附件

律师办理个人信息保护影响评估业务指引

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

前　言

数字经济已成为推动经济社会高质量发展的核心引擎，个人信息作为数字时代的关键生产要素，其安全保护与合规利用既是保障公民基本权益的法治基石，也是激发数据要素活力的重要前提。为深入贯彻落实习近平法治思想，践行“网络安全为人民，网络安全靠人民”的根本理念，精准对接习近平总书记关于“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，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系”的重要指示精神，切实响应“充分发挥海量数据和丰富应用场景优势，促进数字技术和实体经济深度融合”的发展要求，特制定本指引。

当前，我国正迈向“十五五”规划开局的关键阶段，《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》（以下简称：“十五五”规划建议）在“深入推进数字中国建设”部分明确提出，要“健全数据要素基础制度，建设开放共享安全的全国一体化数据市场，深化数据资源开发利用”，将数据要素提升为驱动高质量发展的核心生产要素。这一战略部署在释放数据价值的同时，也对个人信息保护提出了系统性挑战：全国一体化数据市场的构建需打破“数据孤岛”，而跨主体、跨领域的数据流通极易引发隐私泄露、权益受损等风险，成为数据供给的主要制约因素；“全面实施‘人工智能 +’行动”推动数智技术与千行百业深度融合，但人工智能训练数据采集的合规性、算法决策的透明性以及用户权利响应的及时性，已成为个人信息保护的全新痛点。在此背景下，个人信息保护影响评估（PIA）

不仅是《中华人民共和国个人信息保护法》规定的法定环节，更是落实“十五五”规划建议“加强人工智能治理，完善相关法律法规、政策制度”要求的关键抓手，为数据要素安全流通提供“合规通行证”。

在政策衔接层面，广东省已出台《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》，明确从数据产权、流通交易等七方面提出20条举措，力争到2030年建成多元繁荣的数据要素市场生态体系；广州市同步施行《广州市数据条例》，通过构建数据要素统计核算指标体系、探索数据资产化路径，依托粤港澳大湾区核心城市定位打造数据要素流通高地。律师作为法治建设的重要力量，开展个人信息保护影响评估（PIA）业务既是落实《律师事务所管理办法》中“坚持和加强党对律师工作的全面领导”要求的具体实践，更是广州市律师协会引领全市律师行业服务广州数字经济创新发展、助力粤港澳大湾区数据要素市场协同建设的专业担当。

本指引立足《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》等法律法规，结合律师执业特点与个人信息保护影响评估实务需求，系统梳理评估概述、主体与触发条件、核心要点、实施流程四大基础模块，重点聚焦敏感个人信息处理、自动化决策、数据跨境流动等典型场景的专项评估方法，旨在为律师提供体系化、标准化的执业指引，推动个人信息保护影响评估业务专业化发展，助力数据处理者构建“全流程、全链条”的个人信息保护体系，在保障个人信息权益与促进数据合规利用之间实现动态平衡，为国家及粤穗地区数字经济、新经济健康发展提供坚实法治服务。

目 录

一、个人信息保护影响评估概述

（一）个人信息保护影响评估的涵义

我国《个人信息保护法》未明确“个人信息保护影响评估”的定义，在此之前出台的一些技术性规范中，已有与此类似的“个人信息安全影响评估”的概念界定。我国早在 2017 年发布的国家标准《信息安全技术 个人信息安全规范》（GB/T 35273-2017）中就提出“个人信息安全影响评估”（第 3.8 条），2020 年修正时予以保留。2020 年发布的国家标准《信息安全技术 个人信息安全影响评估指南》（GB/T 39335-2020，下文简称《评估指南》）全面规定了“个人信息安全影响评估”，涉及评估原理、评估实施流程等事项。2020 年发布的《个人信息保护法（草案）》第五十四条使用了“风险评估”[1]，2021 年最终通过的版本改为“个人信息保护影响评估”[2]。

我国的个人信息保护影响评估制度源于对欧盟数据保护影响评估制度的借鉴，体现了基于风险路径的个人信息保护模式。《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）在隐私影响评估（Privacy Impact Assessment，简称 PIA）的基础上，确立了数据保护影响评估制度（Data Protection Impact Assessment，简称 DPIA）。以知情同意为基本路径的个人信息保护逐渐流于形式，欧盟数据保护影响评估制度拓展了传统的数据保护模式，侧重于事前的预防方法，通过对数据保护风险的评估和管理，转向了以风险管理为路

[1] 《中华人民共和国个人信息保护法（草案）》全国人大常委会，2020 年 10 月 21 日。
[2] 刘权：论个人信息保护影响评估——以《个人信息保护法》第 55、56 条为中心，上海交通大学学报（哲学社会科学版）2022 年 5 期。

径的新型数据保护模式。通过识别、分析和归类风险，数据保护影响评估可以消除或减轻隐私和个人数据风险。数据保护影响评估的规范基础在于保护公民的基本权利与自由。数据保护影响评估迫使数据处理者“识别、评估并最终管理数据处理给权利和自由带来的高风险”。数据保护影响评估旨在将风险评估的一般逻辑融入整个数据保护法之中，从而将现有风险的系统化梳理与阐明作为评估逻辑。**我国个人信息保护影响评估促使个人信息保护模式，从事后监管向基于风险管理为主的模式转变[3]。**

结合我国相关规范中“个人信息安全影响评估”的定义以及域外个人信息保护影响评估的概念，并考虑我国实践状况，本指引认为，个人信息保护影响评估的概念可以界定为个人信息处理者对其个人信息处理活动可能对个人权益带来的风险、影响以及所采取的保护措施是否有效合规而进行的**系统性评估过程**。个人信息保护影响评估作为一种**预防性合规工具**，旨在帮助组织识别、评估和降低个人信息处理过程中的隐私风险，确保数据处理活动符合法律法规要求，并保障个人信息主体的合法权益。

（二）个人信息保护影响评估的法律性质及法律价值

从法律性质上看，个人信息保护影响评估是我国《个人信息保护法》确立的一项**强制性合规义务**，特定情形下的个人信息处理者必须在处理个人信息前进行此项评估。个人信息保护影响评估的核心目的包括三个方面：

[3] 刘权：论个人信息保护影响评估——以《个人信息保护法》第 55、56 条为中心，上海交通大学学报（哲学社会科学版）2022 年 5 期。

一是**确保合规性**，《个人信息保护法》第56条规定的首要评估内容是评估个人信息处理是否符合合法、正当、必要原则，属于合规评估。合法、正当、必要原则是《个人信息保护法》《民法典》《网络安全法》等确立的个人信息处理基本原则，是个人信息保护规则体系的灵魂;

