关于借鉴欧盟政策加强个人信息跨境传输安全认证制度建设的建议

许皖秀，左晓栋
（中国科学技术大学 公共事务学院，安徽 合肥 230026）

摘 要： 针对如何建设我国《个人信息保护法》第38条确立的个人信息跨境传输认证制度的问题，通过重点分析欧盟数据保护委员会发布的《将认证作为传输工具的指南》中的认证基本框架、对数据进出口方的监管、个人信息主体权利等关键内容，总结该指南关于认证的设计要点与重要结论，提出构建我国个人信息跨境传输安全认证制度的相关建议。

关键词： 个人信息保护；数据跨境传输；数据安全认证
中图分类号： TP3　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2097-1788.2022.06.006
引用格式： 许皖秀，左晓栋. 关于借鉴欧盟政策加强个人信息跨境传输安全认证制度建设的建议[J].网络安全与数据治理，2022，41(6)：40-44.

Suggestions on learning from EU policies to strengthen cross-border transfer of personal information for the construction of a security certification system

Xu Wanxiu, Zuo Xiaodong
(School of Public Affairs, University of Science and Technology of China, Hefei 230026, China)

Abstract: In view of the issue of how to build the certification system for cross-border transmission of personal information established by Article 38 of China's Personal Information Protection Law, this paper focuses on the key contents such as certification criteria, binding and enforceable commitments, and personal information subject rights in the Guidelines for Certification as a Transmission Tool issued by the EU Data Protection Commission, summarizes the design points and important conclusions of the guidelines, and puts forward relevant suggestions for building a security certification system for cross-border transmission of personal information in China.

Key words: protection of personal information; cross-border transfer of data; data security certification

www.ipachina.com

0 引言

我国《个人信息保护法》第38条明确了个人信息跨境传输的几种不同方式，认证为其中之一。2022年11月8日，全国信安标委秘书处发布了《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(征求意见稿)》，并正在组织制定国家标准《信息安全技术 个人信息跨境传输认证要求》。此外，国家网信部门已经发布关于开展个人信息保护认证工作的公告文件。这意味着，我国个人信息跨境传输安全认证制度已进入实质性建设阶段。

个人信息跨境传输安全认证制度是新生事物，面临大量崭新问题[1]。欧盟2018年实施《通用数据保护条例》(GDPR)[2]时，已经提出了数据跨境传输的认证模式，但历经四年仍在探索具体方法。至2022年6月，欧盟数据保护委员会(EDPB)发布2022年第7号指南《将认证用作传输工具的指南》[3](以下简称《指南》)，相关制度设计方告完成。本文对该指南进行了研究，提出了加强我国个人信息跨境传输安全认证制度的建议。

1 全球跨境传输安全认证制度建设的整体情况

1.1 认证制度发展起源

将认证作为数据跨境传输的方式之一是由欧盟GDPR首创的[4]，我国《个人信息保护法》作了借

鉴[5]。但 GDPR 引入认证制度时并非仅面向数据出境,而是为了证明个人信息保护水平。其第 42 条和第 43 条指出,可对数据控制者或处理者的数据处理行为进行认证,并为此规定了各参与方的作用和要求,以及认证和认可过程的总体原则。

最初,欧盟在这方面的主要是探索个人信息保护认证制度的顶层设计,未专门针对数据跨境传输场景[6]。2018 年 5 月,EDPB 发布当年的 1 号指南《关于 GDPR 第 42、43 条的认证和识别认证准则的指南》[7],并于 2019 年 6 月更新至第三版,对认证制度的可重复性原则、问责工具作用、关键概念和认证范围等进行了详细阐释。该文件不是根据 GDPR 进行认证的程序手册,其主要目的是确定 GDPR 第 42、43 条所述各类认证机制的总体要求和认证标准。2018 年 12 月,EDPB 发布当年的 4 号指南《对认证机构的认可》[8],2019 年 6 月更新至第三版。2019 年 2 月,EDPB 发布 2018 年 1 号指南的附录 2《对认证准则的审查和评估》[9]。2021 年 4 月,EDPB 发布 2018 年 1 号指南的补充附录《认证准则评估》[10]。除上述指南文件外,欧盟委员会还于 2019 年 5 月发布了研究报告《数据保护认证机制——对 GDPR 第 42、43 条的研究》,对欧盟个人信息保护认证制度作了系统性研究。但该研究报告不讳言,这一领域还有很多问题尚未有答案。

