小荷才露 — 简析《个人信息保护法》草案的实践影响

作者：杨迅 | 杨坚琪

本文为通力合规团队对《个人信息保护法(草案)》解读系列文章第二篇。

自 2016 年国务院公布的《“十三五”国家信息化规划》提出“推动出台……个人信息保护法”以来，在漫长的等待之后，全国人大常委会终于在 2020 年 10 月 21 日对外公布了《个人信息保护法》草案(下称**“草案”**)的全文。草案不仅仅对于现有的个人信息保护标准进行了重新定位，还对很多长期以来一直处于“灰色地带”的实践进行了明确。本文将主要集中探讨草案中现有规定对企业处理个人信息商业实践的潜在影响。

委托处理：信息服务外包的基石

信息服务外包，即将非主营业务的信息处理，外包给第三方进行，是现代服务业的重要一环。通常而言，信息服务业务的开展需要解决个人信息在外包过程中的转移问题。

在现有的法律渊源中，无论是《民法典》还是《网络安全法》都没有针对“委托处理”个人信息情形做出特别的规定。虽然《个人信息安全规范》针对“委托处理”设置了专门的章节，但是限于效力层级，《个人信息安全规范》对于企业的实践仅仅具有“参照适用”的效力，并不能成为企业对外进行个人信息“委托处理”的合法标准。因此长期以来，对于大量的“委托处理”场景，例如委托第三方提供薪资和福利管理服务，委托第三方提供信息技术服务等，现行的中国法未能提供适当的法律依据以供企业进行遵守。

在这一点上，草案的第二十二条进行了直接回应：对于“委托处理”，草案要求作为有权自主决定个人信息处理目的和处理方式的个人信息处理者，应当与受托方签订含有“必要条款”的合同，并对受托方进行管理和监督。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

将草案第二十二条与其他条款进行对比阅读，我们发现不同于草案针对诸如“对外提供个人信息”、“公开个人信息”等提出的要求，立法者对于“委托处理”下个人信息处理者负有的义务，并不包括获取个人信息主体的**“单独同意”**。这意味着作为个人信息处理者的商业主体，在“委托处理”方面享有更大的自由度和灵活性。在草案现有的法律框架下，只要个人信息处理者满足(1)在个人信息处理规则中说明委托处理的规则并获取相关个人信息主体的“事前”同意;(2)与受托方签订必要的合同；以及(3)符合风险评估的要求，委托处理就可以合法地进行。

换而言之，对于委托处理的具体场景和具体对象，立法者并不要求个人信息处理者对于可能进行的商业活动进行完整和全面的事先披露(这在实践中也是不可能完成的)。这不仅仅减轻了企业的合规成本，更重要的是给与企业委托他人处理信息，合法开展信息服务外包提供的可能性。

但另一方面，草案的规定侧重于“合同”与“风险评估”的法律要求，也意味着信息处理的委托方需要自行控制外包的风险，确保外包的合法性。即，商业主体在委托处理个人信息时，需要注意委托处理合同的内容安排、监督合同的履行情况，从而在“委托处理”场景中达到立法者对于个人信息保护的要求。毕竟，在一个违反个人信息保护法律规定最高处罚金额已经达到人民币五千万或者年营业额百分之五的时代，任何潜在的法律风险都不应当被忽视。

数据提供：数据交易的忧与思

2020 年 3 月的《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》首次明确了“数据”作为重要的新型生产要素的地位。长期以来，作为各类数据中交易价值最大同时也是对个人影响最深的“个人信息”，其如何能够“合法地”进行交易或者流通一直以来是各界讨论的核心问题。

虽然草案看似没有直接针对以个人信息为基础的“大数据交易”进行规定，但是我们还是在草案第二十四条的规定中读出了“唯有保证个人信息安全方可进行大数据交易”的潜在立法意图。

在现有的草案规定下，除非将个人信息进行匿名化处理，否则基于个人信息的“大数据交易”可能无法直接实现，或者说需要极高的合规成本方可实现。草案的第二十四条规定，“个人信息处理者向第三方提供其处理的个人信息的，应当向个人告知第三方的身份、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。**接收个人信息的第三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”。草案并未对本款下的“提供”进行进一步的解释，但是根据一般文义理解，“交易”因为包含个人信息的交换，因此很可能属于监管视野下的“提供”行为，进而受到草案第二十四条的约束。