二是**风险管理**，识别和评估个人信息处理活动可能对个人权益造成的风险，并采取相应措施降低风险；个人信息保护影响评估是一种有效的风险评估工具，它通过提前识别个人信息处理中的风险和潜在不利影响，帮助优化业务流程和采取预防措施。《个人信息保护法》第56条规定的第2项评估内容即评估“对个人权益的影响及安全风险”，属于风险评估，有利于发现风险的类型与大小；第3项评估内容即评估“所采取的保护措施是否合法、有效并与风险程度相适应”，这种评估不是为了消除所有风险，而是让处理者承担更多责任，有助于识别和降低处理风险，实现风险可控，高效利用个人信息。

三是依法减轻或免除违法处理个人信息的责任。通过有效实施个人信息保护影响评估，不仅可以增强个人信息处理者的风险管理能力，对外展示保护个人信息的努力，有利于提升企业声誉，而且还有助于依法减轻或免除因**违法处理**个人信息所应承担的责任。对于民事责任，《个人信息保护法》第六十九条确立了个人信息侵权的过错推定责任，即个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。对于行政责任，《个人信息保护法》

没有确立归责原则，一般应适用《行政处罚法》确立的过错推定原则，即当事人有证据足以证明没有主观过错的应当不予行政处罚。如果个人信息处理者能证明自己过错较小或没有过错，相应的民事责任或行政责任应当依法减轻或免除。个人信息保护影响评估的法律价值主要体现在其为组织提供了**履行尽职免责义务**的证据。根据《个人信息保护法》第五十六条第二款规定，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，相关记录在监管调查、行政处罚或民事诉讼中可以作为证明个人信息处理者已尽到法定义务的重要证据。

表：个人信息保护影响评估与其他相关评估的区别

评估类型	法律依据	评估重点	适用场景
个人信息保护影响评估	《个人信息保护法》	个人信息处理活动对个人权益的影响	处理敏感个人信息、自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息等
数据安全风险评估	《数据安全法》第三十条	数据处理活动对国家安全的威胁	重要数据处理
数据出境安全评估及数据出境风险自评估	《数据出境安全评估办法》第四条	数据出境安全评估是针对数据跨境流动的国家安全、公共利益风	数据跨境传输

		险，是国家监管的强制性评估；数据出境风险自评估是数据出境安全评估的前置程序，由企业自行开展，侧重自身能力与出境活动的适配性	
网络安全等级保护测评	《网络安全法》	网络系统的安全保护能力	网络运营者的信息系统
个人信息保护认证	《个人信息保护法》 《个人信息出境认证办法》（2026年1月1日施行）	个人信息处理活动的整体合规性	适用于符合条件的个人信息处理者向境外提供个人信息，或其他个人信息处理者提升用户信任的场景

二、个人信息保护影响评估的评估主体及触发条件

（一）评估主体

1.个人信息处理者之私权主体。根据《个人信息保护法》第五十五条规定，个人信息处理者是法定的评估主体。《个人信息保护法》第七十三条规定，个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。因此，个人信息处理者包括组织、个人。组织包括法人或非法人组织，如企业、事业

单位、社会团体等。个人则主要指自然人，当其在个人信息处理活动中具备自主决定处理目的与方式的能力时，也会成为个人信息保护影响评估的主体。例如一些独立的自由职业者，若其业务涉及对他人个人信息的处理，就需要按照法律规定履行评估义务。

2.个人信息处理者之公权主体，如国家机关。虽然《个人信息保护法》未明确提及国家机关是否适用个人信息保护影响评估，但根据《个人信息保护法》第三十三条“国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。”之规定，以及学界和实践普遍认为，作为重要的合规评估和风险评估机制，个人信息保护影响评估应同样适用于国家机关[4][5][6]，否则对个人信息的保护就是不全面的。数字时代的国家机关既是个人信息处理者，也是个人信息保护监管者。作为个人信息处理者的国家机关，应当同作为私主体的个人信息处理者一样，有效履行个人信息保护影响评估义务。对此，个人信息处理活动也不限于单纯的作为平等主体的自然人、法人和非法人组织之间，国家机关的个人信息处理行为，亦应受到约束，当国家机关作为个人信息处理者时，也应履行评估义务。

3.评估主体自评制度。《个人信息保护法》第五十五条仅规定了个人信息处理者的自评制度，强调个人信息处理者对自身处理活动的主动合规审查。参考《评估指南》4.4 评估责任主体，个人信息

[4] 刘 权：论个人信息保护影响评估———以《个人信息保护法》第 55、56 条为中心，上海交通大学学报（哲学社会科学版 ），2022 年 10 月第 30 卷（总 147 期）.
[5] 李 芹：基于风险的模式下个人信息保护影响评估制度的体系化建构，浙江学刊，2024 年 5 期。
[6] 程 啸：《个人信息保护法理解与适用》，中国法制出版社，2021-09-01，（第 106 页）。

处理者可以指定评估的责任部门或责任人员，由其负责评估工作流程的制定、实施、改进，并对评估工作结果的质量负责。该责任部门或人员具有独立性，不受到被评估方的影响。通常，组织内部牵头执行评估工作的部门为法务部门、合规部门或信息安全部门。同时，个人信息处理者内部的责任部门可根据部门的具体能力配备情况，选择自行开展评估工作，或聘请外部独立第三方来承担具体的个人信息保护影响评估工作。因此，组织对于可能产生高风险的个人信息处理活动可聘请外部第三方如具备丰富经验及专业性的律师事务所和信息数据安全专家共同作为评估参与人员[7]。

（二）触发条件分析

1、法定评估场景

《个人信息保护法》第五十五条列举了以下五种个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录的情形：处理敏感个人信息；利用个人信息进行自动化决策；委托处理、对外提供、公开个人信息以及向境外提供个人信息；其他对个人权益有重大影响的个人信息处理活动。上述列举的五种情形，现逐一识别分析如下：

（1）处理敏感个人信息

因处理敏感个人信息而触发个人信息保护影响评估的，首先需对敏感个人信息进行识别，可以结合法律规定、国家标准、行业标准、地方规则及团体指南等文件进行识别判断。**法律层面：**根据

[7] 董新义、袁心悦：个人信息保护影响评估的程序法规制，江汉大学学报（社会科学版）2023 年 1 期。

《个人信息保护法》第二十八条，敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。这类信息一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。**国家标准层面：**《数据安全技术 敏感个人信息处理安全要求》（GB/T 45574-2025）不仅确立了敏感个人信息识别和界定规则，更规定了敏感个人信息处理通用安全要求和敏感个人信息处理特殊安全要求。适用于个人信息处理者开展敏感个人信息处理活动，也适用于监管部门和第三方评估机构对敏感个人信息处理活动进行监督、管理和评估。在进行敏感个人信息识别与界定时可以根据该文件的识别和界定规则以及参考附录 A(规范性)敏感个人信息类别进行判断。此外，《信息安全技术 个人信息安全规范》（GB/T 35273-2020）也细化了敏感个人信息的定义、判定规则与示例。全国网络安全标准化技术委员会制定的《网络安全标准实践指南——敏感个人信息识别指南》（TC260-PG-20244A）给出了敏感个人信息识别规则以及常见敏感个人信息类别和示例，可用于指导识别敏感个人信息，也可为敏感个人信息处理和保护工作提供参考。**行业层面：**针对金融、医疗等垂直领域，已出台相应的行业标准，可以参考行业标准辅助识别判断敏感个人信息的内容。如《个人金融信息保护技术规范》（JR/T 0171-2020）、《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）。完成对敏感个人信息的识别和判定后，个人信息处理者在处理此类信息前，必须进行个人信息

