HAI WEN
海问律师事务所

《个人信息保护法（草案）》经典问答

作者：杨建媛 傅鹏 林德娴 邬丹

2020 年 10 月 21 日，全国人大法工委公开就《个人信息保护法（草案）》（下称“草案”）征求意见。草案回应了近年的数据合规实践，借鉴国际经验，开创贴合国情且富有前瞻性的监管新路径，也将为我国在国际数据保护话语体系中占据一席之地奠定基础。于企业而言，强化个人信息保护的趋势已经明朗，数据合规将成为助力企业提升竞争力的重要驱动力。以下选取最受关注的八个典型问题进行讨论。

一、处理个人信息仍然只能使用“同意”原则吗？

长期以来，除为履行法定义务所必需外，取得个人同意是处理个人信息的唯一合法基础。考虑到经济社会生活的复杂性和个人信息处理的不同情况，草案对基于个人同意以外合法处理个人信息的情形作了规定，即：订立或履行合同所必需、履行法定职责或义务所必需、保护自然人的生命健康和财产安全所必需、为公共利益在合理范围内处理个人信息。

尽管如此，“告知-同意”依然是个人信息处理规则的核心，并已经在国内现有的法律和监管体系中得到广泛执行。草案对“告知-同意”规则作出较大幅度的完善和更新，必将对合规生态产生深远影响。

第一，广泛的告知义务。常见的错误认知是：告知仅是基于同意处理个人信息的前置条件。草案明确规定，个人信息处理者在处理个人信息前，均需以显著方式、清晰易懂的告知为前提，并详细列示需要告知的事项。

第二，同意是在充分知情的前提下，自愿和明确的意思表示。“自愿”意即出于个人自由意志做出的意思表示。在单位处理员工个人信息的情况下，即使员工签署《授权同意书》也未必满足“自愿”的要求，因为单位与员工的地位并不对等。结合《个人信息安全规范》，“明确”的意思表示包括主动声明，即个人通过书面、口头等方式主动作出的具有语言内容的声明；也应包括肯定性动作，即主动勾选、主动点击“同意”等肯定性动作。单纯的沉默，即消极的不作为，在没有法律规定、当事人约定或者符合交易习惯的情况下不应当被认为是“明确”。

第三，新概念创设：单独同意。草案没有解释“单独同意”的具体含义，只规定了需“单独同意”的多种具体场景，即：向第三方提供处理个人信息、公开处理个人信息、在公共场所安装图像采集和个人身份识别设备、处理敏感个人信息和向境外提供个人信息。我们理解，“单独同意”是比一般“自愿、明确同意”更高的标准，需由场景触发、通过单独展示的方式告知并获得个人的明确同意。可参考 GDPR 规则中的明示同意。在《关于“同意”的指南》中其被解释为，“建议使用更高标准

的技术方式，以确保获得用户的真实授权，比如增加一道验证手续，在获取用户同意后以链接或短信验证方式要求用户再次确认”。

为订立或者履行个人作为一方当事人的合同所必需亦可处理个人信息。此项为极具突破性的设置，使用得当将为商业场景中处理个人信息提供不少便利。适用本条的核心问题是如何理解“必需”，草案未对此作详细规定。对照 GDPR，我们判断未来实践中将会对“履行合同”采取严格解释的态度。具体而言，“必需”应是合同订立和履行过程中为服务个人必不可少的处理行为，而不能局限在合同的约定或者用语的表达。举例而言，消费者如果希望电商平台的商家将商品直接寄到家里，则商家处理消费者的地址信息即可视为履行商品购销合同所必需；但如果消费者选择将商品寄到特定快递点，则商家除非获得其他合法性基础，否则无法以履行合同为由处理消费者的地址信息。

二、敏感个人信息具体包括哪些，为何会单独成节？

草案处处体现了对个人信息保护的“风险路径”考量，即在规制个人信息处理行为时区分主次、抓大放小，企业也应据此合理分配合规资源。敏感个人信息的处理规则单独成节即是证明之一。

个人信息处理者只有在具有特定目的和充分必要的情形下才能处理敏感个人信息。“告知-同意”义务方面，需额外向个人告知处理敏感个人信息的必要性以及对个人的影响，并取得个人的单独同意或依法取得书面同意。举例而言，在自动售卖机购物或从快递柜取快件时均有使用人脸识别的方式验证身份或进行支付的情形，而人脸作为个人生物特征属于敏感个人信息。此时，如果个人在知情的情况下单独同意售卖机或快递柜的运营方处理其人脸信息，是否可行？尽管满足特定目的的条件，但仅为购物或取快递之目的而收集人脸很难证明具有充分必要性，在告知时也难以解释。与此相反，个人在机场过安检时的人脸识别系为公共安全之目的，具备充分的必要性，且因此场景中处理人脸信息并非基于个人同意而进行，故也无需取得个人的单独同意。但是，向个人告知处理敏感个人信息的必要性及对个人影响的义务仍不能豁免。

