CSA GCR cloud security alliance
GREATER CHINA REGION ®

2023年
数据出境合规年鉴

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《2023 年数据出境合规年鉴》由 CSA 大中华区隐私与法律保护工作组内专家撰写，感谢以下专家的贡献：

工作组联席组长：

原浩

贡献者：

邢海韬　　曾令平　　黄鹏华　　贺志生

杨天识　　高健凯　　赵晨曦

贡献单位：

北京启明星辰信息安全技术有限公司　　北京神州绿盟科技有限公司

关于研究工作组的更多介绍，请在 CSA 大中华区官网

（https://c- csa.cn/research/） 上查看。

在此感谢以上专家及单位。如此文有不妥当之处，敬请读者联系 CSA GCR 秘书处给予雅正！联系邮箱 research@c-csa.cn； 国际云安全联盟 CSA 公众号。

序言

毫无疑问，2023 年可称为中国数据跨境监管的元年，这一年初出境评估的“蓬勃”和将近年末的数据出境法律调整“震荡”态势，说明着包括中国在内，数据跨境监管在各种国际和国内因素共同作用下的抉择艰难。尽管如此，作为数据出境的主体，企业需要一种政策和法律的稳定性和预期性，《2023 年数据出境合规年鉴》（以下简称“报告”）正是从企业合规视角出发的一次对中国数据跨境法律的整体梳理。

报告系统的整理了目前中国数据出境监管的法律制度要求，这一制度呈现为基础法律、规范性文件、标准、指南的立体结构，并从原则到已经具有一定颗粒度的指引，说明监管者规范数据出境活动的良苦用心。同时，这一体系化结构也意味着可解释和可例外的场景虽然很多，包括自贸区等先行先试模式在一定区域范围、数据类型、甚至字段级别的“突破”，但整体上不太可能存在“颠覆性”的规则重塑，因此企业所寻求的稳定性和对出境活动后果的可预期性事实上也是清晰和明确的，大可不必为所谓监管的“不确定性”焦虑。进一步的，报告着力于从已经公开的评估、备案信息中，分析和识别一般规律，包括涉及的行业特征、所在区域的省级网信部门的指导能力、企业对可适用出境路径的定性判断等等，这些抽象的、一般的规律性认识，对未来无论是数据出境的细节考虑，还是常态化的企业数据合规建设应都有启发。当然最为重要的是，需要将 CSA 大中华区在数据技术和管理中的最佳实践和较优做法注入到数据出境场景，成为数据跨境企业赋能的一部分，在更广阔的全球范围内分享中国数据跨境的监管规则变迁、落地个案的优劣得失，并将全球主要国家的政策法律进行符合中国跨境监管要求的解读和适配。在秉持中立性的原则下加强和推动不同国家跨境监管制度的交流和协调，为繁荣数字经济和贸易活动贡献力量，这也是启动报告工作的初衷和意愿所在。从这一意义上，这份发起于数据跨境监管元年的报告将只是一个起点、一个尝试。在全球视野下报告所涉及的领域和方向仍将有诸多方向的持续性进展，值得每位报告参与者和关注报告的每位读者保持关注，甚至倾注更多力量。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

致谢 **4**

序言 **5**

1、法律规定 **8**

1.1 网络安全法、数据安全法 8

1.2 数据出境安全评估办法 9

1.3 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 9

1.4 个人信息出境标准合同办法 10

2、指南规则 **11**

2.1 数据出境的路径 11

2.2 数据出境安全评估申报指南（第一版）（摘引） 12

2.3 重点省（直辖市）基于标准合同签署和备案的指南（概要） 17

2.4 个人信息保护认证实施规则（摘引） 18

2.5 个人信息出境标准合同备案指南（第一版）（摘引） 20

3、出境现状 **26**

3.1 已经通过评估情况 26

3.2 已经通过备案的情况 34

4、合规要求与示范 **36**

4.1 指南文件的一般性规范整理 36

4.2 如何确定适用评估或备案 36

4.3 如何认定数据出境行为（活动） 37

4.4 如何识别数据处理者（境内） 37

4.5 如何确定境外数据接收方 38

4.6 如何理解数据出境方式的公网和专线 39

4.7 出境链路描述示范（含云） 40

4.8 确定数据安全负责人的注意事项（境内和境外） 41

4.9 出境合同与业务主合同关系及其他注意事项 41

4.10 附加考虑：不同行业的重要数据识别与安全进展 42

4.11 附加考虑：应当由哪方描述境外数据安全法律政策环境 43

5、数据安全保障能力 44
5.1 收集 45
5.2 存储 46
5.3 使用 47
5.4 加工 48
5.5 传输 48
5.6 提供 49
5.7 共享 50
5.8 删除 51
6、有效的资质认证 52
6.1 网络安全等级保护 52
6.2 ISO 27001 52
6.3 ISO 27017 53
6.4 BCR 53
6.5 PIP-CB 53

1、法律规定

中国数据出境的法律依据主要由《网络安全法》《数据安全法》《个人信息保护法》等基本法律，《数据出境安全评估办法》《个人信息出境标准合同办法》（含配套标准合同）、《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》等多位阶的法规、规范性法律文件构成。

1.1 网络安全法、数据安全法

2021 年 9 月 1 日起施行的《数据安全法》代表了中国数字安全领域法律政策的新努力，特别是数据分类分级保护制度、重要数据目录管理等都将成为监管和执法的新方向，也成为数字行业密切关注的新焦点。围绕《数据安全法》，目前中国正在构造相应的配套制度体系，包括政务数据安全与开放、数据安全审查、数字交易中介规则等，促进数字经济的安全、规范发展。

对于数据出境评估制度，《数据安全法》第三十一条明确："关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定[1]；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定"。这一对"**重要数据**"的规定，与《个人信息保护法》第三十八条对"**个人信息**"规定的："个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件"共同构成了数据出境监管的基本法律来源。

[1] 《网络安全法》第三十七条规定：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

1.2 数据出境安全评估办法

2022 年 5 月，作为上述基本法律重要配套制度的《数据出境安全评估办法》（以下简称“办法”）通过，自 2022 年 9 月 1 日起施行。该办法旨在落实《网络安全法》《数据安全法》和《个人信息保护法》的出境监管要求，规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动。

按照办法，数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息，在触发相应条件时需要进行法定安全评估。数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动，特别是（1）对重要数据明确“数据处理者向境外提供重要数据，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估，”形成监管闭环；（2）规定两种量级的个人信息出境适用安全评估做出规定，设定了对个人信息适用（最严格的）评估监管时的“**上限**”标尺。

1.3 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

2022 年 6 月，全国信息安全标准化技术委员会发布《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》（12 月发布 2.0 版），规定了个人信息的两种出境场景：（1）跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动；（2）《个人信息保护法》第三条第二款[2]适用的个人信息处理活动，正式回应了《个人信息保护法》规定的“按照国家网信部门的规定经专业机构进行个人信息保护认证”的出境条件。

该规范和更早发布的 GB/T 35273《信息安全技术个人信息安全规范》，2022

[2] 《个人信息保护法》第三条第二款规定：在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：（一）以向境内自然人提供产品或者服务为目的；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形。V2.0 规范对此略有调整，但整体上适用范围等同。

年 11 月标准（工作文件）层面的《 个人信息保护认证实施规则》《信息安全技术 个人信息跨境传输认证要求》（至本报告发布日，为征求意见稿）等，共同完成了个人信息出境安全认证路径的监管规范要求。

1.4 个人信息出境标准合同办法

2023 年 6 月《个人信息出境标准合同办法》正式发布，规定了个人信息出境监管的量化“**下限**”：个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形：（一）非关键信息基础设施运营者；（二）处理个人信息不满 100 万人的；（三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；（四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。与之配套的标准合同和备案制度也被广泛认为是中国版个人信息出境标准合同(SCC)。

至此可以认为，《数据出境安全评估办法》《个人信息跨境处理活动安全认证规范》和《个人信息出境标准合同》在具有可操作性的规范性法律文件层面一并完成了中国数据出境监管规则体系的构建。

2023 年 9 月，为对上下限之外的情形做出进一步澄清，国家网信办发布了《规范和促进数据跨境流动规定（征求意见稿）》，明确了无需适用三种出境路径（不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证，但一般不免除需征得个人主体同意的前提条件）的情况：（1）国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，不包含个人信息或者重要数据；（2）不是在境内收集产生的个人信息向境外提供；（3）为订立、履行个人作为一方当事人的合同所必需，如跨境购物[3]、跨境汇款、机票酒店预订、签证办理等，必须向境外提供个人信息的；（4）按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理，必须向境外提供内部员工个人信息；（5）紧急情况下为保护自然人的生命健康和财产安全等；（6）预计一年内向境外提供不满 1 万人个人信息。尽管有解读认为是对上述规定意味着出境监管的放

[3] 例如目前对软硬件在线激活方式中，头部企业已经大量调整了用户条款和隐私政策：用户点击同意，即完成数据出境，而无需再履行标准合同、认证或评估程序，并不再履行本地化存储等义务。

松，但本质上，并未超出《个人信息保护法》第十三条规定的范围，因此本报告更倾向于认为属于法律规定的澄清而非重大调整。

2、指南规则

2.1 数据出境的路径

如上所述，中国数据出境规则实际上构筑了三种不同的路径（汇总如表一所示），且均以有相对完备的规范性法律文件进行界定和约束。实务中，为了指导企业识别自身具体数据情形，规范出境合规动作，提高监管效能，国家网信办进一步通过各个层面制定了更为详细的指引文件。