保护影响评估，分析处理目的的必要性、安全措施的可靠性以及可能对个人权益造成的影响。

（2）利用个人信息进行自动化决策

根据《中华人民共和国个人信息保护法》第七十三条，自动化决策是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。根据《数据安全技术 基于个人信息的自动化决策安全要求》（GB/T 45392-2025），自动化决策可进一步分解为特征生成和决策两个过程。特征生成的过程包括特征提取、特征选择、特征计算和特征输出等步骤。决策是在特征生成所提供的个人特征信息的参与下，对个人采取具体行动。决策活动可不同程度人工参与，也可无需人工参与。如果企业利用自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。在这类场景下，个人信息保护影响评估需要重点评估决策的透明度和结果公平、公正性，是否对个人在交易价格等交易条件上实行不合理的差别待遇。

（3）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息

当个人信息处理者将个人信息委托给第三方处理、向其他个人信息处理者提供个人信息或者公开个人信息时，应当事前进行个人

信息保护影响评估。这类评估需要重点关注接收方的安全保障能力、合同约束的有效性以及再转移限制的充分性。例如，在委托处理情形下，根据《个人信息保护法》第二十一条，委托方应当与受托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。再如，在向其他个人信息处理者提供其处理的个人信息情形下，根据《个人信息保护法》第二十三条，个人信息处理者应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照该法规定重新取得个人同意。在公开个人信息情形下，根据《个人信息保护法》第二十五条，个人信息处理者应取得个人单独同意为前提。

（4）向境外提供个人信息

根据《个人信息保护法》第三十八条，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：（一）通过国家网信部门组织的安全评估；（二）经专业机构进行个人信息保护认证；（三）按照国家网信部门制定的标准合同与境外接收方订立合同；（四）法律、行政法规或者国家网信部门规定的其他条件。在跨境传输场景下，根据《数据安全技术 个人信息跨境处理活动安全认证要求》（GB/T 46068-2025）有关要求，个人信息保护影响评估需要重点评估：（1）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；（2）跨境处理个人信息的规模、范围、种类和敏感程度,个人信息跨境处理可能对个人信息权益带来的风险；（3）个人信息跨境处理存在泄露、损毁、篡改和滥用等的风险,个人信息生体维护个人信息权益的渠道是否畅通；（4）境外接收方所在国家或者地区的个人信息保护政策法规对履行个人信息保护义务和保障个人信息权益的影响、境外接收方的网络安全环境、个人信息保护能力等因素。

（5）其他对个人权益有重大影响的个人信息处理活动

该条款作为兜底性条款，可以看出，我国个人信息保护影响评估的适用范围为对个人权益有重大影响的个人信息处理活动。换言之，处理活动是否对个人权益具有重大影响，是判断是否需要进行个人信息保护影响评估的标准。由于我国目前没有明确界定对个人权益产生重大影响的标准，且学界认为我国的个人信息保护影响评估适用范围过于宽泛，缺乏必要的限定条件，对此，个人信息处理者在判断其个人信息处理行为是否属于对个人权益有重大影响而依法应进行个人信息保护影响评估时，可以结合我国对欧盟数据保护影响评估制度的借鉴路径，参考《通用数据保护条例》及《数据保护影响评估和确定处理是否“可能导致高风险”的指南》可知，其数据保护影响评估适用于“高风险”行为[8]，同时，结合《评估指南》关于评估必要性分析，评估既可用于“合规差距评估”，也可

[8] 刘权：论个人信息保护影响评估——以《个人信息保护法》第 55、56 条为中心，上海交通大学学报（哲学社会科学版）2022 年 5 期。

以用于合规至上、进一步提升自身风险管理水平和安全水平的目的，因此，基于风险评估目的出发，可以选取可能对个人合法权益产生高风险的个人信息处理活动进行评估，具体高风险个人信息处理活动可以参考《信息安全技术 个人信息安全影响评估指南》（GB/T 39335-2020）附录 B 高风险的个人信息处理活动及场景示例。

2、尽责性评估场景

除了《个人信息保护法》明确规定的 4 种情形以及《评估指南》中罗列的高风险个人信息处理活动外，国家标准《信息安全技术 个人信息安全规范》（GB/T 35273-2020）11.4 明确在以下场景中应进行个人信息保护影响评估:

（1）在产品或服务发布前或业务功能发生重大变化时：其个人信息处理活动尚未进入实际运行，但已形成初步的处理逻辑。此时处理者开展个人信息保护影响评估，可提前识别潜在风险，如过度收集个人信息、处理目的不明确，避免产品上线后或业务功能修改后因合规问题引发法律纠纷或声誉损失。此场景下，评估重点包括处理目的与合法性基础、数据全生命周期合规性、个人权益影响等。

（2）法律法规有新的要求时：由于法律法规的更新会改变个人信息处理的合规边界，此时开展个人信息保护影响评估，可确保处理活动与最新法律要求一致，避免“合规滞后”风险。此场景下，评估重点包括对新旧法规差异分析、根据新法的要求对现有处理活动的合规性验证、对不符合新法规要求的处理活动制定整改措施等。

（3）业务模式、信息系统、运行环境发生重大变更时：业务模式变更可能导致个人信息处理目的、范围变化；信息系统变更可能引入新的安全漏洞；运行环境变更可能改变数据的存储与传输方式。这些变更都可能导致原有的安全措施失效，需通过个人信息保护影响评估重新评估风险。此场景下，评估重点包括分析变更对个人信息处理的影响，如业务模式变更是否改变个人信息的“收集范围、使用方式”、信息系统变更是否会存在新的安全漏洞、运行环境变更是否改变了数据的存储与传输方式等，以评估新环境下的安全风险。

（4）发生重大个人信息安全事件时：重大个人信息安全事件暴露了现有处理活动的缺陷。此时开展个人信息保护影响评估，可分析事件根源，并验证整改措施的有效性，避免类似事件再次发生。此场景下，评估重点为事件原因分析（涵盖技术、管理及第三方等方面）、整改措施的有效性验证（验证技术、管理及第三方等的整改措施是否有效），以及评估是否存在其他风险并制定对应的整改措施。

上述情形表明个人信息保护影响评估不仅是一种被动的合规义务，也应当作为组织主动风险管理的重要手段。在尽责性评估场景下，组织需主动识别并评估可能影响个人信息权益的各类因素。这包括但不限于对新技术应用的预先审查，例如人工智能算法在处理个人信息时可能引入的偏见或歧视风险；对第三方服务提供商的安全管理能力评估，确保其符合组织的信息安全标准；以及对内部员

