个人信息保护合规准则

—— 中国篇

CSA GCR cloud security GREATER CHINA REGION alliance ®

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

《个人信息保护合规准则-中国篇》由 CSA 大中华区数据安全工作组内个人信息保护合规准则项目组专家撰写，感谢以下专家的贡献：

项目组组长：

高巍　　王玮

主要贡献者：

曾令平	陈丑亚	付艳艳	黄妍昕	李沈舟
廖振勇	罗进	王彪	王玮	邢海韬
余其玄	原浩	张兵	张淼	

参与专家：

曾令平	陈丑亚	戴才良	丁哲轩	方伟
付艳艳	高巍	顾伟	黄妍昕	姜国春
黎伊帆	李安伦	李沈舟	廖振勇	陆建松
罗进	时培宇	王彪	王玮	王永霞
王泽	邢海韬	余其玄	袁荣婷	原浩
张兵	张淼	张元恺	赵帅	赵勇智

贡献单位：

OPPO 广东移动通信有限公司	安信与诚科技开发有限公司
北京谷安天下科技有限公司	北京神州绿盟科技有限公司
北京微步在线科技有限公司	北京天融信网络安全技术有限公司
广州熠数信息技术有限公司	杭州美创科技有限公司
杭州世平信息科技有限公司	杭州天谷信息科技有限公司
华为技术有限公司	奇安信网神信息技术（北京）股份有限公司
上海淇毓信息科技有限公司	深圳国家金融科技测评中心有限公司
天翼安全科技有限公司	腾讯云计算（北京）有限责任公司
浙江大华技术股份有限公司	长春吉大正元信息技术股份有限公司

（以上排名不分先后）

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。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号

序言

当今社会，随着互联网技术的不断发展，个人信息保护问题越来越受到人们的关注。在这个信息化时代，个人信息已经成为了一种重要的资产，而其泄露和滥用也给个人带来了巨大的风险和损失。为了保护个人信息的安全和隐私，各国纷纷出台了相关法律法规和标准。

中国《个人信息保护法》于 2021 年 11 月 1 日正式实施。该法规定了个人信息处理者必须遵守一系列合规要求，包括合法、正当原则、目的明确、最小必要原则、公开透明原则、质量保障原则和确保安全原则等。这些要求对于所有处于《个人信息保护法》管辖范围内的个人信息处理者都是具有普适性的。

报告旨在为处于《个人信息保护法》管辖范围内的个人信息处理者提供系统性的实施指导。该报告包含了个人信息保护合规基本要求的相关内容，包括原则、方法论框架等方面。报告提供了一个结构化的“合规要求-控制措施及规程说明-其他考虑”的框架，以指导个人信息处理者在处理活动中应遵守的规范。具体而言，该框架包括以下四个部分： 1.个人信息识别 2.个人信息保护合规基本要求 3.个人信息专项保护要求 4.合规监测改进。每个部分都包含了一些具体的合规控制项和控制细项，共计 12 项合规控制项和 106 个控制细项。通过遵循该文件提供的指导和建议，个人信息处理者可以更好地履行其保护个人信息安全和隐私的责任。

我们希望这份《个人信息保护合规准则—中国篇》能够对广大读者有所帮助，并为促进我国个人信息保护事业做出贡献。

李雨航 Yale Li

CSA 大中华区主席兼研究院

目录

1 总则

1.1 背景

在大数据时代，日新月异的互联网技术带来更加快捷便利的生活，打破时间和空间的限制为用户提供更贴合现代化生活节奏的服务，与此同时也让个人信息面临更多的风险，如被泄漏、滥用等。为加强个人信息保护，在《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国民法典》等已有个人信息保护规定的基础之上，2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》（下文简称《个人信息保护法》），并于 2021 年 11 月 1 日起正式施行。

《个人信息保护法》正式实施后，在网信部门的统筹管理下，各行业监管部门也通过开展一系列的行动推进本行业、本领域开展个人信息保护工作，国家及行业相关配套标准相继发布，但大多数个人信息处理者在个人信息保护合法要求落地实践中仍处于探索阶段，本行为准则在这样的背景下产生。CSA 个人信息工作组结合现行法律法规、国家标准及业界最佳实践，为个人信息处理者提供系统性的实施指导，帮助个人信息处理者承担保护用户个人信息的责任，降低合规风险。本行为准则包含大量来自实际场景的案例或举例，帮助个人信息处理者准确理解控制措施的含义。

1.2 目标

基于《个人信息保护法》及其他相关法律法规制定第一版普适性的行为准则，旨在解决企业的合规挑战，面向所有处于个人信息保护法管辖范围内的个人信息处理者，没有针对行业、领域或规模的特定限制。

在达到全面合规的基础上，重点解决在事务工作中的难点问题，包括：个人信息处理活动中的落地合规要求、委托处理者的管理、个人信息跨界管理、个人信息安全影响评估实施等内容。

