个人信息保护法和数据安全法二审稿对跨国金融机构的影响

作者：杨迅 | 杨坚琪

2021 年 4 月 29 日，全国人大常委会向全社会公布了《个人信息保护法(草案二次审议稿)》(“**《个保法二审稿》**”)和《数据安全法(草案二次审议稿)》(“**《数安法二审稿》**”)，并公开征求意见。《个保法二审稿》和《数安法二审稿》的颁布表明中国政府意在建立一个更加全面的数据保护体系，对跨国金融机构产生显著影响。本文将简要分析《个保法二审稿》和《数安法二审稿》对在华金融机构的影响。

1. 数据出境

《个保法二审稿》和《数安法二审稿》并未实质性地变更原先一审稿草案下的数据出境条件：即，以“自我评估”作为主要的出境审核方式；但若个人信息处理者为关键信息基础设施运营者或者出境数据的数量达到监管部门规定数量的，则应当经过主管部门评估同意后方可出境。但是，《个保法二审稿》和《数安法二审稿》下对数据出境的规则如下变化实际上进一步加强了对数据出境的控制。

首先，《个保法二审稿》对基于“数据出境合同”的合法出境方式施加了额外的要求。根据《个保法二审稿》的修订，“数据出境合同”必须按照网信主管部门制定的标准合同签署。《个保法二审稿》的该等新增要求并不意外，实际上，在 2019 年颁布的《个人信息出境安全评估办法(征求意见稿)》(“**《个人信息出境办法》**”)中，网信办已经对与境外接收方签订的合同中应当含有的“必要内容”提出了要求。但《个保法二审稿》的要求显然比《个人信息出境办法》下的要求更加严格，即不仅要求涵盖法定内容，而且可能在形式上也必须达到政府规定的标准合同的要求。出于各种原因，大多数跨国金融机构都希望能够在全球层面整合和处理个人信息(包括员工信息和用户信息)。而在实践中，同一金融集团内不

For more Llinks publications, please contact:

Publication@llinkslaw.com

如您需要了解我们的出版物，请联系:

Publication@llinkslaw.com

同地区的主体则会签署以 GDPR 要求为蓝本制定的数据分享协议，协议内容可能会依据各地的法律进行略微调整(包括中国)。但是《个保法二审稿》下使用“标准合同”的要求，则意味着上述实践可能并不符合中国政府的要求，因为以 GDPR 下的模板制定的合同可能与网信主管部门制定的“标准合同”存在偏差。也就是说，在这样的情况下各方需要另行签署以“标准合同”为基础的数据出境协议。

其次，《数据安全法二审稿》新增的第 30 条重新规范了“重要数据”的出境制度。依据《网络安全法》第 37 条的要求，关键信息基础设施运营者在中国境内收集的“重要数据”确因业务需要出境的，应当经过网信部门和有关主管部门的评估后方可出境。但是《网络安全法》并没有对除“关键信息基础设施运营者”之外的其他运营者所收集的“重要数据”的出境是否需要评估提出要求。《数据安全法二审稿》则进一步规定，对其他类型的数据处理者出境“重要数据”的，应当参照网信主管部门与其他主管部门共同制定的办法执行。部分的金融数据，例如汇聚后覆盖多省份的金融消费者真实交易信息，在 2020 年颁布的《金融数据安全分级指南》下已经被认为属于“重要数据”。虽然大部分跨国金融机构未必会被认为属于是“关键信息基础设施运营者”，但是如果《数据安全法二审稿》第 30 条的规定未来在正式生效版本中保留，那金融机构(例如证券公司、基金公司、理财子公司)在对外提供“重要数据”时，同样需要满足证监会或者银保监会的评估要求后方可出境。

2. 域外适用效力

《个人信息保护法(草案一次审议稿)》(“**《个保法一审稿》**”)规定了个人信息保护的域外适用。《个保法二审稿》则进一步加强了域外适用的效力。此外，《数安法二审稿》也与《个保法一审稿》和《个保法二审稿》的规定保持一致，明确其具有域外适用的效力。

在《个保法二审稿》和《数安法二审稿》现有规定下，这两部法律具有非常广泛的域外适用效力。只要收集、处理或者处置的是中国境内自然人的个人信息或者与中国的公共利益相关的数据，无论处理者为中国企业还是外国企业，也无论对该等数据的收集、处理或者处置是发生在中国境内还是中国境外，均将受到《个保法二审稿》和《数安法二审稿》的限制。因此，当跨国金融机构的总部或者其在全球各地的分支机构收集、处理或者处置在中国境内收集或者产生的数据时，它们除了遵守所在国的法律规定之外，还需要遵守中国《个人信息保护法》和/或《数据安全法》的规定。

此外，《个保法二审稿》还对违反《个人信息保护法》处理个人信息的公司提出了制裁要求。根据《个保法二审稿》第 42 条的规定，当一个境外公司违法收集、处理或者处置中国境内自然人的个人信息时，其可能被列入“禁止提供个人信息”的黑名单中。换言之，如果跨国金融机构的总部或者分支机构违反中国的《个人信息保护法》的规定，那其中国境内的关联公司也可能被禁止向其提供个人信息，进而导致业务中断。

更重要的是，作为“数据主权”的具体体现，在《个保法二审稿》和《数安法二审稿》均规定若需向境外政府机构提供数据的，需经中国政府的同意。《个保法二审稿》第 41 条和《数安法二审稿》第 35 条均要求，若境外司法或者执法机构存储在中国境内的“个人信息”或者“数据”的，均应当经过中国的主管部门同意后，方可对外提供。例如，当美国证券监管机构(“SEC”)要求披露某中国公司的部分业务