工操作流程的定期审计，防止因人为疏忽导致的数据泄露。通过这些主动措施，组织能够提前发现潜在风险，并采取针对性措施加以防范，从而有效提升个人信息保护水平。

三、评估要点分析

（一）处理目的、处理方式等合法性、正当性、必要性审查

开展个人信息保护影响评估时，首先需要对个人信息的处理目的、处理方式等进行**合法性、正当性、必要性审查**。这一审查是检验个人信息处理是否合规、个人信息保护影响评估的基础，直接决定了个人信息处理活动是否符合法律法规的核心要求。这里所谓的个人信息的处理目的、处理方式，是指《个人信息保护法》第五十五条所列举的应当进行个人信息保护影响评估的个人信息处理活动，即处理敏感个人信息；利用个人信息进行自动化决策；委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；向境外提供个人信息；其他对个人权益有重大影响的个人信息处理活动的处理目的、处理方式。**合法、正当、必要是《个人信息保护法》《网络安全法》《民法典》等法律所明文规定的个人信息处理活动应当遵循的基本原则。个人信息处理者在进行个人信息保护影响评估时，首先要对个人信息的处理目的、处理方式等是否合法、正当、必要作出评估。**如果不合法或者不正当、不必要，则个

人信息处理者不应当进行个人信息处理活动，否则个人信息处理者就属于故意实施违法处理活动，需要承担相应的法律责任[9]。

1、合法性基础

合法性审查首先需评估个人信息处理活动是否具备明确的合法性基础。根据《个人信息保护法》第十三条，处理个人信息的合法基础包括：取得个人同意；为订立或履行合同所必需；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人力资源管理所必需；为履行法定职责或法定义务所必需；为应对突发公共卫生事件或紧急情况下保护生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等行为；处理已公开的个人信息；法律、行政法规规定的其他情形。据此，可以将依法处理个人信息的事由区分为两大类[10]：一是基于个人同意处理个人信息，此种情形为依法处理个人信息的一般情形，也是最为常见的情形。二是基于法律规定处理个人信息。此种属于依法处理个人信息的例外情形，其适用应当符合法律规定的条件。关于个人信息处理的合法性审查本指引根据处理个人信息的事由区分的两大类进行论述：

（1）**基于个人同意处理个人信息：**关于个人同意，《个人信息保护法》第十四条对个人信息处理情形下的个人同意作出了明确规定。依据该条第一款规定，个人同意包括一般要件与特别要件。所谓一般要件，是指一般情形下个人作出同意应当具备的条件，具体包括个人

[9] 程啸：《个人信息保护法理解与适用》，中国法制出版社，2021 年 9 月 1 日，第 635 页。
[10] 王叶刚：《个人信息处理行为合法性研究》（法律科学文库；“十三五”国家重点出版物出版规划项目），中国人民大学出版社，2024-07-31，第 47 页。

应当对个人信息处理行为充分知情、个人应当自愿同意以及个人应当明确同意。所谓特别要件，是指在法律、行政法规对个人作出同意的形式等方面作出特别规定时，个人作出同意应当具备的条件，包括个人的单独同意与书面同意。此外，依据该条第二款规定，个人信息处理行为的相关内容发生变更时应当重新取得个人同意。[11]因此，在评估基于个人同意处理个人信息的合法性时，需要根据《个人信息保护法》对个人同意这一个人信息处理的基本规则（包括个人信息处理行为的合法性、个人撤回同意、个人信息共享、个人单独同意、个人书面同意、个人信息公开、已公开个人信息的处理、个人信息跨境流动、敏感个人信息的处理、未成年人个人信息保护、个人信息的删除等内容）确定是否满足个人同意的一般要件和特别要件。实践中可以结合并参考《信息安全技术 个人信息处理中告知和同意的实施指南》（GB/T 42574-2023）进行评估。

（2）基于法律规定处理个人信息：包括为订立或履行合同所必需；处理个人信息为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人力资源管理所必需；为履行法定职责或法定义务所必需；为应对突发公共卫生事件或紧急情况下保护生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等行为；处理已公开的个人信息；法律、行政法规规定的其他情形。在评估上述情形下的个人信息处理活动合法性时，应针对不同情形下的个人信息处

[11] 王叶刚：《个人信息处理行为合法性研究》（法律科学文库；“十三五”国家重点出版物出版规划项目），中国人民大学出版社，2024-07-31。

理规则进行评估。**本指引主要从私权主体（企业等组织）常见的基于法律规定处理个人信息情形进行分析，具体包括：**

① **为订立或履行合同所必需：**依据《民法典》《个人信息保护法》的规定，其适用应当具备三个条件：一是个人作为合同一方当事人，如果个人一方并非合同当事人，而是合同关系涉及的第三人，即便处理其个人信息是合同订立或者履行所必需的，个人信息处理者处理相关的个人信息也应当依法取得个人的同意，否则将构成对个人信息的侵害。二是处理相关的个人信息是订立或者履行合同所必需的，在司法实践中，在“罗某1诉北京大生知行科技有限公司隐私权、个人信息保护纠纷案”中，法院认为，为订立、履行作为一方当事人的合同所必需是依法处理个人信息的合法性事由之一，在判断个人信息处理者处理个人信息是否属于订立、履行合同所必需时，需要结合相关行业规范和产品功能设置等具体判断。三是个人信息处理者处理相关的个人信息应当符合法律规定。一方面应当遵循个人信息处理的原则，如遵循公开、透明原则，“公开个人信息处理规则，明示处理的目的、方式和范围”。另一方面，个人信息处理者在处理相关的个人信息时，应当遵循个人信息处理的具体规则，如“保存期限应当为实现处理目的所必要的最短时间”。

② **处理个人信息为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人力资源管理所必需：**a.关于按照依法制定的劳动规章制度实施人力资源管理所必需。目前，我国现行立法尚无专门规定

用人单位在工作场所实施监控并处理劳动者个人信息的规则。如果用人单位基于其劳动规章制度对劳动者进行监控并进行个人信息处理行为，依据《个人信息保护法》第 13 条第 1 款第 2 项规定，包含劳动者个人信息处理规则的劳动规章制度必须“依法制定”，如果劳动规章制度本身不具有合法性，其也难以成为用人单位处理劳动者个人信息的合法性基础。此外，还需对劳动规章制度本身的合法性进行审查。具体判断劳动规章制度中的劳动者管理条款是否有效时，需要考虑用人单位管理的具体方式、管理的场所、管理行为所要实现的目的、管理行为对劳动者隐私权、个人信息权益限制的程度等因素，综合予以判断。b.关于依法签订的集体合同实施人力资源管理所必需：用人单位在此种情形下依法处理劳动者个人信息应当具备以下条件：一是用人单位必须依据依法签订的集体合同处理个人信息。该集体合同应当是依法签订的，如该集体合同本身不成立，或者无效，则用人单位不得主张将其作为依法处理劳动者个人信息的依据，按照我国《劳动合同法》关于集体合同的签订主体与签订程序作出的规定进行审查；二是用人单位处理个人信息必须是实施人力资源管理所必需。虽然人力资源管理的概念较为宽泛，但用人单位在依据《个人信息保护法》第 13 条第 1 款第 2 项规定处理劳动者个人信息时，必须证明该处理行为与人力资源管理相关，否则难以依据该规则处理劳动者的个人信息。