数据出境路径	申报数据出境安全评估	通过个人信息保护认证	订立个人信息出境标准合同
适用情形	数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估： （一）数据处理者向境外提供重要数据； （二）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息； （三）自上年 1 月 1 日起累计向境外提供 10 万人个	个人信息处理者开展个人信息跨境处理活动，包括以下主体： （一）跨国公司或者同一经济、事业实体下属子公司或关联公司； （二）《个人信息保护法》第三条第二款规定的境外个人信息处理者（即在中国境外处理中华人民共和国境内自然人个人信息以分析、评估境内自然人的行为的	个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形： （一）非关键信息基础设施运营者； （二）处理个人信息不满 100 万人的； （三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的； （四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。 法律、行政法规或者国家网信部门

	人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息； （四）国家网信部门规定的其他需要申报数据出境安全评估的情形。	活动）	另有规定的，从其规定。 个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。
数据类型	个人信息/重要数据	个人信息	个人信息
有效期	2 年	3 年	依合同约定
法律依据	《数据出境安全评估办法》 《数据出境安全评估申报指南》	《个人信息保护认证实施规则》 《个人信息跨境处理活动安全认证规范 V2.0》	《个人信息出境标准合同备案指南（第一版）》

（表一）

本报告对主要的指引文件内容做部分摘录分析，详细原文可见报告末尾援引链接或进一步在网络上检索。

2.2 数据出境安全评估申报指南（第一版）（摘引）

2022 年 9 月，国家网信办（包括主要的省级网信办）陆续出台了配合《数据出境安全评估办法》的指南文件二、数据出境安全评估申报指南（第一版）（“指南”）。指南文件对评估路径的适用范围、申报方式、流程、申报文件体系、解答咨询联系方式等进行了完整规范，成为企业可参照的模板、手册式指导。大部分触发评估条件的企业均有参考或按照指南进行申报准备。

一、适用范围

数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信办向国家网信办申报数据出境安全评估：（一）数据处理者向境外提供重要数据；（二）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；（三）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；（四）国家网信办规定的其他需要申报数据出境安全评估的情形。

以下情形属于数据出境行为：

（一）数据处理者将在境内运营中收集和产生的数据传输、存储至境外；（二）数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；（三）国家网信办规定的其他数据出境行为。

二、申报方式及流程

数据处理者申报数据出境安全评估，应当通过所在地省级网信办申报数据出境安全评估。申报方式为送达书面申报材料并附带材料电子版。

省级网信办收到申报材料后，在 5 个工作日内完成申报材料的完备性查验。通过完备性查验的，省级网信办将申报材料上报国家网信办；未通过完备性查验的，数据处理者将收到申报退回通知。

国家网信办自收到省级网信办上报申报材料之日起 7 个工作日内，确定是否受理并书面通知数据处理者。

数据处理者如被告知补充或者更正申报材料，应当及时按照要求补充或者更正材料。无正当理由不补充或者更正申报材料的，安全评估将会终止。情况复杂的，数据处理者将被告知评估预计延长的时间。

评估完成后，数据处理者将收到评估结果通知书。对评估结果无异议的，数据处理者须按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范相关数据出境活动；对评估结果有异议的，数据处理者可以在收到评估结果通知书 15 个工作日内向国家网信办申请复评，复评结果为最终结论。

三、申报材料

数据处理者申报数据出境安全评估，应当提交如下材料：

1、统一社会信用代码证件影印件

2、法定代表人身份证件影印件

3、经办人身份证件影印件

4、经办人授权委托书

5、数据出境安全评估申报书

6、与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件影印件

7、数据出境风险自评估报告

8、其他相关证明材料

数据处者对所提交材料的真实性负责，提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

指南通过附件形式提供了更为细粒度的数据出境安全评估申报材料要求、经办人授权委托书（模板）、数据出境安全评估申报书（模板）、数据出境风险自评估报告（模板），具有重大参考价值。**特别需要关注的是，对数据出境安全评估申报书（申报表）如何填写，指南提供了一份较为详细的填表说明（见下），解答了申报中的一些常见困惑，仍无法解惑，或需要进一步寻找样例参考的，可参阅本报告第四章：**

常见问题	参考填写方式

申报书 01 项中的单位名称、性质、注册地、有效期、注册资金等怎么填写？	数据处理者应当对照统一社会信用代码证件中的机构名称、机构性质/类型、有效期等栏目填写。单位注册地应具体到城市，如北京市、河北省石家庄市等。单位办公所在地应具体到门牌号，如北京市海淀区 X 路 X 号。表中注册资金均需明确币种和金额。
申报书 02、03、04 项证件类型怎么填写？	可根据实际情况选择填写居民身份证、护照、台湾居民来往大陆通行证、港澳居民来往内地通行证等。
申报书 05 项中数据出境业务描述怎么填写？	据实填写此次申报的数据出境业务，应与法律文件中涉及业务名称一致。
申报书 06 项中数据出境的目的怎么填写？	如开展业务合作、技术研究、经营管理等，需具体阐述。
申报书 07 项数据出境的方式怎么填写？	说明数据出境的方式，如公共互联网传输、专线传输等。
申报书 08 项数据出境链路怎么填写？	说明数据出境的链路，如链路提供商、链路数量与带宽、境内外落地数据中心名称及机房物理位置、IP 地址等。
申报书 09 项拟出境数据情况怎么填写？	关于个人信息的敏感程度，可参照国家标准《信息安全技术 个人信息安全规范》。涉及行业/领域填写出境数据涉及的行业领域范围，如工业、电信、金融、交通、自然资源、卫生健康、能源、教育、科技、国防科工等。
申报书 13 项相关条款在法律文件中的页码怎么填写？	数据处理者填写对应法律文件条款所在的页码，并对相关条款作高亮、线框等显著标识。
申报书 14 项遵守中国法律、行政法规、部门规章情况怎么填写？	数据处理者简述近 2 年在业务经营活动中受到行政处罚和有关主管监管部门调查及整改情况，重点说明数据和网络安全方面相关情况。

指南提供了《数据出境风险自评估报告》的模板文件（略）。在申报材料的撰写中，最为重要的内容主要体现在第三部分，如何对拟出境活动的风险评估情况进行论述，模板文件提供了六个方面的结构参考（但企业需要根据实际情况分别进行针对性的讨论）：

就下列事项逐项说明风险评估情况，重点说明评估发现的问题和风险隐患，以及相应采取的整改措施及整改效果。

（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性**（其中对必要性的论证成为难点，对必要性论证不足，可能导致评估结果为不通过，或部分（字段）不通过）**；

（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全**（包括境内一方作为数据处理者的双方技术、管理制度、措施的进一步参考，见本报告第五章）**；

（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等，是否充分约定了数据安全保护责任义务**（对个人信息类型的数据而言，中国版 SCC 可作为基础参考，但不应作为重要数据类型数据的合同参考）**；

（六）其他可能影响数据出境安全的事项。

有关国家网信办发布指南后，各省级网信部门发布的类似指南文件，可参见公开检索信息（个别细节上不同省市存在细微差异，本报告认为适用国家网信办的指南文件能够满足初步要求，省级指南仅供查漏补缺）。

2.3 重点省（直辖市）基于标准合同签署和备案的指南（概要）

《个人信息出境标准合同办法》自 2023 年 6 月 1 日起正式施行，明确个人信息处理者应当在标准合同生效之日起 10 个工作日内向所在地省级网信部门备案，为指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同，各省市陆续发布本省市个人信息出境标准合同备案指引或通知，并开通个人信息出境标准合同备案咨询电话。

序号	地区	名称	内容
1	北京	2023 年 6 月 2 日，北京市网信办发布《北京市个人信息出境标准合同备案指引》	《指引》适用于所在地为北京的个人信息处理者，备案主体须为法人实体且应与境内合同签署方一致；分公司不具备独立法人地位，不可代替总部或子公司备案。《指引》明确，个人信息处理者应当在标准合同生效之日起 10 个工作日内通过电子版与纸质版方式向市网信办备案，应自行或委托第三方开展个人信息保护影响评估并根据情况进行整改。
2	上海	2023 年 6 月 7 日，上海网信办公布《关于个人信息出境标准合同备案的通知》	《通知》明确，所在地为上海的个人信息处理者，应按照《个人信息出境标准合同备案指南（第一版）》备案材料要求进行材料准备；材料主要包括统一社会信用代码证件、法定代表人身份证件、经办人身份证件、经办人授权委托书、承诺书、个人信息出境标准合同、个人信息保护影响评估报告。个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过送达书面材料并附带材料电子版的方式，向上海市网信办备案。
3	浙江	2023 年 6 月 14 日，《浙江省个人信息出境标准合同备案指引》	《指引》明确了适用范围、备案方式和备案流程等内容，明确所在地为浙江省的个人信息处理者通过订立标准合同的方式向境外提供个人信息并符合规定情形的，应当向浙江省互联网信息办公室备案标准合同；个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过送达书面材料并附带材料电子版的方式，向省网信办备案。