1.3 遵循原则

1.3.1 合法、正当原则

合法原则是指个人信息处理者应严格遵循法律、行政法规的规定，采取合法的方式，不得违法处理个人信息。

正当原则是指处理个人信息的行为必须是正当的，处理者不应当通过不公正的方法，如通过欺骗或者在信息主体完全不知情的情况下来处理其个人信息。

1.3.2 目的明确、最小必要原则

目的限制原则要求必须是为了特定、明确、合法的目的而收集个人数据，否则不得收集或进行其他的处理活动。

1.3.3 公开透明原则

公开透明原则是指个人信息处理者在处理个人信息时应当采取公开、透明的方式，公开个人信息处理的规则，向信息主体明示个人信息处理的目的、处理的方式和处理的范围。

1.3.4 质量保障原则

质量保障原则是指个人信息处理者应当保证其所处理的个人信息的质量，避免因为个人信息的不准确、不完整对个人权益造成不利影响。

1.3.5 确保安全原则

确保安全原则是指个人信息处理者应当采取必要措施保障所处理的个人信息的安全，防止出现个人信息的泄露或者被窃取、篡改、删除。

1.4 范围

行为准则旨在为处于《个人信息保护法》管辖范围内的个人信息处理者提供系统性的实施指导，并参考了 10 余项我国个人信息保护相关的法律、行政法规及国家标准，并提供了最佳实践可以作为遵守《个人信息保护法》的指南及合规工具使用。任何行业和规模的个人信息处理者都可以使用本行为准则作为实践指导，遵守和实施相关的控制措施将在一定程度上降低合规风险。

行为准则通过结构化的“合规要求-控制措施及规程说明-其他考虑”展现个人信息处理者在处理活动中应遵守的规范，准则内容主要包括个人信息识别、个人信息保护合规基本要求、个人信息专项保护要求、合规情况监测改进四大部分内容，12 项合规控制项，106 个控制细项：