敏感个人信息的范围在草案中只有概括定义及非穷尽列举。实践中，可以参考《个人信息安全规范》表 B.1 对“个人敏感信息”的举例，其对草案中的个人生物特征、医疗健康、金融账户类目均具备参考价值。值得关注的是，种族、民族、宗教信仰均作为敏感个人信息被写入草案。传统上，中国民众对该等信息的敏感度并不高，我们从小就需要在各类表格中填写民族。随着社会的进步与多元，企业在处理个人信息时需要同时具备本地和国际视角，充分尊重不同的族群、宗教、政治、文化背景。

三、　自动化决策是什么，相关规制会对本企业产生影响吗？

草案首次在法律层面提及自动化决策，并且赋予其丰富内涵，导致几乎所有利用大数据的企业都多少会受到规制。具体而言，自动化决策是指利用个人信息

对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，通过计算机程序自动分析、评估并进行决策的活动。

《个人信息安全规范》沿袭了 GDPR 规则，指出自动化决策的特征之一是决策必须能够显著影响个人信息主体权益。例如，能够决定个人信用及贷款额度、面试筛选的决策属于自动决策；而在用户界面根据用户的具体情况推荐不同产品或做默认排序并非自动决策。草案则突破自动化决策需对个人权益造成重大影响的要求，着眼于决策过程的自动化；但同时规定，如果自动化决策对个人权益造成重大影响，个人有权要求处理者予以说明，并有权拒绝其仅通过自动化的方式作出决策。

基于此，有关自动化决策的规定将广泛影响信息社会中的各行各业，尤其是人工智能的应用场景。个人信息处理者应当特别重视自动化决策的合规，例如：通过隐私政策等方式，向个人告知自动化决策的存在、基本的运行逻辑及其对个人的影响；通过定期检验数据和算法等方式，保证决策基础数据的准确性和相关性，以及决策算法的可解释性和非歧视性；通过关闭选项、人工复核等方式，避免个人完全受制于自动化的机器决策。

四、 处理公开的个人信息是否就没有合规隐患，特别是当个人信息系由政府公开时？

长期以来，处理公开的个人信息在多数情况下被视为安全港，特别是当个人信息系通过官方渠道公开。既《民法典》之后，草案亦对处理公开的个人信息设定边界，且更进一步。

《民法典》规定了处理个人信息的免责事由，包括合理处理该自然人自行公开的或者其他已经合法公开的信息，但自然人明确拒绝或处理该信息损害其重大利益的除外。草案则规定，对于已公开的个人信息，个人信息处理者可以在与其被公开时的用途相关合理范围内处理，但是，如果处理活动将对个人产生重大影响，则仍应当告知个人并取得同意。“对个人产生重大影响”较“损害个人重大利益”显然更容易证明，显示出草案对于处理公开个人信息的谨慎态度。

早在草案出台之前，司法实践中与此相关的裁判思路即在发生变化。根据南方都市报运营公众号“隐私护卫队”的报道，北京互联网法院某法官的观察显示：在企业对数据的再度利用中，公开数据是重要的一类，包括权利人自行公开、政府信息公开或司法公开。以裁判文书为例，此前的法院裁判时因裁判文书属于权威信息来源，通常认为只要再度利用时保持内容一致，不存在不当利用的情形，就不构成侵权。然而，在最近的生效判决中则出现不同的裁判结果，考虑公开信息的同时也会考察再度利用公开信息是否可能侵害权利人值得保护的重大利益。

五、 跨境提供个人信息是否需要进行评估，进行评估后是否仍需要个人同意？

草案将个人信息跨境提供置于单独章节，足以见得立法、监管层面对此的关注。总体而言，根据出境主体身份的不同，个人信息处理者或必须通过监管评估、或可以从监管评估、专业机构认证、合同订立当中进行选择，特殊情况下（如因国际司法协助或者行政执法协助需向境外提供个人信息）应按法律、行政法规进行处理。但无论如何，告知-同意义务均不能豁免。具体的关注点如下：

第一，草案要求关键信息基础设施运营者、处理个人信息达到国家网信部门规定数量的个人信息处理者，如确需出境个人信息，应当通过国家网信部门组织的安全评估（即监管评估）。该等规定拓展了《中华人民共和国网络安全法》(“网安法”) 第 37 条中跨境安全评估的适用范围，除关键信息基础设施运营者外，处理个人信息达到一定规模者亦需遵守；同时，相较于《个人信息出境安全评估办法（征求意见稿）》又提升了监管评估的适用门槛。