4	重庆	2023 年 6 月 20 日，网信办开通：个人信息出境标准合同备案咨询通道及备案指引	明确所在地为重庆市的个人信息处理者通过订立标准合同的方式向境外提供个人信息并符合规定情形的，应当向重庆市互联网信息办公室备案标准合同；个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过送达书面材料并附带材料电子版的方式，向市网信办备案。
5	广东	2023 年 7 月 10 日 广东省互联网信息办公室《关于个人信息出境标准合同备案的通知》	《通知》明确，所在地为广东的个人信息处理者，应按照《个人信息出境标准合同备案指南（第一版）》备案材料要求进行材料准备；材料主要包括统一社会信用代码证件、法定代表人身份证件、经办人身份证件、经办人授权委托书、承诺书、个人信息出境标准合同、个人信息保护影响评估报告。个人信息处理者先将备案材料电子版（正式扫描件 PDF 版和 WORD 版，光盘）提交所在地级以上市互联网信息办公室，经材料完整性检查后，由所在地级以上市互联网信息办公室送广东省互联网信息办公室。

此外，为了指导和帮助数据处理者规范有序申报数据出境安全评估、备案个人信息出境标准合同，中央网信办公布各地省级网信部门接收申报材料、备案材料的办公地址和联系电话。

2.4 个人信息保护认证实施规则（摘引）

2022 年 11 月的《个人信息保护认证实施规则》实际上包括了个人信息保护认证的一般规则和跨境处理活动的特殊规则两种情况，对第二种情况，主要适用标准在 GB/T 35273《信息安全技术个人信息安全规范》基础上附加了 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》。整体上，规则的重点关注包括（为方便结构理解，保留了原文序号）：

（一）认证模式

个人信息保护认证的认证模式为：技术验证+现场审核+获证后监督

（二）认证实施程序

特别包括了以下程序：

4.2 技术验证

技术验证机构应当按照认证方案实施技术验证，并向认证机构和认证委托人出具技术验证报告。

4.3 现场审核

认证机构实施现场审核，并向认证委托人出具现场审核报告。

4.5 获证后监督

4.5.1 监督的频次

认证机构应当在认证有效期内，对获得认证的个人信息处理者进行持续监督，并合理确定监督频次。

4.5.2 监督的内容

认证机构应当采取适当的方式实施获证后监督，确保获得认证的个人信息处理者持续符合认证要求。

4.5.3 获证后监督结果的评价

认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形做出暂停直至撤销认证证书的处理。

（三）认证证书

5.1.1 认证证书的保持

认证证书有效期为 3 年。在有效期内，通过认证机构的获证后监督，保持认证证书的有

效性。

5.1.3 认证证书的注销、暂停和撤销

当获得认证的个人信息处理者不再符合认证要求时，认证机构应当及时对认证证书予以暂停直至撤销。认证委托人在认证证书有效期内可申请认证证书暂停、注销。

上述规定构成了具有法律约束力的认证规则体系。

2.5 个人信息出境标准合同备案指南（第一版）（摘引）

《个人信息出境标准合同办法》自 2023 年 6 月 1 日起施行。为指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同（“标准合同”），国家网信办制定了标准合同备案指南。

一、适用范围

个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形：

（一）非关键信息基础设施运营者；（二）处理个人信息不满 100 万人的；（三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；（四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

法律、行政法规或者国家网信部门另有规定的，从其规定。

个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

以下情形属于个人信息出境行为：

（一）个人信息处理者将在境内运营中收集和产生的个人信息传输、存储至境外；（二）个人信息处理者收集和产生的个人信息存储在境内，境外的机构、组织或者个人可以查询、

调取、下载、导出；（三）国家网信办规定的其他个人信息出境行为。

二、备案方式

个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过送达书面材料并附带材料电子版的方式，向所在地省级网信办备案。

三、备案流程

标准合同备案流程包括材料提交、材料查验及反馈备案结果、补充或者重新备案等环节。

（一）材料提交（指南并制备了相关文件模板、范本）

个人信息处理者备案标准合同，应当提交如下材料：

1、统一社会信用代码证件影印件

2、法定代表人身份证件影印件

3、经办人身份证件影印件

4、经办人授权委托书

5、承诺书

6、标准合同

7、《个人信息保护影响评估报告》

（二）材料查验及反馈备案结果

省级网信办收到材料后，在 15 个工作日内完成材料查验，并通知个人信息处理者备案结果。

备案结果分为通过、不通过。通过备案的，省级网信办向个人信息处理者发放备案编号；

不通过备案的，个人信息处理者将收到备案未成功通知及原因，要求补充完善材料的，个人信息处理者应当补充完善材料并于 10 个工作日内再次提交。

（三）补充或者重新备案

在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

1、向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；

2、境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；

3、可能影响个人信息权益的其他情形。

个人信息处理者在标准合同有效期内补充订立标准合同的，应当向所在地省级网信办提交补充材料；重新订立标准合同的，应当重新备案。补充或者重新备案的材料查验时间为 15 个工作日。

个人信息处理者对所提交材料的真实性负责，提交虚假材料的，按照备案不通过处理，并依法追究相应法律责任。

就其中核心要素的《个人信息出境标准合同》，我们认为对其把握应考虑几个方面，（1）标准合同不适用修订，因为修订可能会导致部分内容变化无法符合备案出境路径的监管要求，部分修订或导致其适用法律效力降低或无效；（2）在发生与例如欧盟 GDPR 的 SCC 标准合同适用优先性冲突时，应基于“数据源”原则确定合同的优先次序，进而确定适用法律和管辖法院。（3）合同附录一的个人信息出境说明属于实质性内容，应按照企业业务（主合同）的具体数据流程、过程进行表述，在参考标准合同作为评估路径的数据合同时，应注意附录一内容与申报表内容的一致性等等。

就另一重要备案文件《个人信息保护影响评估报告》，指南也提供了规范范本如下：

一、评估工作简述

评估工作开展情况，包括起止时间、组织情况、实施过程、实施方式等内容。如有第三方机构参与评估，需说明第三方机构的基本情况及参与评估的情况，并在相关内容页上加盖第三方机构公章。

二、出境活动整体情况

详细说明个人信息处理者基本情况、个人信息出境涉及的业务和信息系统、出境个人信息情况、个人信息处理者个人信息保护能力情况、境外接收方情况、是否向第三方提供个人信息以及如何确保标准合同条款落实等。包括不限于：

（一）个人信息处理者基本情况

1. 组织或者个人基本信息；

2. 股权结构和实际控制人信息；

3. 组织架构信息；

4. 个人信息保护机构信息；

5. 整体业务与个人信息情况；

6. 境内外投资情况。

（二）个人信息出境涉及业务和信息系统情况

1. 个人信息出境涉及业务的基本情况；

2. 个人信息出境涉及业务的个人信息收集使用情况；

3. 个人信息出境涉及业务的信息系统情况；

4. 个人信息出境涉及的数据中心（包含云服务）情况；

5. 个人信息出境链路相关情况。

（三）拟出境个人信息情况

1. 说明个人信息处理者和境外接收方处理个人信息的目的、范围、方式，及其合法性、正当性、必要性；

2. 说明出境个人信息的规模、范围、种类、敏感程度，处理敏感个人信息和利用个人信息进行自动化决策情况；

3. 拟出境个人信息在境内存储的系统平台、数据中心等情况，计划出境后存储的系统平台、数据中心等；

4. 个人信息出境后向境外其他接收方提供的情况。

（四）个人信息处理者个人信息保护能力情况

1. 个人信息安全管理能力，包括管理组织体系和制度建设情况，全流程管理、应急处置、个人信息权益保护等制度及落实情况；

2. 个人信息安全技术能力，包括个人信息收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等；

3. 个人信息保护措施有效性证明，例如开展的个人信息保护认证、个人信息保护合规审计、网络安全等级保护测评等情况；

4. 遵守个人信息保护相关法律法规的情况。

（五）境外接收方情况

1. 境外接收方基本情况；

2. 境外接收方处理个人信息的用途、方式等；

3. 境外接收方的个人信息保护能力；

4. 境外接收方所在国家或地区个人信息保护政策法规情况；

5. 境外接收方处理个人信息的全流程过程描述。

（六）个人信息处理者认为需要说明的其他情况

三、拟出境活动的影响评估情况

就下列事项逐项说明影响评估情况，重点说明评估发现的问题和风险隐患，以及相应采取的整改措施及整改效果。

（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；

（二）出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险；

（三）境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全；

（四）个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；

（六）其他可能影响个人信息出境安全的事项。

四、出境活动影响评估结论

综合上述影响评估情况和相应整改情况，对个人信息出境活动作出客观的影响评估结论，充分说明得出评估结论的理由和论据。

在实务中具体准备《个人信息保护影响评估报告》时，通常还应参考另一重要的标准类文件《GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南》，并对其中欠缺的出境影响评估部分进行增强和补充。

3、出境现状

本章汇总了截至 2023 年 11 月，公开信息检索到的通过评估、备案方式履行了出境规则合规义务的企业情况，并在此基础上对其中的一些共性特点进行分析和展示。

3.1 已经通过评估情况

编号	申报组织名称	所属行业领域	业务场景	境外接收方所在地	申报受理	地域	公布时间
1	首都医科大学附属北京友谊医院	医疗健康	与荷兰阿姆斯特丹大学医学中心合作研究项目	荷兰	北京网信办	北京	2023 年 1 月 18 日
2	中国国际航空股份有限公司	航空运输	民航旅客数据出境、外航涉及数据出境等场景（未披露，猜测项）	未披露	北京网信办	北京	2023 年 1 月 18 日
3	马自达（中国）企业管理有限	汽车	产品运营情况、销售对象、客户服务等场景（未披露，	未披露	上海网信办	上海	2023 年 5 月 5 日