1.2 认证制度建设最新进展

今年以来,欧盟成员国逐渐开始实施具体的个人信息保护认证制度。2022 年 6 月,EDPB 宣布,卢森堡的国家数据保护委员会(CNPD)已于 5 月 13 日批准其数据安全认证机制 GDPR-CARPA,成为 GDPR 下第一个在国家层面实施的认证。但该制度不适用于数据跨境传输活动,只是数据保护的通用认证。2022 年 9 月,EDPB 对德国北威州数据保护当局提交的 EuroPrise 认证方案草案发表了评论,这是 EDPB 在历史上发表的第二份认证评论。但在该评论中,EDPB 表示没有批准该申请,认为其认证方案会导致 GDPR 应用的不协调,需做较大修改。由此可见,EDPB 对个人信息保护认证制度的建设持十分谨慎的态度。

直到最近,欧盟才在个人信息保护认证制度框架下明确了将该制度用于数据跨境传输时的基本规则。GDPR 第 42 条(2)款和 46 条(2)款提出可将个人信息保护认证用作数据跨境传输的合法依据。即,位于未获得充分性认定的第三国的数据处理者或控制者申请并获得认证,并向数据传输方或认证机构做出有约束力和可执行力的承诺(如合同条款等),即可实施数据跨境传输。2022 年 6 月,EDPB 发布的《指南》,从一般性规定、实施认可要求、具体的认证准则、有约束力和可执行力的承诺四个方面首次明确了个人信息出境安全认证制度的具体要求。但需要指出,现阶段,欧盟尚未将认证制度实际应用到数据出境中,目前并没有实际获得批准的数据跨境传输认证机制,相关工作进展仅限于制度设计。

2 《指南》的要点和重要结论

《指南》着重提出了以下重要观点和要求,而这些观点和要求值得高度关注与借鉴。

2.1 “两步走”模型

GDPR 第 44 条规定,任何向第三国或国际组织传输个人数据的行为应在符合 GDPR 其他条款要求的基础上,遵守 GDPR 第五章(向第三国或国际组织传输个人数据)规定。为此,《指南》给出了一个“两步走”测试模型,如图 1 所示:第一步,数据传

图 1 “两步走”测试模型

www.pcachina.com

输须符合 GDPR 的一般性要求,包括条例第 5 条规定的数据保护原则、第 6 条规定的合法性要求,对特定类别数据(如敏感个人信息)还应符合条例第 9 条要求;第二步,数据传输必须遵守 GDPR 第五章的规定。

2.2 认证基本框架

认证持有者及认证对象。《指南》进一步明确了在使用认证机制进行跨境传输的场景下,应由位于第三国或作为国际组织的数据进口方取得认证,证明其能够为来自欧盟的个人数据提供 GDPR 要求的保护水平。数据出口方和进口方的具体角色(数据控制者或数据处理者)并无限制,不同角色将对应不同的责任,具体如图 2 所示。

认证对象则是第三国数据进口商对欧盟个人数据的所有处理操作。数据进口商在申报认证时,应说明涉及的数据处理操作(包括可能的数据再转移)、数据类型及数据主体类型、传输目的、传输双方角色(控制者和/或处理者),以及发生数据处理操作的国家。

认证机构的定位。欧盟对数据安全认证提出了总体要求,但不指定具体的认证机制。认证机构自身可以开展认证;也可以仅作为合格评定的执行者,根据授权使用其他实体的认证机制开展认证。《指南》首次明确,出于监管机构有效行使矫正权等考虑,认证机构必须位于欧盟境内,其可将合格评定的部分或全部过程外包给数据进口方所在第三国的机构或专业人员执行,但认证决定不允许外包。在允许外包的范畴内,认证机构必须根据国际标准 ISO 17065 中对外部资源的要求以及数据安全监管机构制定的额外认可要求对境外相关承包机构和专业人员进行评估。

证书发放权限。监管部门和获得认可的认证机构均有权执行合格评定并发放认证证书。认证机构在颁发或续签证书时不需要获得监管部门的单独批准,但有责任提前告知监管部门,以便其在必要时行使矫正权,还应向监管部门报告颁发或撤销所申请认证的理由。监管部门的矫正权是指有权撤销本部门颁发的认证、要求认证机构撤销其颁发的认证,或在持证者不再满足认证要求的情况下要求认证机构不颁发认证。

2.3 数据出口方对认证证书的查验过程

根据 GDPR,位于欧盟境内的数据出口方承担数据跨境传输的总体责任,其有义务根据传输和所涉数据的特点核验数据接收方所持认证是否有效且适用,包括:证书是否真实有效且未过期,认证范围是否覆盖了传输活动的具体情形、是否覆盖了个人数据的过境,是否涉及了数据的再转移,相关证明文档是否充分,数据接收方是否与认证机构签订了认证协议等。发送方还应结合双方具体角色(控制者或处理者),评估第三国现行法律和监管实践是否会影响认证的有效性。如数据进口方根据认证要求提出应实施补充性措施,出口方还有义务验证这些措施的有效性和可行性。