个人信息识别（共 1 项）：

包括一般个人信息和敏感个人信息识别方法及示例。

个人信息保护基本要求（共 3 项）：

1） **组织机制：**包含组织内部个人信息保护架构设计和人员的设置。

2） **个人主体权利的响应：**包含识别个人信息主体基本权利，同时帮助处理者响应个人主体基于合法权利的请求。

3） **个人信息处理活动中的安全合规要求：**从个人信息处理活动各阶段的维度梳理个人信息保护的要求，从技术落地方面提供支持性控制措施的建议。

个人信息专项保护要求（共 6 项）：

1） **敏感个人信息保护：**包含处理敏感个人信息的加强要求。

2） **未成年人个人信息保护：**针对处理个人信息中的高风险场景提出额外的措施和说明，包含敏感个人信息的处理、未成年（不满 14 周岁）个人信息的处理

3） **组织自身的变化下的合规要求：**主要包括合并、重组、分立、解散、破产情形下，个人信息如何处理的问题。

4） **共同处理者与委托处理者的管理：**共同处理者与委托处理者的判别及管理过程的各阶段。

5） **自动化决策场景下安全合规要求：**自动化决策下的个人信息处理原则及基本要求。

6） **个人信息跨境：**针对数据跨境流程中各个环节提出了控制措施，包含跨境前需进行的评估活动，跨境中提供的保护措施以及和监管机构沟通的要求。

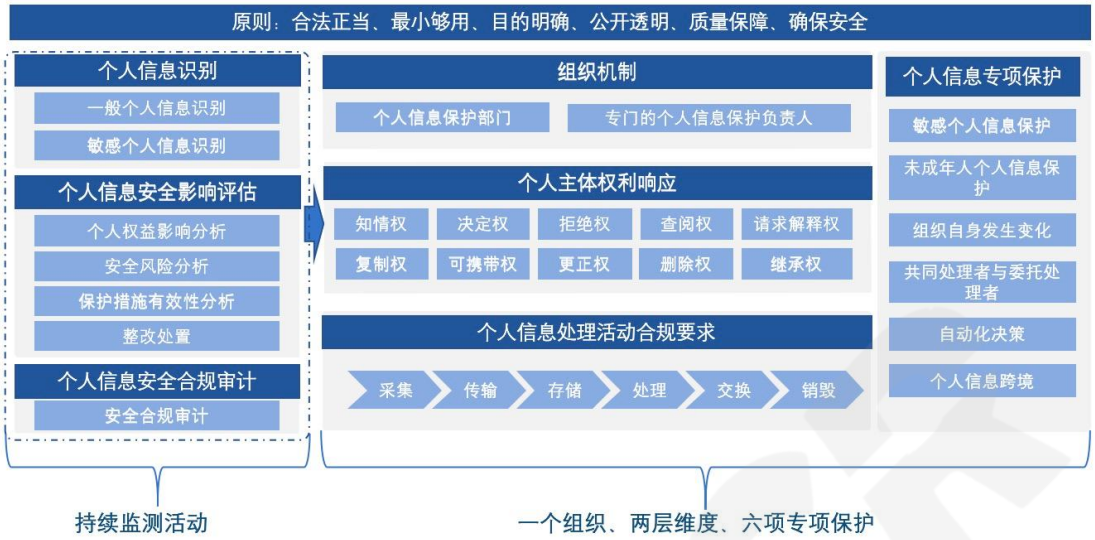
合规监测改进（共 2 项）：

1）**个人信息安全影响评估：**个人信息安全影响评估的适用情形及其方法流程。

2）**个人信息安全合规审计：**个人信息安全合规审计的基本要求。

注：个人信息作为一类特殊且敏感程度高的数据在企业内部需严格保护，满足数据安全保护工作的所有要求，行为准则将不再复述这一类要求。

1.5 方法论框架



注：为确保覆盖《个人信息保护法》中的个人信息处理活动的各阶段，将个人信息处理活动与本章节的处理活动各阶段做了映射：

类别	对应关系					
本文章节号及名称	3.3.1 收集安全	3.3.2 传输安全	3.3.3 存储安全	3.3.4 使用安全	3.3.5 共享安全	3.3.6 删除安全
个人信息处理活动（《个人信息保护法》中列举）	收集	传输	存储	使用、加工	提供、公开	删除

2 个人信息识别

序号	合规要求	控制措施及规程说明	其他考虑
2-1	对个人信息实行分类管理；	制定一个信息分类策略，对个人信息实行分类管理，对识别出的个人信息和敏感个人信息打上标签。	在实践场景下，通常使用自动化的分类分级工具来进行自动化的数据识别和分类分级
2-2	个人信息识别	将以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息识别为个人信息并打上标签。可参考《信息安全技术 个人信息安全规范》附录 A。	包括：“直接标识个人信息”；“准标识个人信息”指对通过信息结合、聚合等方式可以实现识别个人的准标识信息；“关联个人信息”并标签化：基于已知个人信息，所产生或发现的与之身份关联的信息
2-3	敏感个人信息识别	将一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息识别为敏感个人信息。可参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》附录 B、GB/T 41807-2022《 信息安全技术 声纹识别数据安全要求》 、GB/T 41819-2022《信息安全技术 人脸识别数据安全要求》	其中生物特征识别数据是指脸部特征、指纹、虹膜、声音、基因、步态、笔迹等可识别自然人的生理特性与行为特征的信息。由于人生物识别信息要更改非常困难，如指纹、掌纹、虹膜、基因信息等生物识别信息，一旦被泄露，就会对自然人的人身财产安全产生不可逆转的损害。个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。
2-4	对“匿名化个人信息”进行验证和标注：	匿名化后的个人信息不再认定为个人信息，但需结合 GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 37964-2019《信息安全技术 个人信息去标识化指南》等确认匿名化措施的有效性。	一般认为，严格和绝对的匿名化措施并不存在，只能在特定场合与现有技术水平下对其效果进行评价。 组织需注意：去标识化和匿名化具有法律意义上的本质区别，不应通过已去标识化就确认实现了对个人信息的匿名化。

3 个人信息保护合规基本要求

3.1 组织机制

序号	合规要求	控制措施及规程说明	其他考虑
3.1-1	管理层应在公司治理的整体层面考虑个人信息保护	管理层应在组织的整体治理框架中写入个人信息保护相关内容，并体现在章程或组织其他基本纲领文件中。应将个人信息保护作为对管理层和其他职能部门考核、评价的组成部分。	
3.1-2	组织应在个人信息保护官或其他角色下设立专门的个人信息保护部门机构	应建立专门的个人信息保护部门，或在既有的部门机构中增加对个人信息保护的描述，例如内部控制部门、信息安全支持部门等，该等部门接受个人信息保护官或其他角色的领导。	个人信息保护部门机构需要其他机构的协助，例如法务部门。
3.1-3	组织应设立专职或兼职的个人信息保护官，负责个人信息保护相关事宜	应通过组织董事会等程序，在组织日常经营负责人（总经理）的职责中增加个人信息保护内容，或由日常经营负责人委派其他专门人员担任。负责全面统筹个人信息保护工作。	一般建议不低于公司副总经理的层级。组织应考虑配套相应人员、财力等支持个人信息保护。
3.1-4	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人员设置	应指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。	建议满足以下条件之一的组织考虑设置: 1）主要业务涉及个人信息处理，且从业人员规模大于 200 人; 2）处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息: 3）处理超过 10 万人的个人敏感信息的。
3.1-5	提供重要互联网平台服务、用户数量巨大、	成立主要由外部成员组成的独立机构对个人信息保护情况进行监督，并履行以下义务：	