	公司		猜测项）				
4	丝芙兰（上海）化妆品销售有限公司	快消	未披露	法国（未披露，猜测项）	上海网信办	上海	2023 年 5 月 5 日
5	焦点科技股份有限公司	跨境电商	中国制造外贸电商平台业务	德国、美国（未披露，猜测）	江苏网信办	南京	2023 年 5 月 9 日
6	杭州海康威视数字技术股份有限公司	物联网、智能家居	未披露	未披露	浙江网信办	杭州	2023 年 5 月 24 日
7	杭州萤石网络股份有限公司	物联网、智能家居	未披露	未披露	浙江网信办	杭州	2023 年 5 月 24 日
8	北京现代汽车有限公司	汽车	全业务场景，包括生产采购、索赔管理、全球质量反馈等300多个数据项准予出境	新加坡（未披露，猜测项）	北京网信办	北京	2023 年 5 月 25 日
9	捷普电子（威海）有限公司	软件和信息技术服务业	未披露	美国（未披露，猜测）	山东网信办	威海	2023 年 6 月 9 日
10	支付宝（杭州）信息技术有限公司	软件和信息技术服务业	跨境小程序	未披露	浙江网信办	杭州	2023 年 6 月 19 日
11	绿点科技（深圳）有限公司	软件和信息技术服务业	未披露	美国（未披露，猜测）	广东网信办	深圳	2023 年 6 月 20 日

12	安利（中国）日用品有限公司	快消	部分产品和服务涉及跨境业务（未披露，猜测）	美国、日本等（未披露，猜测）	广东网信办	广州	2023 年 6 月 20 日
13	捷普电子（广州）有限公司	软件和信息技术服务业	未披露	美国（未披露，猜测）	广东网信办	广州	2023 年 6 月 20 日
14	现代中国	汽车	SOTA 升级服务等（未披露，猜测）	韩国（未披露，猜测）	北京网信办	北京	2023 年 6 月
15	丰田中国	汽车	管理产品、提供售后服务及支持、改进产品、研发新产品和新战略、数据分析研究等（未披露，猜测）	日本（未披露，猜测）	北京网信办	北京	2023 年 6 月
16	日产中国	汽车	未披露	未披露	北京网信办	北京	2023 年 6 月
17	连通（杭州）技术服务有限公司	跨境支付	跨境清算等场景	美国（未披露，猜测）	浙江网信办	杭州	2023 年 8 月
18	国泰君安证券股份有限公司	金融业	某涉及数据出境事项的系统	未披露	上海网信办	上海	2023 年 8 月
19	去哪儿网（具体申报主体未披露）	酒店航旅	旅游场景下包括机票、酒店、度假、门票等业务形态在内的用户相关	未披露	北京网信办	北京	2023 年 8 月

			个人数据出境				
20	绿点科技（苏州）有限公司	软件和信息技术服务业	员工管理、供应商管理	美国（未披露，猜测）	江苏网信办	苏州	2023 年 8 月
21	捷普绿点精密电子（无锡）有限公司	软件和信息技术服务业	员工管理、供应商管理	美国（未披露，猜测）	江苏网信办	无锡	2023 年 8 月
22	绿点科技（无锡）有限公司	软件和信息技术服务业	员工管理、供应商管理	美国（未披露，猜测）	江苏网信办	无锡	2023 年 8 月
23	菜鸟	电商物流行业	未披露	未披露	浙江网信办	杭州	2023 年 8 月
24	阿迪达斯体育（中国）有限公司	批发和零售业	未披露	未披露	江苏网信办	苏州	2023 年 8 月
25	厦门航空有限公司	航空运输	海外离港业务（未披露，猜测）	菲律宾、荷兰以及旅客出境目的地所在国家或地区（厦航开通的国际航线）	福建网信办	厦门	2023 年 8 月
26	杭州云片网络科技有限公司（猜测）	科学研究和技术服务业	通讯平台全场景、全字段、数千万量级数据	美国等（未披露，猜测）	浙江网信办	杭州	2023 年 9 月 1 日
27	大众汽车金融（中国）有限	金融业	未披露	未披露	北京网信办	北京	2023 年 9 月

	公司						
28	海南邓白氏数据科技有限公司	软件和信息技术服务业	邓白氏编码商业信息服务业务	纽约（境外接收方：Dun & Bradstreet International, Ltd）	海南网信办	海口	2023 年 11 月
29	海南航空控股股份有限公司	航空运输	海外订座业务相关数据项和海外离岗业务相关数据项	未披露	海南网信办	海口	2023 年 11 月
30	企查查科技股份有限公司	科学研究和技术服务业	企业信用信息境外查询平台	未披露	江苏网信办	苏州	2023 年 11 月 9 日
31	国际航空运输协会	航空运输	北亚区财务结算与分销业务的数据	加拿大、马德里、新加坡	北京网信办	北京	2023 年 11 月

（一）机构汇总

备注：（1）其中“未披露，猜测”以及“部分猜测的申报成功企业”来源于互联网公开渠道、企业公开的隐私政策、业务形态等的综合分析。（2）部分已通过案例并未公开，且预计后续随着评估结果的持续也会不再公开，因此实际通过（未通过）情况应高于本报告汇总。

（二）分析说明

截至 2023 年 11 月，互联网公开渠道公布的已通过申报评估的企业共 31 家。对以上通过国家互联网信息办公室的数据出境安全评估的组织进一步进行分析，本报告尝试得出以下几个结论。

1、遵循属地管辖机制，体现了应合尽合的审核原则

通过对以上申报案例进行分析发现，存在关联关系的企业包括：（1）杭州海康威视数字技术股份有限公司和杭州萤石网络股份有限公司，（2）北京现代汽车有限公司和现代中国，（3）捷普电子（威海）有限公司、绿点科技（深圳）有限公司、捷普电子（广州）有限公司、绿点科技（苏州）有限公司、捷普绿点精密电子（无锡）有限公司、绿点科技（无锡）有限公司。

存在关联关系的公司实体间以独立法人为主体分别申报，体现了数据出境的属地管辖、不同数据处理者分别申报的特点；另一方面，关联公司之间如一家实体申报评估通过，则可为其他关联公司申报积累宝贵经验，支持关联公司申报成功。如上案例虽然体现了属地管辖机制，但给集团企业或关联公司间的申报工作带来了负担，因此通过选择任一链接点，或通过协议安排合并为单一主体成为了目前企业申报主体确认时的重要考虑。对于作为网信部门的受理依据的应合尽合的法律依据和严谨性，还有待国家网信部门给予明确指引。

2、数据出境涉及行业分布广泛

从行业分布看，数据出境申报成功企业主要分布在软件和信息技术服务业（27%）、汽车制造业（17%）、航空运输（13%），金融业、物联网/智能家居、科学研究和技术服务业、快消分别占比 7%。可以看出，软件和信息技术服务业和汽车制造业出海企业在出境合规上响应迅速，通过比例较高。第一批申报成功的卫生行业（友谊医院）和航空运输业（国航）并未如坊间预测，带出同行业一系列申报成功案例。

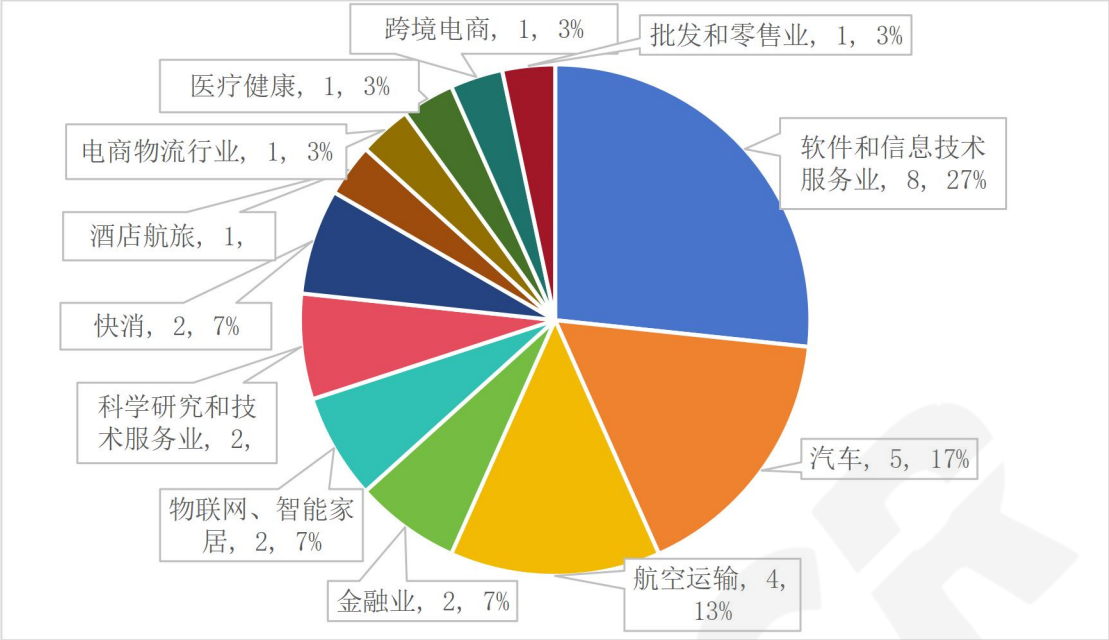

图 1 申报成功企业所在行业分布

3、主要集中在经济发达及沿海地区

从地域分布看，北京市通过申报评估企业有 9 家（数量最多）、浙江有 6 家（均为杭州）和江苏有 6 家（包括苏州、无锡、南京）。体现了这些地域数据出境需求企业众多，监管关注和扶持力度较大的特征，且大多为经济发达及沿海地区。同时，这些省份网信办在数据出境申报评估积累了审核经验，所在区域数据出境需求企业应多和省级网信办沟通，就如何合规出境理解和学习相关经验，提高自身申报评估通过率。