数据或者该等中国公司的最终受益人信息，则在中国处理该等数据或者信息的证券公司仅能在证监会许可同意后，方可遵守 SEC 的要求向其披露信息。一方面其受制于外国政府部门的要求应当披露数据，但另一方面中国政府却禁止其获取数据(除非获取中国政府的同意)，如果《个保法二审稿》和《数安法二审稿》按照目前的形式被采纳，这可能使跨国金融企业面临信息披露层面的困境。

3. 通过公开途径收集个人信息

《个保法二审稿》第 13 条增加了一条合法处理个人信息的理由，即“依照本法规定在合理的范围内处理已公开的个人信息”的，无需征得用户的同意，也能作为合法处理个人信息的理由。与《民法典》第 1036 条的规定类似，本条实际上允许在没有相关个人同意的情况下，收集和使用公开渠道可得的个人信息，但前提是该等收集和使用应当限定在“合理范围”内。

无论是《个保法二审稿》还是现有的其他法律法规，均未界定过何为“合理范围”。根据一般的理解，如果收集、使用个人信息的目的是可以被预见或者被期待的，那么该等收集或者使用很可能被视为在“合理范围”之内。在实践中，金融机构通往往过公开途径收集大量的信息，以便其从事研究和市场分析工作，这些信息中就包含个人信息。因此，《个保法二审稿》新增的“公开途径收集个人信息”例外，实际上在使用公开渠道内的个人信息方面，给与了金融机构更多的自由。

4. 大数据的使用

《个保法二审稿》和《数安法二审稿》均鼓励对大数据科技的应用和开发。

从条文本身来看，《数安法二审稿》第 14 条明文规定鼓励大数据科技的开发，并且鼓励在商业创新中应用大数据技术。这表明中国政府认可大数据技术在各行各业均存在着日益广阔的应用前景。自第三方数据提供商处寻找和使用大数据技术已经成为了金融机构的“惯例”。例如，通过对投资者或者金融消费者的行为数据进行积累和分析，大批金融机构已经结合自身的需求，利用大数据科技建立了包括产品推荐、风控、个性化营销、支持业务决策等各类业务模型，为金融业务的蓬勃发展提供有效支持。

由于模型的建立非常依赖于客户自身的数据(个人信息)，当一旦客户行使“撤回同意”的权利之后，金融机构是否需要删除客户的数据，或者不得继续处理该等数据，进而导致模型无法继续使用底层数据，现行法律并未明确。而《个保法二审稿》对第 16 条的修订则给与该等问题明确的回应，承认了在用户撤回同意后，继续使用基于用户个人信息产生的匿名数据或者大数据技术的可行性。

在《个保法一审稿》承认了个人有权撤回同意之前个人信息处理活动的合法性之外，《个保法二审稿》第 16 条规定，“个人撤回同意,不影响撤回前基于个人同意已进行的个人信息处理活动的效力。”对比《个人信息安全规范》第 8.4 条的注释“撤回授权同意不影响撤回前基于授权同意的个人信息处理”，《个保法二审稿》第 16 条更加突出肯定“处理行为的效力不受影响”。根据《个保法二审稿》第 16 条的规定，基于投资者或者金融消费者的同意，金融机构在此基础上通过数据分析得出的匿名数据、模

型或者大数据技术，即使在投资者或者金融消费者撤回同意后，也不会受到影响，金融机构仍然可以继续研发和使用该等匿名数据、模型或者大数据技术。因此，我们建议金融机构尽快匿名化其收集的个人信息，且该等匿名化操作尽量在投资者或者金融消费者撤回同意之前，以保证未来能够继续使用该等数据的便利性。

5. 加强网络安全保护

《个保法二审稿》和《数安法二审稿》均设置了加强网络安全保护的规则。

从系统安全角度而言，《数安法二审稿》第 26 条特别规定，“在**网络安全等级保护制度**的基础上，建立健全全流程数据安全管理制度”。自公安部门 2007 年开始推行“等保制度”后，计算机信息系统所有者或者网络运营者即有义务根据其系统的重要性以及在系统中储存信息的敏感性，对其定级，并根据定级的结果实施对应的保护措施。而在《数安法二审稿》中融入遵守“网络安全等级保护制度”的要求，则意味着网络安全等级保护制度将对所有的数据处理者适用。因此，金融机构不仅仅应当遵守行业主管设定的安全义务，还应当遵守公安部制定的等级保护义务。

从数据的角度而言，作为本次《数据安全法(草案)》最为重要的修订之一，《数安法二审稿》第 20 条规定“**国家建立数据分类分级保护制度**”，以及“**确定重要数据目录**，加强对重要数据的保护。”也就是说，国家将会主导建立数据分级制度，并对“重要数据”实施额外的保护义务。可见，《数安法二审稿》放弃了由企业和组织自行决定“数据分类分级保护制度”的保护方式，转而实施由中国政府主导负责识别重要数据的类别和范围的模式，同时数据处理者应当依照法律要求实施相应的安全措施以保护各种类型的数据。根据上述要求，金融机构未来应当根据政府要求，在识别由其数据中的“重要数据”的基础上，依据要求采取相应的保护措施。我们建议金融机构定期关注数据安全领域相关法律的更新，以及时了解在金融领域的“数据分级分类和重要数据保护”的要求。

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 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	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 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