③ **依法处理已公开的个人信息：**首先，应明确已公开个人信息的内涵和界定标准，即如何识别哪些个人信息属于已公开的个人

信息。其次，根据《民法典》第一千零三十六条规定及《个人信息保护法》第十三条和第二十七条关于已公开个人信息处理规则的规定进行评估。

2、正当性审查

评估个人信息处理目的是否明确、合理，处理行为是否公平、透明。处理目的应当具有明确性和合理性，避免模糊不清或过于宽泛的目的描述。处理方式应当遵循公开透明原则，个人信息处理者应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理者的名称或者姓名和联系方式、处理目的、处理方式、处理的个人信息种类、保存期限、个人行使权利的方式和程序等事项。律师需要审查隐私政策、用户协议等告知文件的内容完整性和呈现方式，确保个人能够充分理解其个人信息将被如何处理。

3、必要性审查

根据《个人信息保护法》第5条，处理个人信息应当遵循必要原则，因此，需要评估个人信息处理活动是否遵循**必要性原则**。目前，我国法律中尚未明确“必要性原则”的法律定义和具体的适用标准，但在不同的法律法规、标准等文件中均有关于个人信息处理的“必要性原则”相关规定，以《个人信息保护法》的规定为例，该法第五条（必要原则）、第九条（必要措施）、第十九条（必要最短时间）、第二十八条(处理敏感个人信息需具备充分的必要性)、第三十条(处理敏感个人信息时向个人告知处理的必要性)、第三十八条(个人信息跨境提供时采取必要措施)、第四十七条(处理目的不再必要时个

人信息处理者应删除或个人有权请求删除，以及未能删除情况下应采取必要措施）、第五十六条（个人信息保护影响评估要包括处理目的、处理方式的必要性）、第五十九条（委托处理下的受托人应采取必要措施）等规定识别“必要性”。结合《个人信息保护法》及《信息安全技术 个人信息安全规范》（GB/T 35273-2020）关于“必要性原则”的规定，应限定于实现个人信息的处理目的、处理方式的最小范围中。总结而言[12]，“必要性原则”在个人信息处理中的具体要求主要有以下几点：（1）收集的个人信息应具有明确、合理、具体的个人信息处理目的；（2）个人信息处理应当与拟实现的信息处理目的直接相关；（3）个人信息处理应当限于实现处理目的之最小范围；（4）个人信息处理应当采取对个人权益影响最小的方式；（5）个人信息的保存期限应当限于实现处理目的的最短期限。以上五点要求主要包括三大原则，即“目的明确原则”、“最小化原则”以及“存储期限限制原则”。主要分析如下：

（1）“目的明确原则”：如前文正当性所述，《个人信息保护法》第六条要求处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。上述规定明确“与处理目的直接相关”原则，即没有该等个人信息的参与，产品或服务的功能就无法实现，并且在个人信息处理活动须围绕初始目的展开，在初始目的实现、初始目的无法实现或初始目的变更等情况发生时，个人信息处理者均应该采取相应措施。

[12] 张丹 夏星悦：《研究 | 方寸之间，以“度”为尺—个人信息处理“必要性原则”之解析与实务建议》

（2）“最小化原则”：要求处理个人信息应当采取对个人权益影响最小的方式，并限于实现处理目的的最小范围，不得过度收集个人信息。

（3）“存储期限限制原则”：《个人信息保护法》第十九条规定：“除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。”即：如果存在法律、行政法规对个人信息保存期限有规定的情况，该等规定优先适用；若无相关规定，则个人信息处理者需要基于最小必要原则确定相应的个人信息保存期限。因此，应根据既有法律法规涉及个人信息保存期限的相关规定确定所处理个人信息的保存期限。对于未有法律、行政法规对保存期限作出规定的个人信息，其保存期限的确定则需要结合具体的处理目的来考虑。实践中，个人信息处理者应当根据实际的个人信息处理情况，通过对既有各类信息系统中数据资产的充分摸排，逐一厘清为实现各种个人信息处理目的，所需要保存个人信息的必要期限，形成完整的个人信息保存期限表。

（二）个人权益影响及安全风险分析

个人信息保护影响评估的第二项核心内容是分析个人信息处理活动对个人权益的影响及安全风险。这一分析旨在识别和评估处理活动可能给个人信息主体带来的潜在危害和风险。

（1）个人权益影响分析：个人权益包括《民法典》等法律赋予和保护的个人所享有的各项权益，如人身权益、财产权益等。对个

人权益的影响就是指对其个人信息被处理的个人的权益可能造成的不利影响[13]。根据《评估指南》，个人权益影响分析是指分析特定的个人信息处理活动是否会对个人信息主体合法权益产生影响，以及可能产生何种影响。个人权益影响可概括分为以下四个维度：限制个人自主决策权。例如被强迫执行不愿执行的操作、缺乏相关知识或缺少相关渠道更正个人信息，无法选择拒绝个性化广告的推送等；引发差别待遇。例如因疾病、婚姻史、学籍等信息被泄露造成的对个人权利的歧视，因个人消费习惯等信息的滥用而对个人的公平交易权造成损害；个人名誉损害或精神压力。例如被他人冒用身份和公开不为人知的习惯、经历等；人身财产损害甚至引发人身伤害、资金账户被盗或遭受诈骗、勒索等。

评估时可根据数据映射分析结果及确定需要评估的个人信息处理活动，结合相关法律、法规、标准的要求或组织自定义的个人信息安全目标，分析个人信息处理活动全生命周期或特定处理行为对个人权益可能产生的影响，以及个人信息泄露、毁损、丢失、滥用等对个人权益可能产生的影响，以审视是否存在侵害个人信息主体权益的风险，并按照低、中、高三个等级进行风险评定。个人权益影响程度评估可参考《评估指南》附录 D.2。

（2）安全风险分析：所谓安全风险[14]，是指个人信息处理活动会带来的个人信息安全方面的风险，如个人信息是否会出现未经授权的访问或者泄露、篡改、丢失等。

[13] 程啸：《个人信息保护法理解与适用》，中国法制出版社，2021 年 9 月 1 日，第 636 页.
[14] 程啸：《个人信息保护法理解与适用》，中国法制出版社，2021 年 9 月 1 日，第 636 页。

根据《评估指南》，安全风险综合分析是根据风险源识别过程中识别的安全事件发生可能性结果与个人权益影响分析得出的个人权益影响程度相结合，综合分析得出个人信息处理活动的安全风险等级。安全风险分析的具体过程和风险等级的判定可参考《评估指南》附录D.3，安全风险分析的具体过程可参考使用《评估指南》附录表 C.3、表 C.4 和表 C.5。