与此同时，随着国务院印发《关于进一步优化外商投资环境加大吸引外商投资力度的意见》，点名支持北京、天津、上海、粤港澳大湾区试点执行“建立绿色通道”、“正面清单”、“建设服务平台”三大措施；《规定》提出自贸区可制定“负面清单”。随着三大措施和负面清单的实践，上述经济发达及沿海地区与自贸区的过审量或将出现快速增长。部分数据出境需求较强，且对“正面清单”受益明显的企业，或考虑搬迁至采取了上述措施的区域。

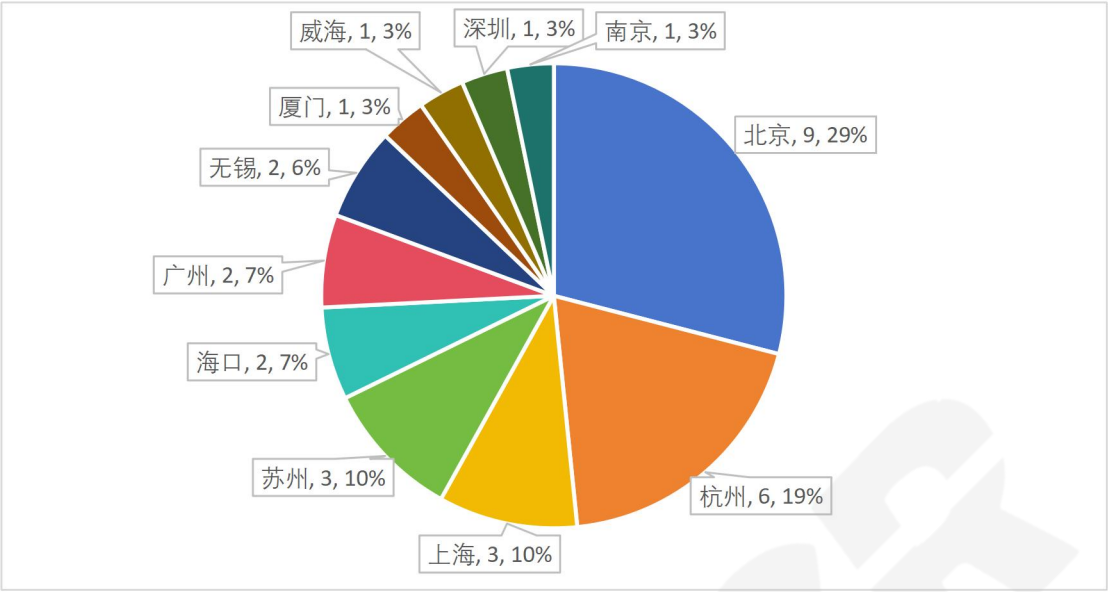

图 2 申报成功企业所在地域分布

4、申报及审批经验缺乏、申报成功率较低

从申报成功时间分布看，2023 年 1 月，北京网信办公布首批 2 家数据出境申报成功企业，为全国数据出境申报评估提供榜样范本。2023 年 5 月、6 月和 8 月，数据出境申报成功企业数量达到高峰，并于 9 月份随着《规范和促进数据跨境流动规定（征求意见稿）》发布逐渐回落。但整体来说，由于数据出境申报相关的法律法规实施时间不长，各地网信部门在不断进行探索，同时大部分企业或服务机构也缺乏申报经验，从而导致当前的数据出境申报效率不高，通过比率仍然很低。如：截至 2023 年 7 月 26 日，上海市网信办已解答咨询电话 4500 余通，接收正式申报材料近 600 件，但彼时上海仅 3 家企业通过数据出境安全评估并对外公布，通过率仅为 0.5%；2023 年 6 月 19 日广东网信办披露“累计收到 220 余份申报材料，其中仅 44 份申报材料通过完备性查验并上报国家网信办”，彼时广东仅 3 家企业通过数据出境安全评估并对外公布，通过率仅为 1.4%。

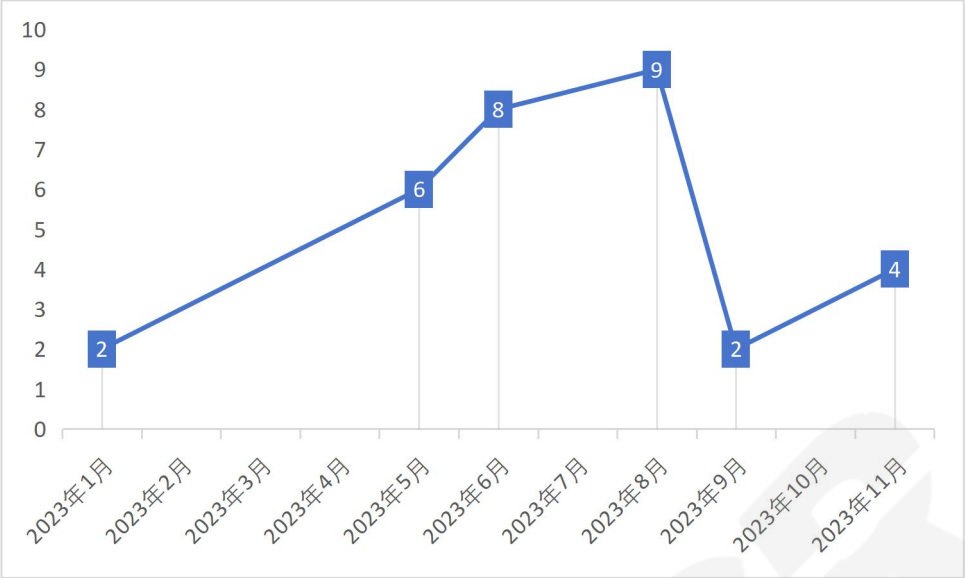

图 3 申报成功企业时间分布

3.2 已经通过备案的情况

（一）机构汇总

编号	申报组织名称	接收方组织名称	所属行业	业务场景	申报受理	地域	公布时间
1	北京德亿信数据有限公司	香港诺华诚信有限公司	信息传输、软件和信息技术服务业	向香港传输与征信相关的个人信息	北京网信办	北京	2023 年 7 月 10 日
2	邦贝液压机械（杭州）有限公司	未披露	制造业	未披露	浙江网信办	杭州	2023 年 7 月 10 日
3	信华信（大连）软件服务股份有限公司	日本某株式会社	信息传输、软件和信息技术服务业	未披露	辽宁网信办	大连	2023 年 7 月

4	海南省星创互联网医药有限公司	未披露	批发和零售业	未披露	海南网信办	海南	2023 年 9 月
5	捷德（中国）科技有限公司（猜测）	未披露	制造业	在华机构的员工个人信息、客户数据	江西网信办	南昌	2023 年 9 月
6	武汉科斯德尔玛检测技术服务有限公司	未披露	科学研究和技术服务业	未披露	湖北网信办	武汉	2023 年 10 月
7	伟创力技术（长沙）有限公司	未披露	信息传输、软件和信息技术服务业	未披露	湖南网信办	长沙	2023 年 11 月

（二）分析说明

通过备案企业共 7 家，分别位于北京、浙江、辽宁、海南、江西、湖北、湖南，从对外公布的数据来看，发现主要场景为跨国公司人力资源管理、征信业客户信息跨境。个人信息出境标准合同备案成功企业也不多，可能原因在于个人信息出境标准合同备案路径的企业仍处于法定整改期（2023 年 11 月 30 日之前）。但事实上，个人信息出境标准合同备案相较于个人信息保护认证更加便利，程序简单，备案也侧重于形式审查，将成为大多数企业个人信息出境的路径选择。

可以预见，随着《规范和促进数据跨境流动规定（征求意见稿）》的发布和即将正式施行，以及个人信息保护认证实施规则和认证机构的明确，使用标准合同备案、第三方安全认证的出境企业将大幅增加。未来会有较多企业通过备案、认证等方式实现合规出境，而《规范和促进数据跨境流动规定（征求意见稿）》提出的自贸区等更为灵活的白名单方式，更为高效、安全、便捷的数据跨境活动提供了更多可能。

4、合规要求与示范

4.1 指南文件的一般性规范整理

对三种出境路径的具体指南文件，其体例上通常包括：（1）明确的适用范围，企业据此确认适用的出境路径，或无需启动任一路径的依据；（2）申报方式与流程，企业需要对具体的文件提交方式、份数、反馈要求等进行了解；（3）申报材料的构成，此部分通常会给出申报材料的空白表单、报告模板和解释等，可直接使用；（4）作为支持文件的其他证明材料，此部分一些企业实务中未予重视，实际上是确认其符合出境规则的“底稿”。一般应包括企业的组织架构、数据安全制度、开展的第三方认证等文件，以确保企业在申报材料中的描述符合真实性、有效性和充分性的要求。

除指南文件（包括数据出境安全评估申报指南（第一版）等）中的填表说明等解释外，本章提供了进一步的解读供企业决策、判定参考。

4.2 如何确定适用评估或备案

适用评估的情形目前明确有：（一）数据处理者向境外提供重要数据；（二）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；（三）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息。

