行向个人信息所有者的自然人单独告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、出境个人信息的种类以及个人向境外接收方行使法定权利的方式和程序等事项，并取得个人的同意，获得用户确认，无论是书面形式还是通过电子交互系统确认的同意。

第十一条 律师审查境外接收方的数据安全保护责任义务条款

数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容（且标准条款不得修改变更）：

（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化

以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；

（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

第三章 数据出境安全风险自评估与个人信息保护影响评估

第十二条 律师指导数据处理者完成数据出境安全风险自评估及形成《数据出境安全风险自评估报告》

一、数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项（必要内容事项且不得变更顺序）：

（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

(五)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等(以下统称法律文件)是否充分约定了数据安全保护责任义务;

(六)其他可能影响数据出境安全的事项。

二、数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险,主要包括以下事项:

(一)数据出境的目的、范围、方式等的合法性、正当性、必要性;

(二)境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响;境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求;

(三)出境数据的规模、范围、种类、敏感程度,出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险;

(四)数据安全和个人信息权益是否能够得到充分有效保障;

(五)数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务;

(六)遵守中国法律、行政法规、部门规章情况;

(七)国家网信部门认为需要评估的其他事项。

第十三条 律师指导数据处理者完成个人信息保护影响评估及形成《个人信息保护影响评估报告》

一、评估步骤

评估前：全面调研待评估的对象，形成清晰的数据清单及数据映射图表，并梳理出待评估的具体的个人信息处理活动。

评估时：通过分析个人信息处理活动对个人信息主体的权益可能造成的影响及其程度，以及分析安全措施是否有效、是否会导致安全事件发生及其可能性，综合两方面结果得出个人信息处理活动的安全风险及风险等级，并提出相应的改进建议，形成评估报告。律师可参考 GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》的要求进行个人信息保护影响评估。

二、个人信息保护影响评估应当包括下列内容：个人信息的目的、处理方式等是否合法、正当、必要；对个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应。个人信息保护影响评估报告和处理情况记录应当至少保存三年。

三、个人信息处理者向境外提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：

（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；

（二）出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对国家安全、公共利益、个人信息权益带来的风险；

(三) 境外接收方承诺承担的义务, 以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全;

(四) 个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险, 个人信息权益维护的渠道是否通畅等;

(五) 境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响(若为数据出境标准合同备案), 或对出境个人信息安全和个人信息权益的影响(若为数据出境保护认证);

(六) 其他可能影响个人信息出境安全的事项。

第四章 数据出境安全评估申报专项法律服务

第十四条 律师协助数据处理器提交数据出境安全评估的申请与配合修改补充

律师协助数据处理器申报数据出境安全评估, 应当通过线上方式提交申报材料(数据出境申报系统网址: <https://sjcj.cac.gov.cn>)。关键信息基础设施运营者或者其他不适合通过数据出境申报系统申报数据出境安全评估的数据处理器, 采用线下方式通过所在地省级网信办向国家网信办申报数据出境安全评估。

律师协助数据处理器准备的申报材料包括: 1. 统一社会信用代码证件影印件; 2. 法定代表人身份证件影印件; 3. 经办人身份证件影印件; 4. 经办人授权委托书; 5. 数据出境安全评估申报表; 6. 与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件; 7. 数据出境风险自评估报告; 8. 其他相关证明材料; 9. 申报材料包括书面材料及光盘。

第十五条 律师协助数据处理器根据省级网信办或国家网信办工作人员的要求及时进行申报材料的修改与补充，可以每次先对书面申请资料进行对应修改并提交，省级网信办定稿后再一次进行文件装订及光盘刻录并加密。