	业务类型复杂的个人信息处理者	1）按照国家规定建立健全个人信息保护合规制度体系； 2）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务； 3）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务； 4）定期发布个人信息保护社会责任报告，接受社会监督。	
3.1-6	境外组织如涉及中国境内个人信息处理的，	境外组织如涉及中国境内个人信息处理的，应当在中国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务。	负责人姓名、联系方式等应报送履行个人信息保护监管职责的部门。
3.1-7	涉及处理儿童人个人信息时应当设置为成人人个人信息保护负责人	组织应当指定专人负责个人信息保护，在必要业务场景下应由个人信息负责人授权人员完成相应的保护工作；	

3.2 个人信息主体权利响应

序号	合规要求	控制措施及规程说明	其他考虑
3.2-1	权利响应及投诉机制	1）应建立投诉机制和投诉跟踪流程，并且在合理的时间内对投诉进行响应 2）设置显著的渠道（例如用户页面展示）及接口部门确保个人信息主体可以及时受理用户的申请，并进行相关的处置 3）告知的渠道和方式可参照 GB/T 35273-2020《信息安全技术 个人信息安全规范》附录 C 执行。	1）应明确相应接口部门的应答口径和技术承接部门的处理机制，并留存相应的处置及解释说明记录；； 2）相应时间不建议超过 15 天，并应当留存处置记录；

3.2-2	个人信息主体享有知情权、决定权、拒绝处理权	公开个人信息处理规则，以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息的处理目的、方式，处理的个人信息种类和保存期限，以及个人行使权利的方式和程序等，个人信息处理规则发生变更时，应当告知个人信息主体 ； 在处理个人信息前或个人信息处理规则发生变更时，确保通过《个人信息处理规则》获得个人信息主体自愿、明确的同意。 企业应当为个人信息主体提供便捷的撤回同意的途径和方式，不得以高于授权同意的标准作为撤回授权的前提；不得以拒绝提供服务或限制服务功能作为撤回授权的前提，除非获得授权是提供相关服务所必需的。 隐私政策的制定可参照 GB/T 35273-2020《信息安全技术 个人信息安全规范》附录 D 执行。	个人信息处理者处理敏感个人信息的，应向个人信息主体告知处理敏感个人信息的必要性以及对个人权益的影响； 如公开《个人信息处理规则》、建立个人信息保护“双清单”，或通过 APP 弹窗、站内信、短信等方式及时告知用户； 避免 APP 更新迭代时，私自变更个人信息授权状态或强制开启授权同意。
3.2-3	个人信息主体享有查阅权、复制权、可携带权	应当为个人信息主体提供便捷的查阅、复制、转移其个人信息的途径和方式，不得以时间、位置等因素对其合理请求进行限制。	
3.2-4	个人信息主体享有更正权	应当为个人信息主体提供申请更正、补充个人信息的渠道； 当接收到个人主体要求更正、补充个人信息时，应当予以核实，并及时做出响应。	
3.2-5	个人信息主体享有删除权	若处理目的已经实现、无法实现或者为实现处理目的不再必要，应当立即删除； 停止提供产品或者服务，或者保存期限已届满，应当删除；	当法律、行政法规规定了保存期限时，处理者与个人约定的保存期限不得少于法律、行政

		基于个人同意处理的个人信息，当撤回同意时，应当删除；	法规规定的保存期限；
3.2-6	个人信息主体享有要求解释权	应建立与个人信息主体的沟通渠道，当个人信息主体要求解释处理规则时，应当给予详细的解释； 应建立对个人主体请求沟通的完整响应过程并留存；	应避免仅使用自动化工具进行响应和回复，特别是个人主体要求人工介入时。
3.2-7	个人信息主体享有继承权	应确定死者与近亲属身份； 应评估请求权利的合法、合理性，及与组织个人信息处理规则的一致性； 提供的个人信息应限定使用范围； 应在法律规定期限内响应，并形成和保留查阅、复制、更正、删除的记录和日志； 由于死者的个人信息包括范围大于近亲属主张，应避免直接提供死者个人信息的完整副本。	应确认死者生前是否有其他安排

3.3 个人信息处理活动中的安全合规要求

3.3.1 个人信息收集安全

序号	合规要求	控制措施与规程说明	其他考虑因素
3.3-1	真实性、合法性和安全性	对采集的数据和数据源进行合法性确认，支持身份鉴别、记录和过程的可追溯，防止数据仿冒和数据伪造。 通过个人用户终端受理终端、客户端软件、浏览器等方式收集时应采取加密等技术措施保证信息数据的保密性，防止被未授权的第三方获取，采取技术措施（如弹窗、明显位置 URL 链接等），引导个人用户查阅隐私政策	
3.3-2	个人信息采集最小化	收集个人信息，应限于实现处理目的的最小范围，且与实现产品或服务的业务功能有直接关联，保障收集个人信息的最少数量、最短周期、最低频次、最小精度，采取对个人权益影响最小的方式，不得过度收集个人信息。	