适用标准合同备案的情形明确为：（一）非关键信息基础设施运营者；（二）处理个人信息不满 100 万人的；（三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；（四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

从上述规定，以及《规范和促进数据跨境流动规定（征求意见稿）》，预计一年内向境外提供不满 1 万人个人信息的，不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

据此，根据 1 万以下、1 万到 100 万、100 万以上量化数据分别对应不需要履行任何行政程序、履行备案、认证、评估的各类情形均已有明确。

4.3 如何认定数据出境行为（活动）

指南明确的数据出境行为包括：（一）数据处理者将在境内运营中收集和产生的数据传输、存储至境外；（二）数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出。概况而言，第一类可以定性为直接出境（有些主体也称之为主动出境），第二类为可访问（或间接出境、被动出境）。

需要明确的是，目前所有涉及数据出境都是在网络空间的前提下讨论的，如果主体通过便携设备、移动介质等物理机制携带、邮寄、托运出境的，不属于《数据出境安全评估办法》规定的出境，但可能受到《出口管制法》《海关法》等其他约束。

4.4 如何识别数据处理者（境内）

从已知案例分析，境内的数据处理者通常是涉及海外直接投资业务（如在境外设立实体的走出去中企）、大中型跨国企业（特别是境外跨国公司的境内实体）、在线贸易（电子商务和支付支持等）、外包服务（如软硬件服务）、中外合作（主要涉及医药、测评等）。数量和涉及行业并未完全反映跨国贸易的全貌，但随着评估申报和备案工作的进展，应该会有更多的覆盖。

通常而言，境内数据处理者应通过营业执照内容体现形式上的主体信息完备性，这可以通过国家企业信用信息公示系统、第三方征信机构的信用报告中快速实现基本资料的获取和填写。

在实质性认定上，特别是涉及多主体、多数据来源的情况下，数据处理者应当是对境内所产生、运营的数据具有支配和控制地位，应当判断哪一主体具有最终和决定性的作用和地位。这也是体现评估工作 “应合尽合”的要求。

一些常见的参考包括：（1）通过股权关系，判定哪一主体为股东或具有股权上的控制权；（2）通过境外集团或总部的决定或授权安排；（3）通过协议中的权利义务约定，确定对数据在境内的处理权限和最终决策层级。

另外需要注意的是，按照《个人信息保护法》规定，“个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。未经个人信息处理者同意，受托人不得转委托他人处理个人信息。”“接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。”

因此受托人一般不属于数据处理者，其仅需要向个人信息处理者（数据处理者）负责。

4.5 如何确定境外数据接收方

境外的数据接收方通常存在几种可能：

（1）最为典型的是与（境内）的数据处理者存在传统意义上的业务、商业关系的主体，比如境内的生物医药类企业作为数据处理者为境外的客户提供样本采集、检测等服务中，数据作为附随资料，受到双方协议的约束，或者成为协议约定的交付物，此时客户应作为境外数据接收方；

（2）在数字经济业态下，数据和基于数据分析形成的交付，也成为跨境业务、商业活动的直接标的，在在线信息交互的场景下，金融、保险、征信等数据直接成为了协议规制的标的，这在新近通过的评估案例中也得到了印证；

（3）另外一种典型情况是存在同处于一个实际控制人的跨国集团企业，集

团在不同国家设立的实体会基于人力资源、业务管理、售后维护等原因进行数据跨境，此时境外的集团、总部可作为数据接收方，但如其不具有最终控制力和决策权的，应适当穿透和将实际控制人（如上市公司可作为境外数据接收方，但无需将其实际控制权的自然人作为数据接收方）作为数据接收方。

（4）未来需要关注的一种情况和跨国集团企业类似，中国企业“走出去”会形成一种反向的数据跨境活动。在这一模式下，实际控制人的所谓总部可能位于境内，从而对境外的数据接收方具有控制作用和支配地位。这种情况同时还涉及境外数据的入境，进而会导致适用境外法律的问题。

这也说明本质上，数据跨境是一个动态和连续的业务过程，如果将其割裂为出境、入境，则不利于企业经营以及整体上的数字贸易活动。

对于数据处理者是否可以和境外数据接收方为同一主体，《数据出境安全评估办法》和《数据出境安全评估申报指南（第一版）》设立了一种基于合同或协议法律保障的机制，在这种机制的结构下，个人信息的主体权利是否可以得到保障，是基于境内的数据处理者和境外的数据接收方的协议，特别是违约责任和法律适用得以实现，如果数据处理者是否可以和境外数据接收方为同一主体，则意味着协议机制的失灵（或至少是打折），因为主体的实质性混同将削弱保障的法律实现，因此一般而言数据处理者是否可以和境外数据接收方为同一主体不常见，也非鼓励的出境主体模式。

4.6 如何理解数据出境方式的公网和专线

数据出境的方式，指南文件列举了两种典型，公共互联网传输、专线传输。实务中两种方式可以做进一步细分，且在一定情形下也可能存在重合，或组合的情况。

需要注意的是，填写和描述出境方式，不应仅简单的选择公共互联网传输、专线传输，而应对整体的出境方式进行过程性描述，即数据如何启动或触发传输、传输可能的跨境路径、如何进入境外接收方的系统，特别是需要考虑加密等技术

措施如何在传输过程中得到应用等等。

此外，同一类型的数据，也可能通过不同的方式“重复”出境，这也要求对不同出境方式所使用的程序功能、涉及数据的业务的流程进行适当的对应表述。

4.7 出境链路描述示范（含云）

通过和运营商的协议或沟通，可以获得基本的出境链路信息。目前比较规范的表述方式举例如下（当然实务中也存在如何表述无 IP 或数据中心地址不详等问题的考虑等）：

链路供应商：[•]（可适当援引通讯服务提供商信息，或境外提供商及在境内的业务合作方）

链路数量：1

带宽：[•]GB

模式：专线传输

链接方式：点对点专线

公网 IP 地址：

境内数据中心：

境外数据中心：美国微软 Azure 云，位于[•]的数据中心

（云）服务器 IP 地址：

境外数据接收方 IP 地址：

4.8 确定数据安全负责人的注意事项（境内和境外）

对于已经有信息安全或网络安全架构的企业而言，在其组织架构内增加表述数据安全负责人主要涉及内部的决策和职责描述。

对于没有基本安全架构的企业，或者境内没有专门机构的企业而言，需要考虑一个较高层级的安全负责人和规范的任命程序，因其需要对安全事务负责，并需要与网信办等监管机构建立联系。同时也需要梳理和说明境内的安全负责人与境外的总部或集团安全负责人的上下级关系。

此外需要注意，对数据安全负责人的国籍并无强制性要求，主要是在确定安全事项，或发生安全事件响应时，能够与监管机构建立联系、接受问询，因此具有国内经常居住地的人士具有优势，这也是为何需要提供负责人身份信息（电话、邮箱、证件号码）的考虑。

4.9 出境合同与业务主合同关系及其他注意事项

在《数据安全法》和《数据出境安全评估办法》之前的企业业务中，业务合同可能并未充分考虑数据出境问题，因此在《数据出境安全评估办法》和指南要求进行合同条款的引述时，最直接的“补救”方式是在境内的数据处理者和境外数据接收方之间签署一份单独、但从属于业务主合同的“数据合同”作为补充或者附件。

对于数据类业务，则在业务主合同中可能已经存在大量的数据出境条款，但从已知案例看，此类数据出境主要引用了欧盟 GDPR 的标准合同，可能需要按照中国的《个人信息保护法》和中国版的个人信息出境标准合同进行调整。

此外需要注意的是，不能用个人信息出境标准合同替代出境合同，因为个人信息出境标准合同适用的是无需评估，仅需进行合同备案的“小量”个人信息出境场景，其设定的基线条款不一定完全满足出境评估的要求。更不应以个人信息出境标准合同作为“重要数据”出境评估的参照。

在申报材料中引用出境合同作为主要的法律文件时，除了需要复制和展示中文条款内容外，还需要对文件的名称、页码进行标注，以方便监管机构审核时快速、准确的检索和比对。

4.10 附加考虑：不同行业的重要数据识别与安全进展

目前已知的涉及重要数据识别和安全保障的规定包括：

（1）2022 年 4 月后，《信息安全技术 重要数据识别规则》进行了较大调整。整体上，该规则给出了识别重要数据的“影响对象”维度的细粒度要素要求。将国家安全、经济运行、社会稳定、公共健康和安全 4 大类细化为 19 小类影响对象。

（2）2022 年 9 月的《网络数据分类分级要求（征求意见稿）》进一步给出了如何细化“影响程度”的参考规则。

（3）《汽车数据安全管理若干规定（试行）》确认的汽车领域重要数据。

（4）《人类遗传资源管理条例实施细则》

（5）《智慧民航数据治理规范 数据安全》

（6）《工业和信息化领域数据安全管理办法（试行）》

（7）《中国禁止出口限制出口技术目录》

（8）《信息安全技术 重要数据处理安全要求》

值得注意的是，按照 2023 年 9 月的《规范和促进数据跨境流动规定（征求意见稿）》，“未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。”因此，数据处理者是否申报重要数据出境，取决于前置的部门、领域重要数据识别条件，鉴于目前除汽车领域外，尚无正式的重要数据识别规则施行，因此可以预见涉及潜在的重要数据申报出境