（三）保护措施合规性与有效性评估

个人信息保护影响评估的第三项核心内容是评估所采取的**保护措施是否合法、有效并与风险程度相适应**。这些保护措施既包括技术措施，也包括组织措施，前者如采取加密、去标识化等安全技术措施，后者包括内部的管理制度和操作规程、个人信息处理权限的划分等。这一评估旨在确保个人信息处理者采取了与风险水平相匹配的安全保障措施。

1、**技术措施评估：**在进行评估时，律师应当结合数据的性质、数据处理的情形及应用场景充分评估这些技术措施是否与处理活动的风险程度相匹配，例如在涉及处理敏感个人信息时，参考《数据安全技术 敏感个人信息处理安全要求》（GB/T 45574-2025）中的敏感个人信息处理相关安全要求评估个人信息处理活动是否采取相匹配的加密、访问控制措施等以保障敏感个人信息的安全。在涉及自动化决策时，参考《数据安全技术 基于个人信息的自动化决策安全要求》

（GB/T 45392-2025）评估是否采取符合标准的算法透明度措施、用户选择退出机制等以保障个人在自动化决策中的权益等等。

2、**管理措施评估：**评估个人信息处理者是否建立了完善的个人信息保护管理体系和制度。这些管理措施包括：制定内部管理制度和操作规程，明确个人信息处理的标准流程和要求；对个人信息实行分类管理，根据个人信息的重要性和敏感程度进行分类，采取不同的保护措施；合理确定个人信息处理的操作权限，遵循最小权限原则，仅授权必要人员访问相关信息；定期对从业人员进行安全教育和培训，提高员工的安全意识和操作规范；制定并组织实施个人信息安全事件应急预案，确保安全事件发生时能够及时有效响应。律师应当审查相关制度文件、培训记录、应急演练记录等，评估管理措施的有效性和执行情况。

3、合同约束评估：当个人信息处理涉及委托处理、向其他处理者提供或跨境传输的，需要评估合同约束的充分性和有效性。对于委托处理个人信息的，委托方应当与受托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。对于向境外提供个人信息的，审查是否符合法定的跨境传输条件，如通过国家网信部门组织的安全评估、经国家网信部门规定的专业机构进行个人信息保护认证、与境外接收方签署国家网信部门制定标准合同等。律师应当审查相关合同条款是否充分约定了数据安全保护责任义务，是否明确了境外接收方

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、评估实施流程指引

（一）评估准备阶段

开展个人信息保护影响评估的准备阶段是确保评估工作顺利推进的基础。本阶段主要包括以下工作内容：

1、评估必要性分析：首先需要确定拟进行的个人信息处理活动是否属于《个人信息保护法》第五十五条规定的必须进行个人信息保护影响评估的情形，或者是否符合国家标准《信息安全技术 个人信息安全规范》（GB/T 35273-2020）中建议开展个人信息保护影响评估的场景。对于确需开展个人信息保护影响评估的项目，应当明确评估的范围和重点，例如是否涉及敏感个人信息处理、自动化决策、数据跨境传输等特殊场景。

2、组建评估团队：个人信息保护影响评估应当组建跨职能的评估团队。团队构成包括：组织内部成员：业务负责人负责统筹协调、技术部门负责数据安全措施评估、法务合规部负责法律审查；组织外部支持：根据需要聘请律师事务所提供法律意见、第三方安全机构进行技术评估。团队应当明确负责人和各成员的职责分工，确保评估工作的专业性和全面性。业务部门负责提供业务逻辑和数据流程说明；技术部门负责评估数据加密、存储等技术措施；法务合规部门负责审核法律依据及合同条款。

3、制定评估计划：根据《评估指南》，评估计划应详细说明工作内容、任务分工和时间表，并考虑评估可能的中止或撤销情况。操作中需考虑人员资质、技能、经验和能力；任务所需时间；以及评估阶段所需资源，包括自动化工具。复杂或资源密集的评估场景应更新方案；常规或简单场景可沿用原计划或简化步骤。涉及相关方时，计划应明确咨询条件、对象和方式（如公众调查、研讨会、焦点小组、听证会、线上体验等）。

4、确定评估对象和范围：根据《评估指南》，主要从以下三个方面描述评估的对象和范围：描述系统基本信息、描述系统涉及信息、描述处理流程和程序信息。

5、制定相关方咨询计划：

评估涉及多方利益相关者，包括员工、个人信息主体、消费者代表、合作伙伴、系统维护人员及其他合规意义的组织人员。评估人应确保流程透明，降低风险，明确这些相关方与个人信息处理活动的直接利益关系，并识别可能访问个人信息的组织或个人。

评估人需对相关方进行分类，识别特定组织或个人，并确保个人代表的典型性。在确定相关方时，应考虑个人信息的范围、规模、业务重要性及成本收益。大型评估可能需要考虑多方，而小型评估则可减少相关方的确认。

制定咨询计划时，应明确各相关方受影响程度、后果及安全控制措施，并包含咨询范围与时间表。咨询计划旨在确定相关方数量与范围，明确他们参与评估的方式，以及就评估报告征求并反映相关方的

意见。组织可要求合作伙伴进行个人信息安全影响评估，或协助组织评估，其报告可作为咨询结果。

表：个人信息保护影响评估准备阶段主要工作、方法及成果

工作内容	具体方法	产出成果
必要性分析 **梳理需要进行评估的场景**	对照《个人信息保护法》第 55 条（如处理敏感信息、自动化决策、数据跨境传输等） 参考《信息安全技术 个人信息安全规范》（GB/T 35273-2020）建议场景	《必要性分析报告》 《评估场景清单》
制定实施计划	明确各阶段任务节点、分配人员资质与技能要求	《个人信息保护影响评估实施计划》（含时间表、任务分工、资源清单）
确定评估对象和范围	系统基本信息描述：信息系统架构图、数据生命周期流程图（收集、存储、使用、共享等） 数据类型与处理流程分析：数据清单（含敏感信息分类）、处理活动分类（如委托处理、公开披露）	系统信息说明书、数据流程图（含数据流向标注）、数据资产清单、处理活动分类表
制定相关方咨询计划	利益相关者分析矩阵、通过线上问卷进行公众调查	利益相关者清单、咨询方案（含时间表、参与方式）、反馈意见汇总报告

（二）评估实施阶段

评估实施阶段是个人信息保护影响评估的核心环节，需要通过多种方法和工具全面评估个人信息处理活动的合规风险和保障措施。本阶段主要包括以下工作内容:

1、数据处理活动分析：全面梳理和分析个人信息处理活动的基本情况，涵盖处理目的与合法性基础，确认处理目的的明确性与合理性，以及处理行为的合法性依据；数据处理必要性，验证收集的个人信息是否为实现业务功能所必需，是否符合最小必要原则；告知与同意机制的审查，评估是否履行了充分的告知义务，并取得了有效的同意。对于跨境传输场景，确保其符合法定的跨境传输条件，例如通过国家网信部门组织的安全评估、经国家网信部门规定的专业机构进行个人信息保护认证、与境外接收方签署国家网信部门制定标准合同等。