基于第二十四条的约定，如果需要进行“大数据交易”，个人信息处理者需要重新征得每个个人信息主体的“单独同意”，这在实践中无疑将大大增加企业的合规成本，原因是: (1)第二十四条下的“个人信息”不仅仅包括原始的“个人信息”，还包括个人信息处理者处理后的“个人信息”，因此本条的适用范围非常广泛，间接提高了“大数据产品”的流通门槛; (2)由于通常大数据交易涉及的个人信息主体众多，重新获得“单独同意”不仅仅需要从技术手段上进行考虑，还必然涉及到高昂的时间成本和管理成本；和(3)个人信息处理者需要设置适当的合同安排和管理机制以管理第三方在“**(授权)范围内**”使用大数据交易背景

下的个人信息，进一步提高了对个人信息处理者的管理水平要求。考虑到以上种种因素，对于资金和技术实力均不占据显著优势的大数据行业初创企业而言，在短时间内，合法地进行基于个人信息的大数据交易可能存在困难。

不过，出于维护个人信息安全的目的，采用例如联邦学习、同态加密等技术手段在“适当匿名”环境下进行大数据交换、合作或者交易已经是业界的新潮流，中国在这方面毫无疑问也走在前列。因此在面对类似的技术时，与《民法典》、《网络安全法》等保持一致，草案认为“匿名化”后的个人信息将不受到个人信息保护相关法律的限制：也就是说，如果个人信息处理者向第三方进行的是大数据交易的基础是匿名化后的个人信息，那么这样的“提供”行为将不受草案第二十四条的限制，这对于以隐私保护为基础的数据流通提供了合法性依据。但值得注意的是，草案第二十四条特别还要求个人信息接受方不得利用技术等手段重新识别个人身份，对于业界而言，意味着例如托库、撞库等反向识别个人信息的方式存在着合法性风险。

通过以上的分析我们认为，如果草案以目前形式得以通过，那么开展以个人信息为基础的大数据交易时，企业不可避免需要考虑利用新技术、新模式，在不转移数据本身的基础上，拓展个人数据的利用价值。

数据出境：跨境经营的曙光

对于在华的跨国公司而言，为了控制成本、加强统一管理或者利用境外已有的 IT 设施的目的，其往往会选择将个人信息直接传输至境外，在全球平台上处理。但随着《网络安全法》等法律法规不断加强对于个人信息出境的监管要求，如何合法地将境内运营时收集或产生的个人信息传输至境外，则成为了所有在华企业长期担心的隐忧。

在过去的几年中，网信办先后公布了《个人信息和重要数据出境安全评估办法(征求意见稿)》、《个人信息出境安全评估办法(征求意见稿)》(“**《2019 出境安全评估办法》**”)以及《数据安全管理办法(征求意见稿)》，规定对于个人信息和重要数据出境的安全审查规则。这些规定扩大了需要安全审查的个人信息出境范围，并取消了需要出境的最低标准，因此一直以来都被外界质疑存在“违反上位法”以及“不具备可操作性”的问题。针对这些质疑，草案的第三十八条至第四十三条重新梳理了数据出境规则，为数据出境活动重新设置了合理的法律依据，从而减轻了出境合规负担。

首先，传承《网络安全法》的要求，草案单独对“关键信息基础设施运营者”设置了特殊的出境要求。原则上，关键信息基础设施运营者收集的个人信息必须保存在境内，如果需要向境外传输的，除非法律另有规定，则需要通过网信部门组织的安全评估。为了管控出境风险，草案还为网信部门提供了特别的监管权利：即，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，其在数据出境时也应当参照“关键信息基础设施运营者”的要求进行管理。

其次，若不属于“关键信息基础设施运营者”的商业机构需要进行跨境个人信息传输的，则在满足以下任意一项条件后即可出境：(1)通过网信部门组织的安全评估；(2)经过安全认证；(3)通过与境外接收方签署含有法律要求必须条款的合同；或者(4)法律另行准许的。值得特别注意的是，跨境传输个人信息中以“合同签

署”方式视为满足出境合法性要求的规定显然学习了欧盟的立法经验，而在这点上，《2019 出境安全评估办法》则细致地规定了必备条款应当涵盖的内容。因此，在草案转化为正式法律的过程中，具有出境需求的企业可以提前参照《2019 出境安全评估办法》中的规定准备与个人信息跨境传输的相关协议。