第十六条 律师协助数据处理器根据国家网信办的批复，对不具有出境必要性的数据进行本地化储存，并形成书面报告。

第十七条 律师协助数据处理器完成数据出境安全评估的审查流程；审查通过后，提示数据处理器在评估有效期内开展数据出境活动，并在必要时重新申报评估。

第五章 个人信息标准合同备案专项法律服务

第十八条 律师协助数据处理器进行个人信息出境标准合同的起草与审核

律师应根据国家网信部门发布的《个人信息出境标准合同办法》及配套的《个人信息出境标准合同模板》，或者根据《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同》及其实施指引的规定，结合数据处理器数据出境的具体目的、路径、接收地区及接收方主体性质，协助数据处理器判断并选择适用全国个人信息出境标准合同或粤港澳大湾区个人信息跨境流动标准合同。

律师应结合数据处理器数据出境具体情况，起草并完成标准合同的全部条款，明确双方权利义务、风险应对、争议解决等条款；审核合同条款的合法性与合规性，确保无偏离模板要求的条款及内容，避免因不符合标准合同模板而导致备案失败。

律师应协助数据处理者选择与确定境外数据接收主体，如协助梳理企业集团境外服务器分布及接收数据的机构，确定一个主要境外主体作为数据出境接收方签署数据出境标准合同，明确其数据安全保障责任与义务及个人信息发生泄露时的报告义务。

第十九条 律师协助提交数据出境标准合同备案的申请与配合修改补充

律师协助个人信息处理者在标准合同生效之日起 10 个工作日内，通过数据出境申报系统备案，系统网址为 <https://sjcj.cac.gov.cn>。律师应根据数据处理者适用的标准合同类型，协助其在数据出境申报系统中正确选择备案事项及对应模块，包括“个人信息出境标准合同备案”或“粤港澳大湾区个人信息跨境流动标准合同备案”，并协助完成相关信息填报。

律师协助数据处理者准备并提交如下备案材料：1. 统一社会信用代码证件影印件；2. 法定代表人身份证件影印件；3. 经办人身份证件影印件；4. 经办人授权委托书；5. 承诺书；6. 标准合同（范本见附件 4）；7. 《个人信息保护影响评估报告》。

律师协助数据处理者根据省级或市级网信办工作人员的要求及时进行备案材料的修改与补充，一般需要当天立即配合提交，配合材料查验及反馈备案结果。

第二十条 省级网信办应当自个人信息处理者提交备案材料之日起，在法定期限内完成材料查验，并向符合备案要求的个人信息处理者发放备案编号。

适用粤港澳大湾区个人信息跨境流动标准合同备案的，材料查验期限一般为 10 个工作日；适用全国个人信息出境标准合同备案的，材料查验期限一般为 15 个工作日。

备案过程中需要补充完善材料的，个人信息处理者应当在 10 个工作日内提交补充完善材料；逾期未补充完善材料的，备案机关可终止本次备案程序。

第二十一条 律师定期协助数据处理者开展备案后管理

在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

（一）向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；

（二）境外接收方所在国家或者地区（包括香港、澳门）的个人信息保护政策和法规发生变化等可能影响个人信息权益的；

（三）可能影响个人信息权益的其他情形。

个人信息处理者在标准合同有效期内补充订立标准合同的，应当向原备案机关提交补充材料；重新订立标准合同的，应当重新备案。补充或者重新备案的材料查验时间为 10 至 15 个工作日。

第六章 数据出境保护认证专项法律服务

第二十二条 律师应当协助数据处理者在申请认证向境外提供个人信息前，按照法律、行政法规的规定履行数据出境的单独告知并取

得个人同意等义务，定期进行年度个人信息保护影响评估并形成报告。律师可参考 GB/T 46068-2025《数据安全 个人信息跨境处理活动安全认证要求》的要求协助数据处理者规范自身个人信息跨境处理活动。

第二十三条 个人信息处理者通过认证方式向境外提供个人信息的，应当向专业认证机构申请个人信息出境认证。

第二十四条 中华人民共和国境外的个人信息处理者申请个人信息出境认证的，应当由其在境内设立的专门机构或者指定代表协助进行申请。跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动可由境内一方申请认证，并承担法律责任。