2.4 数据过境问题

用作传输工具的认证机制针对欧盟数据传输到第三国以及进口商后续进行的数据操作,但也应明确写出其是否覆盖数据过境的情况(如海底光缆通过其他国家)。如覆盖,则由持证的数据进口方负责其安全;如不覆盖,则由对传输活动承担总体责任的数据出口方负责其安全。《指南》附录针对这两种情况分别给出了补充性措施的示例,如图 3 所示。可以看出,在过境阶段,EDPB 的主要顾虑也是第三国政府强行获取数据。

2.5 保障个人信息主体权利的行使

保障数据主体权利是 GDPR 数据认证的重点考虑之一,包括访问权、更正删除权、限制(使用)权等。为确保数据主体能够获得有效的司法救济并在必要时强制行权(包括提出索赔等主张),《指南》规定,认证准则应要求数据进口方充分说明在相关第三国,数据主体能否以及能在多大程度上行使这些权利,是否需要采取补充性措施来保障其行权,还应要求其建立用于个人行权的投诉处理程序。进出

图 2 数据出口方和进口方具体角色

www.pcachina.com

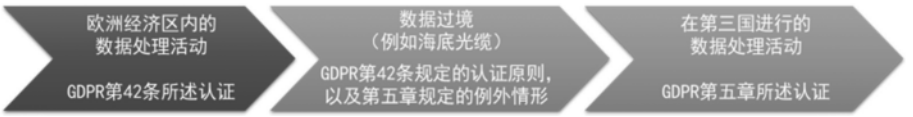

图 3　补充性措施示例

口双方应在约定传输活动的合同(如数据共享合同、服务合同等)明确写出数据主体享有第三方受益人权利,且应为其提供行权机制。即,数据主体有权通过向进口方或主管监管机构投诉等途径,要求进口方执行其在认证下的承诺;在进口方违反认证规定时,数据主体有权援引第三方受益人权利,通过主管机构或主管法院向数据进口方和/或出口方提出索偿等主张;数据主体还可委托非营利机构、组织或协会代表其行使权利。

此外,为保障相关方有效行权,《指南》提出,认证准则应要求数据进口方配合数据出口方的主管监管部门并接受其审计和检查,遵守其决定。

2.6 针对可能影响数据跨境传输安全采取的举措

对第三国法律环境进行评估。《指南》指出,EDPB 对于数据传输至欧盟外的主要顾虑在于第三国政府可能通过对数据进口商的管辖权强行获取数据,或因第三国法律与监管实践的阻碍使数据保护措施失效,以及相关方(特别是欧盟数据主体)难以有效行使其权益。为应对此类风险,《指南》通篇从不同角度多次强调了相关评估要求,数据进口方有义务采用适当、正确的方式对所在国立法情况和监管实践进行评估,还应向认证机构和数据出口方书面承诺,所在第三国法律或实践(包括政府的数据访问要求)不会阻碍其履行认证下的义务,且一旦影响到其履行承诺,将立即通知出口方和认证机构并采取应对措施。

认证机构在开展合格评定时应检查进口方履行评估义务的情况,必要时进行现场审核。为此,认证机构应具备必要的资源,包括与“适当的保护措施”相关的专业知识、对第三国相关法律框架的深入了解以及足够的第三国语言技能等。颁发认证后,认证机构应跟踪关注可能对数据处理活动造成影响的第三国立法和/或判例法变化。数据出口方在对进口方的认证证书进行查验时,应根据双方具体角色(数据控制者或处理者),考虑第三国现行法律和实践下该证书是否有效。如其收到进口方关于法律环境变更可能造成影响的通知,应研判是否即刻终止数据传输。

防止第三国政府部门获取数据。除对第三国法律环境进行评估时应考虑当地政府是否可能强行要求获取数据访问权限外,认证准则还应要求进口方制定应对第三国当局数据访问要求的措施,包括立即通知数据出口方、审查访问要求的合法性等,还应要求不得因第三国当局的数据访问要求而导致大规模、恣意的数据传输情况。

2.7 数据进口方的监督和追责

为防止数据传输到境外后失控,欧盟要求实施有约束力、可强制执行的承诺。形式上主要是两份合同——进口方与认证机构签订的认证合同,以及进出口双方签订的包含进口方所作承诺的合同。在数据传输认证下,数据进口方必须在认证合同中承诺会遵守认证准则(包括关于数据主体权利的准则),且数据出口商和传输所涉数据主体均应作为该合同的第三方受益人。《指南》进一步明确,认证机构应对数据进口方的可追责性进行充分评估,并在签发认证后负责持续监督其客户对认证准则的遵守情况。监管部门可在必要时行使其矫正权。