最后，草案还特别强调了“国际司法协助或者行政执法协助”渠道下的个人信息传输要求：即，未经主管部门允许，不得私自通过国际司法协助或者行政执法协助渠道向境外传输个人信息。这实际上是又一次反应习近平主席关于“数字主权”理论的具体立法举措，也是针对类似美国云法(CLOUD ACT)的强硬回击。实际上，2019 年颁布的《证券法》已经存在类似的规定：根据《证券法》第 177 条特别规定，未经证监会和有关主管部门同意，任何人均不得将与证券业务相关的资料向境外提供。我们还特别注意到，考虑到国际环境的问题，草案配合 2020 年 9 月发布的《不可靠实体清单规定》设计了个人信息领域的“反制措施”，即如果境外接收方处于我国采取反制措施的国家或地区，那么境内主体向其传输个人信息也将受到限制。可以说，中国政府在建设“数据主权”制度上已经存在初步的整体框架。

综合来看，对比之前《2019 出境安全评估办法》中关于个人信息出境的要求，草案更加贴合实际地重构了数据出境制度，合理区分了外部“评估制度”和内部“合同要求”的适用情形。对需要在全球平台处理信息的跨国公司而言，信息出境可能不再是不可控制的法律风险，而是内控制度下的可行选择。

内控制度：信息化时代企业的合规要素

在现有技术条件下，任何信息网络都不可能保证绝对的安全。相应地，企业的职责也并不是确保个人信息的完全安全，而是就个人信息保护制度建立和执行一套完整的安全管理措施。

在草案颁布之前，诸如《个人信息安全规范》和《互联网个人信息安全保护指南》等一批推荐性规范或者标准中，已经存在关于个人信息保护的企业内部制度建设要求，但是这些规范或者不全面，或者不具有强制的执行效力，也没有罚则，因此长期以来在企业内部制度建设中并没有得到全面贯彻。此外，现有的监管往往针对于与个人信息的处理相关的违法情形，对于企业内部制度建设的关注较少。

但是，随着草案对于企业在个人信息保护方面的内控制度提出建设要求，并且设定对企业和责任人的双罚制度，这意味着个人信息保护内控制度应当得到商业机构的高度重视。我们将草案规定的内控制度要求总结如下：

第一，个人信息处理者应当根据企业自身的实际情况，结合个人信息的处理目的、处理方式、个人信息的种类以及对个人的影响、可能存在的安全风险等，选择适合的内控措施以减少个人信息风险。草案第五十条建议企业采取以下的必要措施：

- 制定内部管理制度和操作规程；
- 对个人信息实行分级分类管理；
- 采取相应的加密、去标识化等安全技术措施；

- 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；及
- 制定并组织实施个人信息安全事件应急预案。

第二，学习 GDPR 的先进经验，草案第五十一条要求处理满足特定数量要求的个人信息处理者应当指定个人信息保护负责人，并将其基本信息(如姓名、联系方式等)报送相关的主管部门。但是对该负责人的资历要求，草案则并没有给与进一步回应。

第三，草案要求个人信息处理者应当进行对个人信息处理活动和保护措施进行定期审计，并在进行以下的个人信息处理项目开展事先的风险评估:

- 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、向第三方提供个人信息、公开个人信息;
- 向境外提供个人信息；以及
- 其他对个人有重大影响的个人信息处理活动。

就风险评估的内容，草案要求至少包含以下三方面: (1)个人信息处理目的是否满足“合法、正当和必要”原则; (2)对个人的影响程度和可能的风险；以及(3)是否采取适当的安全保护措施。此外，草案还要求风险评估报告应当至少保存三年。

最后，草案还要求建立适当的个人信息安全事件应急机制，以保证个人信息处理者在发生个人信息泄露事件后，能够及时采取补救措施的同时在最短时间内告知相关的个人信息主体。

实际上，草案的大部分内控制度要求都没有超脱已经颁布的规范或者标准的范围，这对于长期以来重视个人信息保护制度建设的企业而言是一个重大利好消息。但是，在草案正式通过之后，如何衔接《网络安全法》下的“网络安全”要求和《个人信息保护法》下的“个人信息保护要求”，则成为另一个值得探讨的法律问题。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 16/19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环皇后大道中 5 号 衡怡大厦 27 楼 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野