第二十五条 认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

如发现认证委托人、个人信息处理者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。

第二十六条 认证证书的有效期为 3 年。证书到期需继续使用的，个人信息处理者应当在有效期届满前 6 个月提出认证申请。

第二十七条 认证证书有效期内，若获得认证的个人信息处理者名称、注册地址，或认证要求、认证范围等发生变化时，认证委托人应当向认证机构提出变更委托。认证机构根据变更的内容，对变更委托资料进行评价，确定是否可以批准变更。如需进行技术验证和/或现场审核，还应当在批准变更前进行技术验证和/或现场审核。

第二十八条 当获得认证的个人信息处理者不再符合认证要求时，认证机构应当及时对认证证书予以暂停直至撤销。认证委托人在认证证书有效期内可申请认证证书暂停、注销。

第七章 数据出境合规管理体系建设

第二十九条 律师应当协助数据处理器建立分类分级管理制度、个人信息安全管理制度、数据安全管理制度、数据安全事件应急预案等数据出境合规管理制度。

第三十条 数据分类分级保护制度。律师应协助数据处理器准确识别境内运营中收集和产生的重要数据与个人信息，明确不同级别数据的出境管控要求。例如，对于重要数据，部分行业、领域数据分类分级标准规范和重要数据识别申报规则已经公开发布，如工业领域的《工业领域重要数据识别指南》、电信领域的《电信领域重要数据识别指南》、自然资源领域的《地理信息数据分类分级工作指南(试行)》、统计领域的《统计数据安全管理办法》等，未被相关部门告知或公开发布为重要数据的，无需作为重要数据申报数据出境安全评估。

第三十一条 个人信息安全管理制度。律师应协助数据处理器履行个人信息出境的告知义务、完善单独同意获取流程、完成个人信息保护影响评估要求，制定个人信息出境处理的内部管理制度和操作规程，明确个人信息保护负责人及其职责，合理确定个人信息处理的操作权限。

第三十二条 数据安全管理制度。律师应协助数据处理器履行数据安全保护义务，依法建立健全全流程数据安全管理制度和操作规程，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据出境安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第三十三条 数据安全事件应急预案。律师应协助数据处理者建立健全网络数据安全事件应急预案，发生网络数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。

发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；（三）个人信息处理者的联系方式。

第八章 律师从事数据出境合规法律服务业务的执业规范与风险防范

第三十四条 律师从事数据出境合规法律服务业务应遵守如下执业规范：

（一）律师从事数据出境合规法律服务要严格依据《中华人民共和国律师法》《律师职业道德和执业纪律规范》等规定，恪守行业规范、职业操守和职业道德；

（二）律师从事数据出境法律服务应充分了解《数据出境安全评估办法》《个人信息出境标准合同办法》《个人信息保护认证实施规则》等数据出境相关法律法规及国家网信部门发布的申报指南、技术标准等，以及出境目的地相关的法律法规；

（三）律师从事数据出境法律服务应充分了解客户的业务模式、数据类型、出境场景、境外接收方资质、数据处理规模及频次，审查其数据出境合法性基础，避免法律服务与业务实际脱节；

（四）律师为跨国企业集团、关键信息基础设施运营者提供数据出境合规服务时，应充分了解其全球数据治理架构、境外服务器分布、

集团内部数据控制关系，协助其建立符合中国监管要求的数据出境管控机制；

（五）律师协助客户完成数据出境安全评估、标准合同备案、认证申请及监管检查时，应协助客户查明违规事实、识别责任主体、发现合规管理漏洞；

（六）律师从事数据出境法律服务应当实事求是，不得伪造个人信息保护影响评估报告、虚构数据出境场景、协助客户瞒报重要数据或大规模个人信息出境数量等，杜绝发生任何协助客户逃避监管的不当行为；