3.3-3	数据质量的管理	对个人信息进行质量管理和监控，实现异常数据及时告警或更正。避免因个人信息不准确、不完整对个人权益造成不利影响。	
3.3-4	在公共场所安装图像采集、个人身份识别设备	在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。	

3.3.2 个人信息传输安全

考虑到个人信息与数据的技术实现逻辑是一致的，故本小节的控制措施参考了《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》的 7.1.2 部分。

序号	合规要求	控制措施与规程说明	其他考虑因素
3.3-5	传输节点的安全认证	在建立传输加密通道前，对传输通道两端的主体身份进行鉴别和认证，确保数据传输双方是可信任的。	
3.3-6	传输通道加密	对个人信息传输通道采用 TLS/SSL 等安全协议，防止传输过程中的个人信息的泄露。	
3.3-7	传输数据的内容加密	1）传输敏感个人信息时，应采用加密、去标识化、脱敏、隐私计算及身份认证技术等安全措施，保护传输内容的安全； 2）应对传输的个人信息进行完整性校验，并支持数据容错或恢复	密码技术的使用应遵循《中华人民共和国密码法》。

3.3.3 个人信息存储安全

个人信息存储安全有个大的前提：个人信息处理者在中国境内收集和产生的个人信息应当在存储在中国境内。同时，本小节控制措施参考了《GB/T 35273 2020 信息安全技术 个人信息安全规范》的 6.3 部分，为个人信息处理者提供了可落地的操作指引。

序号	合规要求	控制措施与规程说明	其他考虑因素
3.3-8	存储时间最小化	1）个人信息的保存期限应当为实现处理目的所必要的最短时间； 2）超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。	《反洗钱法》要求客户身份资料、客户交易信息在交易结束后， 应当至少保存五年。 《电子商务法》要求商品和服务信息、交易信息保存时间自交易完成之日起不少于三年。
3.3-9	去标识化处理	1）对个人信息实行分类分级管理，并采取与个人信息等级相适应的密码技术、假名化技术、抑制技术、泛化技术、随机化技术等对收集个人信息进行去标识化处理。 2）将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。使其在不借助额外信息的情况下，达到无法识别个人信息主体的效果。	
3.3-10	个人敏感信息的存储	对个人信息处理者的要求包括： 1）存储个人敏感信息时，应采用加密等安全措施； 2）个人生物识别信息应与个人身份信息分开存储； 3）原则上不应存储原始个人生物识别信息（如样本、图像等）	对于生物识别信息的存储， 1）原则上不应存储原始个人生物识别信息，可采取的措施：仅存储个人生别信息的摘要信息； 2）在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能； 3）在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

3.3.4 个人信息使用安全

序号	合规要求	控制措施与规程说明	其他考虑因素
3.3-11	个人信息访问控制措施	个人信息处理系统的访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； 对个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。	确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；
3.3-12	界面展示限制	涉及通过界面展示敏感个人信息的，个人信息处理者应对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。 可脱敏处理技术包括：统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术、数据合成技术。具体可参照 GB/T 37964-2019《信息安全技术个人信息去标识化指南》	在控制重标识风险的前提下,结合业务目标和数据特性,选择合适的去标识化模型和技术,确保去标识化后的数据集尽量满足其预期 的(有用)
3.3-13	用户画像的合规使用	1）用户画像中对个人信息主体的特征描述，不应包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；表达对民族、种族、宗教、残疾、疾病歧视的内容。 2)除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。	在业务场景下使用用户画像，可采用隐私计算等技术，不对外直接提供用户身份标识
3.3-14	个人信息加工安全	1)应对涉及个人信息的数据分析需求进行了人工审核，对数据分析的数据源、数据分析需求、分析逻辑进行审核，以确保数据分析目的、分析操作等方面的正当性，针对具体的数据分析场景制定了相应的个人信息保护方案。 2）应采用差分隐私、K 匿名等技术，降低个人数据分析、加工过程中数据泄露风险。	

3.3-15	不能将生物识别特征作为唯一个人身份认证方式	数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息。	

3.3.5 个人信息共享披露

序号	合规要求	控制措施与规程说明	其他考虑因素
3.3-16	个人信息合法共享	1）任何组织、个人不得非法买卖、提供或者公开他人个人信息；在向他人提供个人信息时，应当进行合规性审批； 2）应事先获得用户的单独同意；	在法定情形下的共享包括：根据法律法规规定、监管要求、诉讼争议解决需求，或按行政、司法机关依法提出的要求，对外共享的个人信息。
3.3-17	第三方信息共享、转让	1）个人信息处理者应向个人告知个人信息接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类； 2）征得个人信息主体的单独同意； 3）事前进行个人信息保护影响评估，评估数据接收方的身份和数据安全能力，采取有效的措施保护共享、转让过程的数据安全； 4）通过合同等方式规定数据接收方的责任和义务；	个人生物识别信息、辅助原则上不应共享、转让。确需共享转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和安全能力等，并征得个人信息主体的明示同意。
3.3-18	个人信息的公开披露	1）个人信息原则上不应公开披露，经法律授权或具备合理事由确需公开，且必须满足前述安全合规要求。 2）事先开展个人信息安全影响评估，并对处理情况进行记录； 3）向个人信息主体告知公开披露个人信息的目的、类型，并征得个人信息主体的明示同意；	不应公开披露个人生物识别信；不应公开披露公民的种族、民族、政治观点、宗教信仰等个人敏感信息的分析结果。