的处理者，将有一个较为充裕的缓冲期，可借此时机建立、完善和规范内部重要数据安全管理制度和措施。

4.11 附加考虑：应当由哪方描述境外数据安全法律政策环境

境外数据接收方对境外的数据安全法律政策环境更为熟悉，但数据出境评估、备案中，往往会由境内的数据处理者或者第三方评估机构起草数据安全法律政策环境，这就要求境内数据处理者或者第三方评估机构对全球主要国家、地区的法律、政策有整体和系统的了解。尽管在审核、备案实务中对此部分的描述没有苛刻的表述要求，但一般也应能够涵盖到数据出境后的所在国主要的法律、政策内容，并能够反映新近的变化和发展趋势。

如下的初步的美国数据安全法律政策环境可作为报告撰写参考。比较而言，其他国家在欧盟 GDPR 前后多已制定或修改国内个人信息保护立法，较之美国法律的体系和案例相对简单：

境外接收方所在国美国在个人信息保护方面没有统一的法律，主要由联邦和州法律组成多层级、相对独立的复杂体系。

在联邦法律层面，《联邦贸易委员会法》广泛授权美国联邦贸易委员会采取执法行动，作为主要的监管机构保护消费者免受不公平或欺骗性行为的影响，并执行联邦隐私和数据保护法规。

综合性法案还包括《联邦隐私法案》和《电子隐私法案》等。两者主要限制政府机构如何收集、使用和存储个人信息，包括对电子通信（如电子邮件）的搜索和监控。儿童信息在联邦层面受到《儿童在线隐私保护法》（COPPA）等的保护。行业方面的典型法案包括《证券交易法》和相关法规，是适用于上市实体的主要法律规范。该法要求上市公司在发生重大事件，包括网络事件时应在上市公司公告等文件中进行披露。《健康保险携带和责任法案》（医疗电子交换法案 HIPAA）、《公平信用报告法》等主要用于保护个人健康信息等数据。

1998 年 10 月，美国颁布《防止身份盗窃及假冒法》，该法对美国法典中关于个人信息犯罪内容进行了修正，将身份盗窃犯罪纳入到刑法中，将侵犯身份信息犯罪归纳为八种方式。这些生效法案及修订对各种非法利用个人信息的行为进行明确的界定。

此外，美国是 2001 年 11 月由欧洲委员会的 26 个欧盟成员国以及加拿大、日本和南非等 30 个国家布达佩斯所共同签署国际公约《（打击）网络犯罪公约》（Cyber-crime Convention）的缔约国之一。2022 年，首个获得两党、两院支持的联邦层面数据隐私法草案——《美国数据隐私和保护法（草案）》提出，但与美国的立法传统存在一定差异，是否通过仍存在不确定性。《云法案》在 2018 年 3 月颁布，位于美国境外但被美国法院认为“与美国有足够联系且受美国管辖”的外国公司也适用于执法场景的数据获取，据此境外接收方所在国可能基于执法或司法上需求对境外接收方数据提出管辖。

整体上，个人信息（隐私权利）在美国法具有中特别突出的法律价值，隐私权得到美国从联邦和州层面的普遍认可，并建立了相对完整的个人信息和隐私保护的程序和实体法。在发生侵害个人主体隐私或个人信息权益时，具有相应的程序法和案例法寻求救济的途径。但通常认为这些法律规定主要保障美国公民或所在州的个人信息，对境外个人信息的保护能力相对有限，这也是为何包括中国版 SCC 在内，在协议中强调司法管辖权的缘由。

5、数据安全保障能力

指南文件核心要求，除数据出境的合法性、正当性、必要性外，主要就是对境内数据处理者和境外数据接收方的数据安全保障能力进行评估和评价。不仅如此，保障能力实际上也构成对“正当性”的必要支撑，是在法律文件的“约定控制”外的技术和管理维度的能力体现。技术、管理与协议共同构成了数据处理者风险控制能力，是出境监管规则的重要关注。

指南文件要求对数据安全管理能力和数据安全技术能力分别进行评估描述。实务中企业也多分别从技术措施和管理制度方面分别展开。本报告注意到了指南

文件的风险控制用意，同时从技术措施和管理制度的共性出发，考虑从数据生命周期的收集、存储、传输、使用、提供、加工、披露/公开、删除各个阶段，导入常见和典型的安全技术保护措施和管理制度，并在各个生命周期阶段列举了部分（非全部）可供参考的部分标准、指南类文件，范围上涵盖到国家标准、行业标准、团体标准等等。在适用中可以分别引用，也可作为综述或框架性指引。需要强调的是，数据生命周期并非简单和机械的区分，事实上大量的最佳实践在不同的数据生命周期阶段都有应用，典型的如访问控制策略、配置和制度，与之对应，《信息安全技术—个人信息安全规范》（GB/T 35273-2020）等标准也体现出对不同周期阶段的整体适用。

5.1 收集

个人信息和重要数据的分类分级要求是目前数据安全在“出境导向”下安全能力建设的原点。因此围绕分类分级，适用不同情形分别取得个人主体同意、重要数据的对象（客户）的同意，是生命周期安全治理的首要任务。本报告认为，在数据分类分级制度、数据资产管理制度、隐私政策、用户协议等层面建立的合法合规合理收集机制，无论其形式和结构如何，均应至少关注以下基线，从而在业务合规的根本性上建立、规范和牢固数据收集行为：

数据的收集需满足最小必要等原则；

应从字段级的粒度，论证收集数据应具有明确、合理、具体的处理目的，仅收集实现处理目的所必要的最小范围的数据；

基于同意机制收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等个人信息处理规则，并获得个人信息主体的明示同意，不能使用默认勾选同意等方式；

若通过第三方进行数据收集，如嵌入可收集个人信息的 SDK 等，需和第三方明确数据处理规则和保护责任，要求第三方处理活动满足相关要求；

需要从数据源出发确定数据收集的法律适用。例如，在中国法的标准合同与（如）欧盟 GDPR 的标准合同发生冲突时，应以数据主体作为选择法律适用的事实依据，避免产生法律适用的困惑，从而无法准确界定收集的各类数据的权属、权益。

与收集相关的标准、指引类文件可参考《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》，或进一步的行业类文件如《汽车采集数据处理安全指南》等。

5.2 存储

存储阶段涉及数据在境内和境外保存地点、期限、安全处置等问题。应通过数据加密等方式保障安全，特别是对重要数据和敏感个人信息，强烈建议应使用加密等保障方式。同时，数据加密操作不当、配置错误或加密漏洞等反而容易导致数据丢失或引入其他风险，因此除了需要相关系统、技术支持外，还需要相应完善的管理制度，包括需要建立数据加密和密钥管理规定以及具体的操作流程等细化规则。

存储的数据加密可以简单分为三个层次，可以依据安全和合规要求选择：

一是文件级别加密。从操作系统或文件系统层面对数据存储的载体数据库文件进行加密操作。可实现文件级别的加密，力度粗糙；

二是表级别加密，即透明加密。通常由数据库厂商提供，在数据库引擎中实现，以达到数据在数据库共享内存中以明文的形态存在，在数据文件中以密文形式存储，实现效率性能和安全的平衡。可实现对表级别的加密，力度相对粗糙；

三是列级别或字段级别加密，即对数据明文进行加密后再存储到数据库。字段级别的可实现在数据表中，仅对具体某个具体类型的重要数据或敏感个人信息进行加密，如身份证号，而其他非重要数据或敏感个人信息以明文的形式存在。加密力度精细，可依据具体要求来选择需要进行加密的字段或列。加密算法建议

选择强度不低于 AES-256 或对应国密算法的算法。

此外，密钥是数据加解密操作的关键，遗失密钥意味着数据没有解密就不可用。实际使用中还会涉及多级密钥分发等问题，因此需要使用密钥管理系统（KMS）管理密钥的生命周期，包括密钥生成、密钥导出、密钥分发、密钥导入、密钥存储、密钥使用、密钥备份和恢复、密钥销毁、密钥归档等。

与存储相关的标准、指引类文件可参考《T/CITIF 002-2023 数据存储安全能力成熟度模型》等。

5.3 使用

使用环节对应指南文件的数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等内容。通常使用阶段可通过访问控制、去标识化展示、安全审计等来保障安全。同样除了需要相应的系统、技术支持外，还需要建立访问控制的管理制度，对使用过程中的访问控制要求等内容进行规定。

通过统一认证和访问控制实现对数据使用中涉及的各类系统进行管理和安全水位对齐。统一认证确保各系统的认证方式以及涉及的密码策略可以保持一直的安全基线，避免各系统密码强度不一致等问题。

访问控制旨在对各系统中涉及重要数据或敏感个人信息的权限进行识别和管理，为基于风险的控制策略和配置提供基础。可根据权限中是否可以涉及重要数据或敏感个人信息，对权限进行分级、角色和配置实施。

统一认证和访问控制的同时也对各系统的访问日志进行统一收集和管理，便于后续对日志开展安全审计的工作，形成从实施到验证再到改进的迭代循进。

与使用相关的标准、指引类文件可参考《GB/T 37964-2019 信息安全技术 个人信息去标识化指南》《T/TAF 139-2022 电信和互联网个人信息保护能力审计规范》等。

5.4 加工

数据加工根据参与方的不同可以分为自身加工和与第三方加工两种方式。如果是数据处理者自身加工数据，则数据处理目的不能超过收集数据时所使用的范围，同时也需要满足最小必要的原则，仅使用实现目的所需要的最小范围。