（七）律师从事数据出境法律服务要严守保密义务，除按照与客户签订的合同履行义务外，还必须对其提供法律服务过程中接触、了解到的国家秘密、商业秘密、个人信息、未公开的评估报告、系统账号密码及数据映射表负有保密义务，项目结束后应及时销毁相关敏感材料；

（八）律师从事数据出境法律服务要防止利益冲突，不得利用服务中获取的数据资产信息为自身或关联方谋取不正当利益，并积极向客户进行解释或说明；

（九）律师从事数据出境法律服务应当严格按照《中华人民共和国律师法》《律师职业道德和执业纪律规范》及《律师执业行为规范》等行业规则，公平开展同业竞争，防止出现以不正当手段承揽数据出境业务、压低收费标准扰乱市场秩序、诋毁同行专业能力等行为，共同维护数据合规法律服务行业的健康发展。

第三十五条 律师从事数据出境法律服务业务应防范如下行政法律风险：

（一）数据出境法律服务业务属于法律服务的专项领域，虽具有较强的专业性和监管特殊性，但律师开展相关业务时，仍需严格遵循

律师执业行为规范及执业纪律要求，明确自身执业边界，不得超出执业范围提供服务，确保执业行为的合法性与合规性。

（二）针对数据出境业务涉及监管部门多、合规审查标准严、法律依据层级多且更新快、跨境因素复杂等特点，开展服务时应重点关注利益冲突排查、收案收费规范、勤勉尽责履职、数据安全与保密等核心执业要求，严格防范因违反《律师协会会员违规行为处分规则（试行）》《律师和律师事务所违法行为处罚办法》以及《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规、监管规定，而被采取行业惩戒或行政处罚。

第三十六条 律师从事数据出境法律服务业务应防范如下民事法律风险：

（一）律师承接数据出境法律服务业务，必须由律师事务所与客户签订书面委托合同，明确委托事项、服务范围、双方权利义务、收费标准及民事责任划分等核心内容。

（二）为有效防范民事责任风险，应组建专业化的数据出境法律服务团队，强化专业能力建设，系统研习数据出境相关法律法规、部门规章、规范性文件及行业标准，深入掌握不同行业、不同类型数据出境的监管要求，同时加强对跨境数据流动域外规则的研究，避免因专业能力不足导致服务成果存在缺陷，进而引发民事纠纷。对涉及国家安全、公共利益的重要数据或大规模敏感个人信息出境项目，应审慎评估自身专业能力和风险承受能力，必要时建议客户聘请技术专家协同提供服务。

第三十七条 律师从事数据出境法律服务业务应防范如下刑事法律风险：

（一）律师在提供数据出境法律服务过程中，若发现客户存在规避数据出境监管、违规传输敏感数据/核心数据、泄露国家秘密或危害

国家安全等违法犯罪意图或行为，应坚决予以拒绝，明确阐明拒绝理由及相应法律后果，同时留存相关记录，避免陷入违法犯罪链条。

（二）律师在协助客户办理数据出境安全评估、标准合同签订备案、涉案数据处理者数据合规整改等业务时，应严守执业底线，严格按照法定程序和监管要求开展工作，坚决抵制伪造数据出境材料、协助客户隐瞒违规事实、毁灭相关证据、泄露服务过程中获取的国家秘密、商业秘密或个人敏感信息等违法犯罪行为，在助力客户防范数据出境刑事风险的同时，切实防范自身涉嫌危害国家数据安全、侵犯公民个人信息等刑事责任风险。

第九章 附则

第三十八条 本指引旨在向律师提供办理数据出境法律业务的一般性实务操作指引，而非强制性规定或执业服务标准，亦不作为律师出具法律意见书、专项报告的法律依据，仅供律师执业实践参考使用。

第三十九条 本指引发布于 2026 年 5 月。

第四十条 本指引由广州市律师协会数据与数字经济专业委员会解释。