关于出口商与进口商的合同,《指南》提出,进出口双方可在现有的合同中加入承诺,也可以另外签订单独合同,认证机制可以提供合同模板。不论何种形式,文书中必须写明,数据进口方承诺在处理欧盟个人数据时将遵守认证规则,且第三国法律或实践不会阻碍其承诺的履行。合同中还应写明传输涉及的数据主体享有第三方受益人权利,并提供承诺履行机制。如认证机制覆盖数据再转移情形,也应在合同中说明。

3 对我国的启示

一是将跨国公司分支机构间的数据跨境传输情形与认证相剥离。“约束性企业规则”是欧盟提出的适用于跨国公司分支机构间实施数据跨境传输的机制,但我国《个人信息保护法》未采用这一机制。然而,《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》1.0 版在“适用范围”中实质性纳入了这一工具。从原理看,“约束性企业规

www.bachina.com

则”与认证无必然联系。从欧盟数据出境安全认证制度的设计看,也没有针对跨国公司跨境传输数据场景的特殊考虑。为此,建议将“约束性企业规则”作为《个人信息保护法》第三十八条第一款第四项中“国家网信部门规定的其他条件”,与认证制度分别建立。

二是尽快明确个人信息跨境传输认证制度的整体框架,包括认证范围、参与方及其主要作用、认证过程等。关于认证范围,建议借鉴欧盟方案,广泛定义为境外的数据接收方对我国《个人信息保护法》规范范围内个人信息的全部处理活动。关于认证主体,建议基于我国《个人信息保护法》对“域外效力”的制度设计(法律要求境外数据处理者在境内设立机构或指定代表),明确境外数据接收方是第一认证对象,对境内数据发送方的认证为辅。应在制度层面进行规定,境外数据接收方需接受认证机构的持续监督,必要时接受中方数据安全监管机构的审计或检查。

三是强化对认证机构以及数据进出口双方的监督管理。对认证机构,建议根据国情在现阶段仅明确一家,并加快制定对数据安全评估实验室的认可要求及认证合同模板。关于认证机构职责,可要求其关注对数据接收方所在国法律环境和数据接收方可追责性的评估(传统上认为这不属于认证机构的责任,但欧盟已经作出先例)。考虑到数据接收方所在国的机构更便于对接收方进行监督检查,建议适当允许将部分合格评定和后续监督活动进行外包(可由中检集团等中资机构的境外分支机构负责),并明确允许外包的范围、条件及相关要求。此外,可结合数据分级分类制度,根据拟传输个人信息的敏感程度或数量,对其认证执行不同力度的监管。对数据接收方,建议抓紧制定适用于数据出境安全认证的合同模板及约束性承诺的基本内容,并明确追责机制和相关罚则。对数据发送方,建议进一步明确其对数据跨境传输及可能的数据再转移承担总体责任,在其出境前的自评估过程中纳入对接收方认证证书的核验要求。

4 结论

欧盟《指南》在个人信息跨境传输认证制度的建设方面具有诸多亮点,而我国作为个人信息跨境传输大国,借鉴国外先行经验构建并完善个人信息跨境传输制度具有重要意义。尤其是在《个人信息跨境传输认证规则》已经发布的背景下,做好个人信息跨境传输认证制度的整体框架建设、明确认证适用情形、强化对认证机构与数据进出口双方的监管工作尤为重要,而本文内容对于个人信息跨境认证工作的开展具有实践层面的意义。

参考文献

[1] 张继红.数据认证:模式选择与应用规范[J].中国政法大学学报,2021(2):64-77.

[2] The European Parliament and of the Council.EU General Data Protection Regulation(GDPR)(EU)2016/679[Z].2016.

[3] European Data Protection Board.Guidelines 07/2022 on certification as a tool for transfers[Z].2022-06-14.

[4] 解彦曦,张弛.欧盟《通用数据保护条例》数据保护认证制度研究[J].信息安全研究,2021,7(11):1071-1076.

[5] 童启鑫.欧盟GDPR视域下我国个人信息保护的发展路径研究[J].北京政法职业学院学报,2020(2):99-105.

[6] 高富平.GDPR的制度缺陷及其对我国《个人信息保护法》实施的警示[J].法治研究,2022(3):17-30.

[7] European Data Protection Board.Guidelines 01/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation[Z].2018-05.

[8] European Data Protection Board.Guidelines 004/2018 on accreditation of certification bodies[Z].2018-12.

[9] European Data Protection Board.Review and evaluation of certification criteria[Z].2019-02.

[10] European Data Protection Board.Certification criteria assessment[Z].2021-04.

(收稿日期:2022-11-09)

作者简介:

许皖秀(1999-),女,硕士研究生,主要研究方向:数据安全、数据跨境。

左晓栋(1975-),通信作者,男,博士,教授,主要研究方向:网络安全法、数据安全法。E-mail:hurricane_z@ustc.edu.cn。

www.pcachina.com

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com