2、数据映射分析：通过数据映射分析明确个人信息的流向和处理全过程。数据映射分析包括：第一，关注数据流向，明确发送方、接收方、数据类型、数据量级；第二，明确业务场景，确定评估的具体业务场景，明确涉及的个人信息处理活动；第三，确定法律触发点，确认是否涉及《个人信息保护法》要求的强制评估场景。数据映射分析通常采用数据清单和数据映射图作为工具，清晰展示个人信息在不同系统、组织和个人之间的流动路径。

3、风险识别与评估：基于数据映射分析的结果，识别和评估个人信息处理活动可能带来的风险。风险识别主要包括：数据敏感度分级，根据《个人信息保护法》第二十八条，识别敏感个人信息，区分一般个人信息与敏感个人信息，评估泄露后的潜在危害；处理活动风险，评估技术风险、合同风险等；权益影响评估，分析对个人信息主体的潜在影响，按《评估指南》量化风险等级。风险评估应当综合考虑安全事件发生可能性和个人权益影响程度两个要素，按照“低、中、高”确定风险等级。

4、安全保障措施评估：评估现有安全保障措施的有效性和充分性，并提出改进建议。安全保障措施包括：技术措施，如加密传输、数据脱敏、定期安全审计、日志留存等；管理措施，如制度构建、人员管理、应急响应；合同约束，要求境外接收方签署数据保护协议，明确处理目的、存储期限、第三方共享限制。对于评估中发现的高风险问题，应当提出针对性的风险处置建议，如减少高敏感数据的传输、补充单独同意流程、完善隐私政策、制定数据泄露应急预案等。

表：个人信息保护影响评估实施阶段主要工作、方法及成果

工作内容	具体方法	产出成果
数据处理活动分析	文档审查、访谈、流程梳理	数据处理清单、合法性分析报告
数据映射分析	数据流图、系统架构分析	数据映射图/表、数据清单、数据流向表

风险识别与评估	风险矩阵、场景分析、威胁分析	风险清单、风险等级评定、风险分析报告
安全保障措施评估	技术测试、合同审查、管理审计	安全措施评估报告、改进建议清单
跨境传输专项评估	法律环境分析、接收方评估	跨境传输风险评估、合同条款建议

（三）评估跟进阶段

评估报告编制阶段是个人信息保护影响评估的收官环节，需要将评估过程和结果以书面形式固定下来，形成可供查阅和验证的评估记录。本阶段主要包括以下工作内容：

1、报告内容编制：个人信息保护影响评估报告应全面展现评估过程及成果，内容应涵盖以下要点：评估结果摘要，包括风险等级划分及改进建议；评估对象的详细描述，涵盖所涉及的个人信息种类及处理活动；评估方法与流程，详述所采用的评估方法、工具及流程；风险评估结果，明确识别出的风险点及风险等级评定；针对性的整改建议，包括风险应对措施及改进建议；以及支持性文件，如数据处理协议、技术方案、用户告知文本等。报告应使用明确、精确的语言，避免含糊和歧义的表述，确保报告的使用者能够准确把握评估结果与建议。

2、合规存档：依据《个人信息保护法》，个人信息保护影响评估报告及处理情况记录应保存不少于三年，以供监管机构审查。存档资料应涵盖以下内容：各类文件底稿，包括问卷及书面回复、访谈记

录或摘要、屏幕截图或录像资料、合同及处理记录、核验或回访记录等;事件描述与图表,涉及处理细节的叙述、业务流程与数据流向图;现有资源,如等级保护测评报告、安全审计报告、算法备案报告;以及专项测试报告或记录,例如安全有效性测试、匿名化或去标识化效果测试。存档工作应采取有序化管理,确保资料易于检索和查阅,建议同时保留纸质和电子版档案。

3、持续监测与更新:个人信息保护影响评估不是一次性的活动,而应当是一个持续的过程。个人信息处理者必须执行以下措施:持续监控并关注相关法律法规的最新动态,定期对业务模式的变更以及数据量的增长进行复审;开展内部培训,对业务和技术团队进行隐私保护教育,以增强合规意识;完善相关机制,依据评估结果优化内部个人信息保护的管理体系和操作流程。在出现可能影响风险评估结果的变动时,例如处理目的、方式、范围的变更,或境外接收方政策环境的改变等情形,应重新进行评估或更新现有的评估报告。

五、不同触发情形的专项评估

(一)处理敏感个人信息的专项评估

处理敏感个人信息时,个人信息保护影响评估需要特别关注以下方面:

1、合法性基础与单独同意:评估是否已取得个人信息主体对处理敏感个人信息的**单独同意**。根据《个人信息保护法》第二十九条,处理敏感个人信息应当取得个人的单独同意,法律、行政法规

规定处理敏感个人信息应当取得书面同意的，从其规定。律师需要审查同意的方式是否符合要求，是否通过弹窗、单独协议等方式获取用户的明示同意，以及是否向个人告知了处理敏感个人信息的必要性及对个人权益的影响。

2、处理必要性与目的限制：评估处理敏感个人信息是否具有特定的目的和充分的必要性。敏感个人信息只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。律师需要审查处理敏感个人信息是否为实现业务功能所必需，是否存在替代方案，以及处理目的是否明确、具体。

3、增强型保护措施：评估是否采取了与敏感个人信息高风险特性相匹配的强化安全措施，这些措施涵盖但不限于：加密存储与传输，即对敏感个人信息实施加密处理；访问控制，即执行严格的权限管理以限制敏感个人信息的访问范围；安全审计，即定期对敏感个人信息的访问和使用情况进行审计；去标识化处理，即在可行的情况下对敏感个人信息进行去标识化处理。律师需对这些技术措施的有效性进行评估，并审查相关管理制度的完善性。

4、特殊类型敏感信息的特别要求：针对某些特殊类型的敏感个人信息，如生物识别信息、未成年人信息等，评估是否满足了相关特别要求。例如，处理不满十四周岁未成年人个人信息的，应当取得未成年人监护人的同意，并应当制定专门的个人信息处理规则。处理人脸等生物识别信息的，应当同时评估是否遵循了《最高人民法院关于

审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》等相关司法解释的要求。

（二）利用个人信息进行自动化决策的专项评估

利用个人信息进行自动化决策时，个人信息保护影响评估需要特别关注以下方面：

1、决策透明度与可解释性：评估自动化决策的透明度与可解释性。根据《个人信息保护法》第二十四条，个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。律师需要审查是否公开了自动化决策的基本原理、主要参数和逻辑，是否提供了拒绝自动化决策的选项，以及是否设立了人工复核渠道。