		4）承担因披露个人信息对个人信息主体合法权益造成损害的相应责任。 5）不应披露儿童个人信息	
3.3-19	导入导出安全	1）对个人信息的导出操作人员进行细粒度的访问控制与全过程审计； 2）定期检查或评估信息导出通道的安全性和可靠性	

3.3.6 个人信息删除安全

序号	合规要求	控制措施及规程说明	其他考虑
3.3-20	超过法定保存期限及时删除	不应只采用删除索引、删除文件系统的方式进行信息销毁；应通过多次覆写等方式安全地擦除个人信息； 若技术上无法实现删除时，应使其保持无法被访问和检索。	若技术能力上无法实现及时删除时，应当建立定期的删除机制；
3.3-21	存储介质销毁	存储个人信息的介质进行报废处理时,应采用物理损毁等方式，例如消磁、焚烧、粉碎等销毁介质,确保个人信息不能被恢复。	

4 个人信息专项保护

4.1 敏感个人信息保护

序号	合规要求	控制措施及规程说明	其他考虑
4.1-1	处理的必要性	只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。 个人数据处理需要明确敏感个人数据的处理目的，并且需采取身份认证、访问控制、存储加密、日志审计等严格安全防护措施对敏感个人数据进行保护。	
4.1-2	取得单独同意	在处理敏感个人数据前，个人信息控制者需要提供获取个人单独同意的机制。比如弹出单独的对话框给个人进行确认，或者在推送的隐私协议中中加粗等显著标识	法律、行政法规规定处理敏感个人信息应当取得书面同意的，个人信息处理者应提供书面同意的获取机制进行处理。
4.1-3	告知权益影响	个人信息控制者在处理敏感个人信息前，应当进行权益影响评估识别可能对个人信息主体权益造成对影响，并提供一个告知的机制（如单独弹出一个对话框或者页面，提供用户确认的按钮），以用户清晰易懂的语言准确告知个人处理其敏感个人信息的必要性和对其权益的影响，并且使用加粗等显著的标识。	
4.1-4	收集处理生物识别信息前的告知，	1）充分告知须包含以下内容： a）所采集的个人生物识别信息的类型、范围、数量； b）个人信息主体不想注册或无法注册时，还应告知可用替代程序的信息； c）有关于生物特征识别系统中所采集的个人生物识别信息处理方式的描述； d）有关于生物特征识别信息管理负责人的信息，包括姓名、	在提供多种可供选择的身份认证方式时，建议不将生物特征识别信息作为初始默认选项。

		组织机构、职位、联系方式等。 2）生物鉴别信息可遵循 GB/T36651—2018《信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架》的相关要求	
4.1-5	禁止存储原始个人生物识别信息（如样本、图像等）。	1）仅存储个人生物识别信息的摘要信息； 2）在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能； 3）在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。	
4.1-6	个人生物识别信息与个人身份信息分开存储。	不仅应将个人生物识别信息与个人身份识别信息在物理上分开存储，还可以将这两者的控制权限分配给不同的操作人员，以实现分隔效果。	采用数字水印等技术保障生物特征识别信息可溯源

4.2 未成年人个人信息保护

儿童个人数据：根据《中华人民共和国网络安全法》《中华人民共和国未成年人保护法》等法律法规，中国制定《儿童个人信息网络保护规定》，较于《个人信息保护法》中对个人数据保护的相关要求，儿童个人（不满十四周岁的未成年人）数据保护有着特别的要求。

序号	合规要求	控制措施及规程说明	其他考虑
4.2-1	单独同意	个人信息控制者在处理未满十四岁未成年人个人信息前，需要提供获取其父母或者其他监护人的同意（比如要求输入身份证号码进行关系验证）	

4.2-2	专门的儿童个人信息保护规则和用户协议。	个人信息处理者征得同意时，应当同时提供拒绝选项，并明确告知。明确告知需包含以下事项： 1）收集、存储、使用、转移、披露儿童个人信息的目的、方式和范围； 2）儿童个人信息存储的地点、期限和到期后的处理方式； 3） 儿童个人信息的安全保障措施； 4）拒绝的后果； 5）投诉、举报的渠道和方式； 6）更正、删除儿童个人信息的途径和方法。	
4.2-3	处理未成年人敏感个人信息	处理未成年人敏感个人信息的，应当具有特定的目的和充分的必要性，采取严格保护措施；在事前进行个人信息保护影响评估并对处理情况进行记录；个人信息保护影响评估报告和处理情况记录应当至少保存三年。	
4.2-4	未成年人访问控制	个人信息处理者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制未成年人个人信息知悉范围。工作人员访问未成年人个人信息的，应当经过相关负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法处理未成年人个人信息。	