如果是与第三方共同加工的方式，（就个人信息而言）可采用相应的隐私增强技术进行安全保障，特别是在无法和无需取得个人信息主体同意的情况。通过隐私增强技术可以实现接收方在无法识别特定自然人且不能复原的前提下，仍能进行汇聚融合等加工。常见的隐私增强技术路线主要有：

安全多方计算（MPC）：是解决一组互不信任的参与方之间在保护隐私信息以及没有可信第三方的前提下协同计算问题而提出的理论框架。保障多个参与方进行协同计算并输出计算结果的同时，各个参与方除了计算结果之外无法获取任何其他信息。

联邦学习（FL）：用于建立一个基于分布数据集的联邦学习模型，是一种在原始数据不出库的情况下，协同完成机器学习任务的学习模式。

可信执行环境（TEE）：是一种具有运算和储存功能，能提供安全性和完整性保护的独立处理环境。其基本思想是：在硬件中为敏感数据单独分配一块隔离的内存，所有敏感数据的计算均在这块内存中进行，并且除了经过授权的接口外，硬件中的其他部分不能访问这块隔离的内存中的信息。以此来实现敏感数据的隐私计算。

与加工相关的标准、指引类文件可以包括更细粒度的隐私计算的参考文件，如《JRT 0196-2020 多方安全计算金融应用技术规范》等。

5.5 传输

数据传输包括了确保数据在境内主体之间、从境内向境外传输、境外可能

的向第三方提供过程的安全考虑，是指为防止数据传输过程中的数据泄露采取的一系列数据（主要是）加密保护策略和安全防护措施。重点需要梳理以下几个维度的安全：

明确负责数据出境传输安全工作的团队及其工作职责；

出境传输通道两端主体的身份鉴别；

在出境数据分类分级的基础上，根据业务出境的场景，制定出境数据加密传输方案及出境传输通道的加密方案；

梳理出境数据传输接口，形成出境接口清单；

使用行业最佳实践或不低于通行惯例的加密传输算法和协议，例如 TLS 1.3；

开展接口调用日志记录及监控审计，评估加密算法和协议安全漏洞等。必要时应引入第三方渗透测试等方式评估验证安全性。

与传输相关的标准、指引类文件可参考《T/ZIIC 003-2022 工业互联网数据传输安全技术要求》等。

5.6 提供

出境数据的提供与使用部分用途、方式重合，特别是在涉及员工个人信息等方面，除了使用环节外，提供应增加关注数据的访问控制（境内与境外的权限可能不同）、备份与恢复等内容。其中数据的备份与恢复是指通过规范出境数据存储的冗余管理工作机制，保障数据的完整性和可用性。重点需要梳理以下几个维度的安全：

明确负责出境数据备份与恢复工作的团队及其工作职责；

制定出境数据备份与恢复的操作规程；

建立出境数据备份与恢复清单；

建立出境数据备份与恢复平台，按照上述清单定制执行备份，并对备份数据完整性和可用性进行验证。

出境数据访问控制安全，是指出境数据访问过程中通过身份识别与访问控制管理、公钥基础设施等安全防护措施以保障出境数据访问控制的安全，其与传输、存储安全也密切相关。重点需要梳理以下几个维度的安全：

明确负责出境数据访问控制策略的团队及其工作职责；

制定出境数据访问控制身份鉴别与访问控制、公钥基础设施等策略；

梳理出境数据访问控制的接口及数据类型，形成出境数据接口清单；

开展访问控制接口调用日志记录及监控审计。

与向境外数据接收方提供相关的标准、指引类文件方面，除了与境内数据处理者参考《网络安全标准实践指南———网络数据分类分级指引》和更细粒度的行业文件如《智能网联汽车数据分类分级实践指南》等，以确立一致性的数据分类分级前提之外，还应综合参考前述标准评价境外数据接收方的角色和安全能力。

5.7 共享

共享安全是确保出境不同组织间的数据交互过程中的安全而采取的一系列措施。需要注意的是，目前的数据出境规则对向第三方共享提出了较高的业务必要性要求，企业应先行评估共享的必要性，并重点需要梳理以下几个维度的安全：

明确负责出境数据共享安全工作的团队及其职责；

针对出境数据的脱敏、溯源、留存期限、监控审计、共享接收方的身份鉴别、共享平台或接口的访问控制等维度制定相应的安全策略；

明确出境数据共享双方的安全责任，尤其是接收方的安全责任，应在出境数据共享过程中，对接收方的出境数据安全防护能力（作为整体）进行评估。

与共享相关的标准、指引类文件最重要的参考包括《信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求》等。

5.8 删除

尽管删除并非《数据安全法》界定的数据处理活动，但确实符合中国出境规则合规性的重要环节，其与提供服务的终止、账户的注销等个人主体权益关系密切。删除需要对数据及其存储介质实施相应的操作手段，使得出境数据彻底消除且无法通过任何手段恢复，以符合《个人信息保护法》规定的匿名化目标。重点需要梳理以下几个维度的安全：

明确负责出境数据删除工作的团队及其职责；

根据出境数据分类分级情况，结合出境业务场景需要，明确不同的删除方法和删除工具；

建立出境数据台账清单，确保过期、过线出境数据按时删除；

对数据删除过程全程记录，并对数据删除效果进行评估；

针对已外部共享的出境数据，明确删除记录并作验证。

与删除相关的标准、指引类文件可综合性的参考《GBT 37988-2019 信息安全技术 数据安全能力成熟度模型》等。

此外，当涉及更细化的数据类型或交易场景时，则需要进一步考虑其他参考或针对性的进行评价。例如，采用《GB/T 41819-2022 信息安全技术 人脸识别数据安全要求》对涉及人脸信息的数据进行全生命周期考虑。

6、有效的资质认证

指南文件要求提供数据安全保障措施有效性证明，包括数据安全风险评估、数据安全能力认证、数据安全检查测评、数据安全合规审计、网络安全等级保护测评等等。本部分罗列了目前行业普遍认可的一些有效的资质认证供组织合规性参考。

6.1 网络安全等级保护

网络安全等级保护是指对网络（含信息系统、数据）实施分等级保护、分等级监管，对网络中使用的网络安全产品实行按等级管理，对网络中发生的安全事件分等级响应、处置。

“等级保护 2.0”或“等保 2.0”是一个约定俗成的说法，指按新的等保护标准规范开展工作的统称。通常认为是《网络安全法》颁布实行后提出，以 2019 年 12 月 1 日，《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》正式实施为象征性标志，也是最核心的要求规范文件。在出境监管规则中，尽管为强制要求必须通过等级保护，但毫无疑问，通过适当等级保护的系统、网络具备符合出境规则的基本条件。

6.2 ISO 27001

ISO 27001 是信息安全管理体系的国际标准，旨在通过明确的管理控制实现信息安全。 最早由英国标准协会（BSI）于 1995 年 2 月提出，并于 1995 年 5 月修订而成。1999 年 BSI 重新修改了该标准。ISO 27001 目前最新版本是 2022 版。标准化后的 ISO/IEC 27001 是一个正式规范信息安全管理体系 (ISMS) 的安全标准，规定了定义如何实施、监控、维护及不断改进 ISMS 的各项要求。此外，其中还规定了一系列最佳实践，包括文档编制要求、责任划分、可用性、访问控制、安全性、审核，以及纠正和预防措施。

ISO 27001 认证已经成为企业核心竞争力的重要标志，通过 ISO/IEC 27001 认

证，有助于组织遵守与信息安全有关的各种法规及法律要求，并为包括中国在内的大多数国家所认可（并已经通过中国国标转化适用）。

6.3 ISO 27017

ISO 27017 旨在帮助云服务提供商实施和维护信息安全管理体系(ISMS)，并为客户提供高质量的云服务。该标准建立在 ISO 27001 基础上，并专门关注云计算环境中的信息安全风险和管理控制。它提供了云服务提供商和客户之间的共同框架，以确保信息安全和隐私得到充分保护。通过获得 ISO 27017 认证，云服务提供商可以证明其采取了适当的信息安全措施，符合国际标准和客户的需求和期望。同时，客户也可以通过查看认证证书，确认云服务提供商的信息安全水平。

6.4 BCR

BCR 规则是指约束公司规则（Binding Company Rules），它们有时被称为全球数据保护的“黄金标准”。这些规则最初由欧盟委员会创建，目的是方便个人数据的跨境转移。现在，它们已在 GDPR 第 47 条中明确表示允许跨境数据转移。BCR 是欧盟 GDPR 规定的数据跨境传输机制之一，特别适用于跨国公司内部的数据跨境传输。为了指引 BCR 的制定、申请与审批，EDPB 第 29 条工作组分别针对数据控制者和数据处理者发布了工作文件，即 BCR-C 和 BCR-P。目前在跨国企业涉及欧盟业务的集团架构中得到应用，可作为符合个人信息出境规则的参考性资质，以支持中国法下的数据出境合规性。

6.5 PIP-CB

PIP-CB 认证指包含跨境处理活动的个人信息保护认证，适用范围是个人信息跨境处理活动，该认证的价值在于符合个人信息跨境处理合法路径之一。在认证已经方面，目前已生效的国家标准《个人信息安全规范》为个人信息保护认证的合规控制点，信安标委秘书处发布的《认证规范》作为标准技术性文件支持（可进一步参见本报告第一章的第三部分内容）。

CSA GCR cloud security alliance GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905