他山之石，可以攻玉——欧盟-美国数据隐私框架介评

作者：潘永建 | 邓梓珊 | 黄文捷

2022 年 12 月 13 日，欧盟委员会启动欧盟-美国数据隐私框架（“DPF 框架”）充分性决定的通过程序，发布《欧盟委员会根据<欧洲议会和理事会关于在欧盟-美国数据隐私框架下充分保护个人数据的第 2016/679 号条例>的 XXX 执行决定(草案)》（“《充分性决定(草案)》”）[1]。该充分性决定在正式通过之前还应当获得欧盟数据保护委员会 EDPB 的意见、获得欧盟成员国代表组成的委员会的批准；此外，欧洲议会还有权对《充分性决定(草案)》进行审查。《充分性决定》正式生效后，DPF 框架将从效果上替代原先的欧盟-美国隐私盾框架，促进跨大西洋的个人数据流动。在该框架下，个人数据将得以从欧盟自由且安全地传输至获得美国商务部认证的美国组织。

经过多年的制度建设，我国在包括数据跨境流动在内的领域建立了较为完整的法律体系。2022 年中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》，要求“深入参与国际高标准数字规则制定，……积极参与数据跨境流动国际规则制定，探索加入区域性国际数据跨境流动制度安排。推动数据跨境流动双边多边协商，推进建立互利互惠的规则等制度安排。鼓励探索数据跨境流动与合作的新途径新模式。”他山之石，可以攻玉。本文旨在简要评介《充分性决定(草案)》，或能为我国个人信息保护认证等数据跨境流动机制建设提供参考借鉴。

1. 背景

充分性决定。欧盟《一般数据保护条例》(“GDPR”)规定了从欧盟的数据控制者或数据处理者向第三国传输个人数据的规则，要求对欧盟个人数据给予的保护不得因传输至第三国而受到损害。欧盟委员会有权通过执行法令的形式决定(即“充分性决定”)，第三国、某个地区或第三国的一个或多个特定区域可以给予欧盟个人数据充分的保护；在这种情况下，从欧盟向该等第三国转移个人数据无需获得来自欧盟相关监管机构任何进一步的授权。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

[1] COMMISSION IMPLEMENTING DECISION of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

充分性标准测试。根据 GDPR，欧盟委员会作出充分性决定的前提是对第三国的法令进行全面评估，包括适用于数据接收方的规则以及对公共机构获取个人数据权限的限制和保障措施，评估的重点在于第三国对个人数据的保护是否达到与欧盟对个人数据的保护"实质等同"的程度。Schrems 案[2]建立了"充分性标准"测试，即，第三国关于隐私权保护相关规定的实质内容及该等规定的实施、监督及执行作为一个整体，是否提供了所要求的保护水平。

欧盟-美国隐私盾框架被取代。2016 年 7 月 12 日，欧盟通过了《关于欧盟-美国隐私盾的充分性决定》，其允许将个人数据自由传输给在美国通过隐私盾认证的组织。2020 年 7 月，在 Schrems II[3]案中，欧盟法院认为美国的监控立法违背了《欧盟基本权利宪章》(The Charter of Fundamental Rights of the European Union)，导致欧盟公民的个人数据无法得到应有的保护，因此判决当时适用的《关于欧盟-美国隐私盾的充分性决定》无效。至此，欧盟-美国隐私盾框架不再是将个人数据从欧盟传输至美国的有效机制。

关于新 DPF 框架的洽谈。继 Schrems II 案后，欧盟与美国政府就跨大西洋的个人数据流动展开了洽谈。作为洽谈的重要成果，美国于 2022 年 10 月 7 日通过了第 14086 号行政令《加强美国信号情报的安全保障活动》(Enhancing Safeguards for US Signals Intelligence Activities)，该行政令由美国司法部长发布的《数据保护审查法院条例》(Regulation on the Data Protection Review Court, "AG 条例")作为补充。欧盟委员会对包括美国第 14086 号行政令和 AG 条例在内的美国法律和实践进行全面评估后得出结论，美国对个人数据的保护已达到与欧盟对个人数据的保护"实质等同"的程度。鉴于此，欧盟委员会发布了《充分性决定(草案)》，并决定根据《充分性决定(草案)》适用新的 DPF 框架。

2. DPF 认证程序

DPF 框架的运作系基于一套认证程序。在 DPF 框架下，美国组织自愿向美国商务部("DoC")申请 DPF 认证，同意接受 DoC 发布的欧盟-美国数据隐私框架原则及补充原则(合称"DPF 原则")。自愿参与 DPF 认证的美国组织必须向 DoC 或其指定的其他机构自证其遵守 DPF 原则。尽管参与 DPF 认证的决定是自愿的，但是，一旦美国组织向 DoC 进行自证并公开承诺其遵守 DPF 原则，其遵守 DPF 原则就具有强制性。