4.3 组织自身的变化下的合规要求

序号	合规要求	控制措施及规程说明	其他考虑
4.3-1	合并时的个人信息处理	应在协议中明确增加个人信息转移，并由合并后的组织承接的条款； 应明确合并后的组织的安全保护义务并完成系统、网络的接入等措施； 1）因合并而转移个人信息的，应重新履行知情同意等义务，并在未取得同意时，删除或按照个人主体要求转移个人信息； 2）因合并后业务或数据聚合、关联，导致形成可识	新设合并，与吸收合并下，个人信息的处理主体可能不同，前者由于产生新的组织，因此应考虑重新取得知情同意； 1）因合并导致触发重要数据监管要求的，应按照重要数据保护的相关法律规定执行，例如“涉及重要数据和一百万人

		别个人信息的，应重新履行知情同意等义务； 3）合并一般意味着业务类型的增加，对于已经收集、获取的个人信息，如发生增加后的业务等情况的，应重新履行知情同意等义务， 4）应考虑更新或修订个人信息处理规则 5）对于因合并需要转移个人信息的，需要向个人告知接收方的名称或姓名和联系方式。	以上个人信息的，应当向设区的市级主管部门报告”
4.3-2	分立时的个人信息处理	应在协议、设立法律文件中明确增加个人信息因分立而转移，或形成多份（副本），并明确由分立后的哪一方或多方组织承接的条款； 由于分立后将产生一个以上的组织，应重新履行知情同意等义务，并在未取得同意时，删除或按照个人主体要求转移个人信息； 应考虑更新或修订个人信息处理规则； 应在设备设施等硬件资产权属处置中同时考虑个人信息等数据的转移； 分立通常意味着业务类型的重大变化，对于已经收集、获取的个人信息，如发生用途变化等情况的，应重新履行知情同意等义务； 对于因分立需要转移个人信息的，需要向个人告知接收方的名称或姓名和联系方式。	在原组织存续，同时分立出新组织的，如约定由新组织获取、接受个人信息，因考虑重新取得知情同意； 在分立后原组织不再存续的情形下，由于原有的处理个人信息的主体灭失，因此分立后的各个组织均应考虑重新取得知情同意
4.3-3	解散、注销时的个人信息处理	组织解散、注销时意味着个人信息处理主体不复存在，应提前履行向个人信息主体的告知义务； 应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告（主管部门要求的移交、删除，应取得个人信息主体的同意，法律另有规定的除外）； 如个人信息主体要求转移或删除个人信息的，组织应在解散、注销的过程终结之前，完成转移或删除（优	

		先于向主管部门移交或删除要求）；	
4.3-4	破产时的个人信息处理	在破产重整过程中，如有投资方等承接组织资产、股权或业务的，应重新履行知情同意等义务； 在破产清算过程中，应按照“解散、注销时的个人信息处理”的规定进行处理	组织破产时可能因是否存在拯救的必要与可能，从而使得包括数据在内的资产形成不同走向（重整或者清算），在重整（成功）的情形下，组织将继续存续，因此可按照既有的个人信息处理规则进行个人信息处理，但投资方等决定改变组织经营业务等情况的除外； 破产清算的情况，类似于组织注销解散。

4.4 共同处理者与委托处理者的管理

4.4.1 处理者身份的判定

依照《个保法》相关的要求，对于个人信息处理的目的和处理方式由两个以上的个人信息处理者决定的时候，该类人员被认为是共同处理者。受托处理者主要是接受个人信息处理者的委托、按照其提出的要求执行个人信息处理的工作。

序号	合规要求	控制措施及规程说明	其他考虑
4.4-1	共同处理者的保护要求	两个以上的信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务，但该约定不影响个人向其中任何一个个人信息处理者行使法定的权利，同时，由于共同处理者在处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。	由于共同处理涉及需要与其他处理者的协调与约定，容易存在责任不清、易产生连带责任的问题，因此通常不建议采用共同处理者的方式。
4.4-2	委托处理者的合规要求	供应商作为受托人，应该依照与个人信息处理者（组织）就委托处理的目的、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约定（委托合同、协议等）进行个人信息的处理，同时接受个人信息处理者（组织）对其处理活动的监督。受托人在处理个人信息时，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、被撤销或者终止时，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	

4.4.2 委托处理者管理过程

对于委托处理者管理中的个人信息处理的要求应融入到供应商管理的全过程之中。以下主要罗列了从供应商认证、供应商对个人信息的处理（个人信息的引入和引入后管理）、供应商审计、供应商退出等全过程中，个人信息应如何处理的注意事项。