第二，相比较监管评估、经专业机构认证、或符合其他法定条件，与境外接收方订立合同似乎是门槛最低的出境方式。草案规定，“与境外接收方订立合同，约定双方的权利和义务，并监督其个人信息处理活动达到本法规定的个人信息保护标准”。然而，参考 GDPR 的“标准合同条款”模式，尤其是美欧隐私盾协议被判无效的同时，法院确认标准合同条款仍然是将欧盟个人数据转移到欧盟境外的有效机制，但要求企业对个人数据接收国的法律及个人数据转移场景进行个案评估。

第三，对比 GDPR，草案并未采用以国家或地区为单位的“充分性认定”模式，也未对同一集团下不同实体之间的跨境提供设置单独规则。我们理解，框架性评估往往是通过众多个案评估，提取评估经验后的产物。相同商业模式下或同一集团内的个人信息出境模式常具有相似性，建立标准化的评估体系后即可极大降低合规成本。

六、 草案对于个人信息权利与义务的规定有哪些突破、创新？

草案构建了个人信息的权利义务体系。该等内容在企业实践中均已涉及，但在此之前尚未在法律层面予以全面规范。就个人权利而言，个人享有知情、决定权，查阅、复制权，更正、补充、删除权，以及要求解释说明、申请受理的权利。就个人信息处理者义务而言，个人信息处理者应采取必要的技术与管理措施、设置个人信息保护负责人、定期开展合规审计、事前风险评估、个人信息泄露后应及时补救并通知。简单选取值得讨论的两点：

第一，相较于网安法将违法违约收集个人信息作为个人行使删除权的前提，草案扩张了删除个人信息的情形，包括：约定的保存期限已届满或处理目的已实现，处理者停止提供产品或者服务，个人撤回同意，个人信息的处理违法或违约，或其他法定情形。对比 GDPR 和 CCPA，两者均规定若干删除的例外，例如为履行法定义务、维护系统安全、保障诉讼、行使言论自由、出于科学研究等公共利益。草案未提供例外，但保留了法定的保存期限未届满、或者删除个人信息从技术上难以实

现时，停止处理个人信息的选择。

第二，此外，草案要求个人信息处理者发现泄露事件即应通知有关部门，但对于能够有效避免信息泄露造成损失的，可免除通知个人的义务。然而，按照严格标准数据安全事件几乎每天都在发生，在缺乏准确界定的情况下泛化的通知义务可能使企业陷入决策困境，同时无谓加重处理者和监管部门的负担。

七、 未来中国也可以对个人信息处理的违法行为行使域外管辖权吗？

草案将在中国境外处理境内自然人个人信息的部分活动也纳入管辖范围，初步判断实践中可部分对标 GDPR 下的提供商品或服务原则及监控原则。“以向境内自然人提供商品或服务为目的”，在实际中可能会考量个人信息处理者是否“有意”在中国境内向个人提供商品或服务。“为分析、评估境内自然人的行为”系从处理目的的角度出发，落脚于使用个人信息开展行为的分析、评估活动；监控原则则是从行为角度，要求存在监控行为并且还包括后续的利用。两者具备相似性，如用户画像及相关的定向推送、消费者习惯分析均为典型场景。

草案除规定了域外管辖权外，还要求适用本法的境外个人信息处理者在我国境内设立专门机构或指定代表，并将有关机构或代表的信息报送主管部门。其出发点应当是为执法设置抓手，确保域外管辖权得以有效落实。

八、 个人信息主体的违法成本有多高，相关违法行为的查处力度会有多大？

草案全方位地规定了违法处理个人信息的行政处罚、民事赔偿和刑事责任，尤其是第 62 条高达 5000 万元或上一年度营业额 5%的天价罚款，堪比 GDPR 中 2000 万欧元或上一年度全球总营业额 4%的标准，宣示了中国对规范个人信息处理的决心。

对于违法行为的查处力度尚难以预估，但草案已经对履行个人信息保护职责的部门进行执法予以充分赋权，包括对有证据证明是违法个人信息处理活动的设备、物品，可以查封或者扣押。查封、扣押属于行政强制措施，原则上只能由法律设定。《中华人民共和国证券法》第 170 条规定了证券监管机构对证券交易记录、证券账户等金融信息相关的查封与扣押，而草案赋予主管机关在处理个人信息案件时的查封、扣押权，使个人信息监管过程中的行政强制措施有法可依。