美国组织向 DoC 提供的自我认证材料至少应包括以下信息: (1)美国组织名称; (2)美国组织将在 DPF 框架下从欧盟接收个人数据的活动描述; (3)美国组织对个人数据相关的隐私政策; (4)美国组织中处理与 DPF 原则相关的投诉、访问请求和其他问题的联系机构; (5)有权审理美国组织可能存在的不公平或欺骗性行为、违反有关隐私的法律法规的任何索赔的法定机构; (6)美国组织参与的任何隐私计划的名称; (7)核查方法(自我评估或外部合规审查); (8)用以调查 DPF 原则相关申诉的独立追索机制。

同时，为了获得 DPF 认证资格，美国组织必须完成以下事项: (1)同意接受美国联邦贸易委员会("FTC")、美国运输部("DoT")及其他欧盟认可的美国机构的调查与执法; (2)公开承诺其遵守 DPF 原则; (3)按照 DPF 原则修改其隐私政策并公开; (4)充分执行 DPF 原则。

[2] Case C-362/14, Maximillian Schrems v Data Protection Commissioner.
[3] Case C-311/18, Commissioner v Facebook Ireland Limited, Maximillian Schrems.

DoC 将在《数据隐私框架名单》中公开通过认证的美国组织的名称。自被列入《数据隐私框架名单》之日起，相应的美国组织即可适用 DPF 框架进行数据跨境传输。参与认证的美国组织在通过认证之后还需每年重新认证，以证明其持续遵守 DPF 原则。

3. DPF 原则

DPF 框架下规定了若干原则，其构成了 DPF 框架的精髓，具体包括:

- **告知:** 通过认证的组织应向个人告知: 其参与 DPF 框架; 收集的个人数据类型; 美国组织名称; 收集和使用个人数据的目的; 如何联系美国组织; 接收个人数据的第三方的类型或身份; 个人的权利; 美国组织向个人提供的限制使用或披露其个人数据的选项及方式; 免费处理个人投诉并提供适当追索权的独立的争议解决机构; 美国组织接受 FTC、DoT 及其他美国机构的调查和执法; 个人在一定条件下援引有约束力的仲裁的可能性; 为相应公共机构的合法请求而披露个人数据的要求; 其向第三方传输数据情形下的责任。

- **选择:** 通过认证的组织应向个人提供选择(选择退出)的权利，以决定: 是否将其个人信息披露给第三方、用于与最初收集或随后由个人授权的目的实质不同的目的; 对于敏感个人信息相关的上述处理活动，通过认证的组织应获得个人的明示同意(选择加入)。

- **再转移的责任**: DPF 框架规定了通过认证的组织向数据控制者、代理人分别再转移数据的限制。

- **安全性:** 采取合理和适当的措施，以保护个人数据免受损失、滥用和未经授权的访问、披露、更改和破坏，同时适当考虑处理过程中涉及的风险和个人数据的性质。

- **数据完整性和目的限制:** 不得将个人数据用于与最初收集或随后由个人授权的目的不匹配的目的; 确保个人数据相对其预期用途而言是可靠的、准确的、完整的且最新的。相关组织只要保留个人数据，就必须遵守该原则。

- **访问:** 保证个人对其个人数据的访问、更正、修改、删除的权利。

- **追索、执行和责任:** 有效的隐私保护必须包括强有力的机制以确保: DPF 原则得到遵守、因未遵守 DPF 原则而受到影响的个人的追索权、通过认证的组织未遵守 DPF 原则将承担相应后果。

  这一机制至少应当包括:
  (1)随时可用的独立追索机制，在该机制下每个个人的投诉和争议都能依据 DPF 原则获得调查并迅速解决，且无需个人承担任何费用，在适用法律或私营部门倡议规定应当获得赔偿的情形下获得相应赔偿;
  (2)核实通过认证的组织对其隐私实践的证明和断言是否真实、是否确实执行的后续程序;
  (3)通过认证的组织未能遵守 DPF 原则的救济义务和法律后果，对其制裁必须足够严格。

各组织及其选定的独立追索机制必须对 DoC 提出的与 DPF 框架相关的询问和要求作出迅速回应。如果个人按照适用程序和条件以援引有约束力的仲裁，各组织有义务就个人的索赔参与仲裁并遵守相应条款。如果通过认证的组织再转移数据且数据接收方未能根据 DPF 原则处理数据，通过认证的组织对再转移的数据仍然负有责任，除非其能提供相反证据。如果组织因为未遵守 DPF 原则而受制于法院命令或其他美国法定机构的命令，组织应当在符合保密要求的前提下，将其提交给法院或美国法定机构的合规或评估报告中与 DPF 框架相关的部分向公众公开。

- **补充原则：**补充原则针对若干主题事项进行了规定，包括：敏感数据；新闻业的例外情况；次要责任；尽职调查与审计；数据保护机构(通过在欧盟层面设立的非正式的数据保护机构专家组的形式进行运作)的角色；自我认证；核查；个人数据访问权；人力资源数据；再转移的强制性合同；争议解决与执行；选择-选择退出的时间；旅行信息；医药和医疗产品；公开记录和公开信息；公共机构的访问请求。