2、算法公平性与偏见检测：评估自动化决策算法的公平性与是否存在不合理偏见。自动化决策可能导致基于个人特征的不合理差别待遇，如大数据“杀熟”等歧视性行为。律师应当评估算法是否经过公平性测试，是否建立了算法偏见检测和纠正机制，以及是否定期对算法进行审计和优化。

3、数据质量与准确性：评估用于自动化决策的个人信息的质量与准确性。自动化决策的准确性很大程度上取决于输入数据的质

量。律师需要审查是否有机制确保用于自动化决策的个人信息的准确性、完整性和时效性，以及是否提供了个人信息更正渠道，以确保决策基于最新、准确的信息。

4、用户控制与退出机制：评估是否提供了有效的用户控制与退出机制。根据《个人信息保护法》要求，利用个人信息进行自动化决策，进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。律师需要审查是否提供了清晰的选项让用户可以选择退出个性化推荐或自动化决策，以及退出机制是否便捷、有效。

（三）委托处理、向其他处理者提供、公开个人信息的专项评估

当个人信息处理涉及委托处理、向其他个人信息处理者提供个人信息或公开个人信息时，个人信息保护影响评估需要特别关注以下方面：

1、受托方或接收方安全保障能力评估：评估**受托方或接收方的数据安全保障能力**。根据《个人信息保护法》第二十一条，委托处理个人信息的，应当与受托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务，并对受托方的个人信息处理活动进行监督。律师应当对受托方或接收方进行尽职调查，评估其数据安全管理制度、技术保护措施、人员管理水平等，确保其具备与处理风险相匹配的安全保障能力。

2、合同约束与责任划分：评估与受托方或接收方签署的合同是否充分约定了数据安全保护责任义务。合同应当明确约定处理目的、期限、处理方式、个人信息的种类、保护措施、双方的权利和义务，以及信息安全事件发生时的责任划分和赔偿机制。对于向其他个人信息处理者提供个人信息的，还应当约定接收方在处理个人信息时遵循的原则、限制和条件。律师应当审查合同条款是否充分、明确，是否符合法律法规要求。

3、再转移限制：评估是否对个人信息的再转移进行了合理限制。委托处理或向其他个人信息处理者提供个人信息时，应当通过合同等方式约定，未经个人信息处理者同意，受托方或接收方不得将个人信息再次委托或提供给第三方。律师需要审查合同中是否包含了适当的再转移限制条款，以及是否有机制监督受托方或接收方遵守这些限制。

4、公开个人信息的特殊风险评估：当涉及公开个人信息时，评估公开的必要性及可能带来的后续影响。公开个人信息可能带来无法控制的二次传播和滥用风险。律师应当评估公开个人信息是否确有必要，是否采取了适当的措施，如匿名化、去标识化等方式以降低风险，是否向个人告知了公开可能带来的风险，以及是否提供了撤回公开或删除的机制。

（四）向境外提供个人信息的专项评估

向境外提供个人信息时，个人信息保护影响评估需要特别关注以下方面:

1、出境合规路径合法性：评估选择的数据出境合规路径是否符合法律规定。根据《个人信息保护法》第三十八条，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：通过国家网信部门组织的安全评估；经专业机构进行个人信息保护认证；按照国家网信部门制定的标准合同与境外接收方订立合同；法律、行政法规或者国家网信部门规定的其他条件。律师需要根据出境数据的类型、规模和处理者性质，判断应当适用的合规路径，并评估是否符合该路径的所有要求。

2、境外接收方保障能力评估：全面评估境外接收方的个人信息保护政策和措施。律师应当审查境外接收方所在国家或者地区的个人信息保护政策法规和网络安全环境，评估境外接收方是否采取了与风险程度相适应的管理措施和技术手段保障出境个人信息的安全，以及是否承诺承担相应的责任义务。对于欧盟等有充分保护水平的国家和地区，还需要特别审查其是否符合 GDPR 等当地数据保护法规的要求。

3、个人信息主体权利保障：评估个人信息出境后，个人行使权利渠道是否通畅。个人信息出境后，个人信息主体仍然享有查询、更正、删除等权利。律师需要审查境外接收方是否建立了便捷的个人权利响应机制，个人是否能够通过境内处理者或直接向境外接收方行使权利，以及权利响应的时间和程序是否合理。

4、跨境传输安全措施：评估跨境传输过程中的安全措施是否充分。跨境传输环节可能面临更高的安全风险。律师应当审查传输过程中是否采取了加密传输、安全通道等技术措施，是否有机制防止数据传输过程中的窃取、篡改和泄露，以及是否制定了跨境传输安全事件的应急响应预案。

（五）其他对个人权益有重大影响的处理活动的专项评估

对于其他对个人权益有重大影响的个人信息处理活动，个人信息保护影响评估需要特别关注以下方面：

1、处理规模与范围评估：评估个人信息处理的规模与范围是否可能导致重大影响。处理大规模个人信息或处理范围广泛可能放大安全事件的影响范围和程度。对于超过100万人的个人信息可被认定为处理大规模个人信息，对于处理覆盖全国或省级以上的易被认定为范围广泛，律师需结合项目的具体情况及当时政策监管要求评估处理活动的规模、覆盖范围、持续时间等因素，判断其是否可能对个人权益产生重大影响。

2、新技术新应用风险评估：评估采用新技术新应用可能带来的新型风险。采用人脸识别、声纹识别、基因分析等新技术处理个人信息可能带来传统评估未能覆盖的新型风险。律师应当评估技术本身的成熟度、安全性，以及可能带来的伦理和社会影响，确保处理活动符合科技伦理要求。

3、结合场景的综合风险评估：基于具体业务场景进行全面的权益影响分析。某些处理活动在特定场景下可能对个人权益产生重大影响，如在公共场所安装图像采集设备、对员工进行持续监控等。律师应当结合处理活动的具体场景，综合分析可能对个人的人身财产、名誉、身心健康等产生的潜在影响，确保评估全面、准确。

六、结语

个人信息保护影响评估作为《个人信息保护法》规定的强制性合规义务，已成为企业个人信息处理活动不可或缺的组成部分。对于律师而言，协助客户开展个人信息保护影响评估工作不仅需要全面理解法律法规要求，还需要具备风险评估、技术保障、合同审查等多方面的专业能力。

本指引从个人信息保护影响评估的基本概念、评估主体、触发条件、评估要点、实施流程以及不同触发情形的专项评估等方面，提供了系统性的指导和建议。希望本指引能够帮助律师在实际工作中更好地协助客户开展个人信息保护影响评估评估，确保个人信息处理活动的合规性，降低法律风险，同时促进数据的合法、合理利用，实现个人信息保护与数据价值挖掘的平衡。

需要强调的是，个人信息保护影响评估不是一次性的合规任务，而应当是一个持续的过程并保持符合政府监管的要求的标准。随着业务发展、技术变革和法律法规更新，个人信息处理活动可能面临新的风险和挑战。律师应当建议客户建立个人信息保护影响评估的定期复

查和更新机制，确保个人信息保护工作持续有效，适应不断变化的内外部环境。