  关于核查原则，核查目的在于核实通过认证的组织对其隐私实践的证明和断言是否真实、是否确实执行。核查可以通过自我评估或外部合规审查的方式开展。核查结果必须证明其隐私政策符合 DPF 原则、已全面执行隐私政策、对员工开展相应培训、对未遵守相关程序的员工进行惩戒等事项。核查至少每年进行一次。核查记录应妥善保存，以供执法机构调查时出示。限于本文篇幅原因，对此不再展开介绍其他补充原则。

DPF 框架下对于个人权利的救济有许多强制性的规定，这些规定主要散见于各个 DPF 原则中，值得关注的救济规定包括：个人可以直接向相关组织投诉，还可以向组织指定的独立争议解决机构、国家数据保护机构、DoC、FTC 甚至仲裁机构投诉；组织在收到个人投诉后应当在 45 日内向个人主体提供答复；数据保护机构专家组通常应当在收到个人投诉后 60 日内出具处理意见；如果组织在出具处理意见后 25 天日未能遵守意见且未能就此提供合理解释，数据保护机构可能向 FTC 报告进而引起 FTC 执法行动；如果组织未能遵守争议解决机构或自律组织出具的裁决，必须向 DoC、FTC 或有关法院告知组织不合规情况；DoC 承诺其将尽最大努力解决组织不遵守 DPF 原则的投诉；在穷尽了所有救济手段的情况下，个人可援引有约束力的仲裁以解决投诉。

4. 违反 DPF 原则的后果

如果美国组织持续不遵守 DPF 原则，其可能被 DoC 移出《数据隐私框架名单》，不过 DoC 在除名之前将提前 30 日向其发出通知并提供回应机会。

如果美国组织虚假声称其遵守 DPF 原则，还可能被 FTC 认定为违反《联邦贸易委员会法》关于禁止不公平和欺骗性商业行为的规定。FTC 可能通过行政停止令(Cease and desist order)或向联邦地区法院提出申诉的方式来处理相关案件，最终可能导致美国组织被 FTC 处以民事罚款、或因违反联邦法院命令而遭受民事或刑事藐视的追诉。

5. 借鉴意义

《个人信息保护法》对于个人信息的跨境传输规定了三条路径，其中之一即为业界俗称的“认证机制”。自 2022 年 6 月起，关于个人信息跨境传输认证机制的规则陆续发布，包括《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》(“《认证规范》”)和《个人信息保护认证实施规则》。尽管有诸多细节问题有待明晰，中国个人信息跨境传输认证机制的相关法规体系正在逐步完善。(详见通力法评《个人信息出境认证机制展望——以<个人信息跨境处理活动安全认证规范>为起点》)。

欧盟 DPF 框架所依据的充分性决定原则，与“认证机制”的适用场景并不相同。前者适用的是欧盟对“国家/地区”的认定；而后者适用的是中国认证机构对特定数据处理者(或其数据出境活动，仍待明确)的认定。尽管如此，二者所指向的主题事项相似，均试图通过“认证”这一机制，使得符合条件的实体能够实现个人信息的跨境流通，无需“一事一议”地获得提前审批或授权。欧盟 DPF 框架的出台时间点恰逢中国个人信息跨境传输认证立法酝酿之时，或许可以向该种数据保护制度借鉴一二。

- **个人权利救济**

  如上所述，DPF 框架下对于个人权利的救济有许多强制性的规定。此外，作为救济措施的一部分，独立追索机制便捷高效地确保个人权利的保护，确保个人的投诉和争议获得迅速的调查和处理、保证个人获得赔偿的权利、确保未能遵守 DPF 原则的组织受到法律制裁并切实履行其向个人的赔偿义务。

  相较而言，在《认证规范》目前确立的个人信息跨境传输认证机制下，个人信息主体权益主要通过个人信息处理者和境外接收方签订的合同得到保障。尽管合同中应当约定保障个人信息主体权利的途径和方式以及相应的救济措施，但由于在司法体系下个人追索权的实现过于耗时且经济成本高，预计真正提出追索的个人寥寥无几，从现实结果来说，个人信息主体权益难以得到高效且便于落地的保障。因此，从个人信息主体权利的保障而言，可以借鉴 DPF 框架，建立类似追索机制、为个人提供切实的救济途径，使得每个人的投诉和争议都能得到调查、解决和赔偿。

- **核查机制**

  建立有效的监督、核查机制确保已出境个人信息的处理活动确实符合法律法规的要求，也是保护个人信息主体合法权益的关键要素。DPF 框架下的核查机制旨在确保美国组织的隐私实践确实是遵照 DPF 原则实施的。尽管《认证规范》中有类似的监督机制(即个人信息处理者和境外接收方有义务承诺接受认证机构对个人信息跨境处理活动的监督，包括答复询问、配合检查、服从采取的措施或做出的决定等，并提供已采取必要行动的书面证明)，但《认证规范》并未就监督的目的、事项、重点进行规定；监督的范围似乎也限于“个人信息跨境处理活动”，不确定其是否涵盖境外数据接收方对出境数据的处理活动。故可考虑借鉴 DPF 框架、从上述维度对“认证机制”进一步明确和细化。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@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	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	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