序号	合规要求	控制措施及规程说明	其他考虑
4.4-3	供应商认证阶段	应确保供应商具有数据收集与处理能力，其采购和使用的数据具有合法性，并建立了相应的数据和隐私保护框架和策略。主要包括如下几个维度： 1）是否建立了隐私保护框架以确保其数据收集、处理及保护的能力； 2） 是否采取了适当的技术及组织措施保障数据的安全；是否建立了数据泄露事件响应机制；	需要对第三方供应商进行尽职调查，同时应确保供应商建立了相应的数据和隐私保护策略，保证数据源头的合规。
4.4-4	供应商对个人信息进行处置（个人信息引入时和引入后管理）	1）需要确保组织所提出的数据需求不得违反强制性的法律法规，且符合数据主体的预期； 2）委托处理者应明确所采集的数据及其采集过程不得违反强制性的法律法规要求； 3） 需要确认所获取的数据得到了数据主体的明示同意； 4）需要明确所使用数据的目的和方式符合数据主体的预期或理解；	1)需要明确组织与供应商之间的数据使用协议，依照数据使用的协议及要求，明确组织及相关供应商之间的数据角色。 2)需要明确对于不具备完全民事行为能力的数据主体的数据处理是否已经得

		5）在数据主体预期范围外的数据引入或使用，需要确认供应商或组织已经得到了相关数据主体的同意 6）需要确认数据供应商应具备相应的合法性以收集数据主体的数据并提供给组织； 7）供应商在进行数据提供或处理时，应已经获得了授权，且该授权明确同意向第三方披露或转让数据信息，或已经依照相关要求向数据主体履行了告知义务及处理情况； 8）需要检查供应商所获得的数据主体的签字授权材料或其他合规证明材料。	到了监护人的同意。
4.4-5	数据引入后管理	1）引入的数据应在授权或协议范围内使用，且不得以任何方式再次销售或共享给第三方； 2）共享场景下需要与被共享方签署数据保护协议，并约定其数据及隐私保护的义务； 3） 引入后的个人数据存在与其他供应商共享使用或外包业务流程供其使用时，应采取必要的技术措施做好权限管理，从而确保数据的有限访问； 4）对个人数据的留存期限需要做明确的约定，对未做约定的数据需要定期审视；	1)采取充分的技术和组织措施保障个人数据安全性，包括但不限于个人数据匿名化、假名化、加密、有限访问等措施 2)与供应商在签订协议时需明确供应商对数据的访问控制措施
4.4-6	供应商审计阶段	供应商应保留所需的各种证明材料以便在审计阶段提供，包括供应商在处置数据或依照协议进行数据处置过程中的证明材料等；	在审计时，应重点关注证明材料的完备性以及是否覆盖了所涉及场景；
4.4-7	供应商退出阶段	1） 供应商在退出时，应对从组织获取的个人数据依照相应的协议进行清理； 2）组织从供应商处获取的个人数据，应依照组织的隐私保护框架进行处置，以确保符合相应的强制性法律法规要求； 3）对于因供应商违反数据保护条款或者相关法律	1)退出时应对数据的获取及销毁等过程进行重新审视，确保数据的处置合法依规； 2)对于具有较大量的个人数据处置者（供应商），

		法规要求可能给组织带来的任何损失、损害、成本、索赔和费用，供应商应给予赔偿、进行辩护和或解决，使组织免受损害；该类条款的使用或约定应在可预见或合理的时限条款中进行约定。	应依照组织内的相关规定对其进行必要的审计，以确保数据已经依照协议或合同进行了处理；

4.5 自动化决策场景下的安全保护

序号	合规要求	控制措施及规程说明	其他考虑
4.5-1	保证透明度和结果公平、公正	在隐私政策中明确告知使用自动化决策或者进行用户画像分析的业务场景，对所使用的个人信息类型、目的和方式、算法推荐服务的基本原理、目的意图、运行机制等基本要素进行明示； 确保消费者画像公正、客观、真实，提供不针对个人特征的选项；	利用数据和算法推送新闻、广告时，用显著的方式标明“定推”； 在对个人权益有重大影响的决定的场景下，对自动化决策的结果引入人工审核。
4.5-2	向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。	在信息推送和商业场景下，向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭推荐服务的选项。个人用户选择关闭推荐服务时应当立即停止提供相关服务。	个人信息处理者针对场景特点提供不针对其个人特征的选项，个性化推荐的内容和不针对个人特征的内容可以通过不同的栏目、板块、页面来展示，也可以在个性化推荐的内容上添加“定推”等说明性标识来区分。
4.5-3	响应要求解释的权利及拒绝的权利	当通过自动化决策产生对他人有重大影响的决定时，应提供对个人信息处理规则的解释说明，支持对自动化决策涉及的标签、画像信息的解释说明，当个人信息主体拒绝自动化决策做出的决定时应当予以响应。	综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的透明度和可解释性，避免对用户产生不良影响，预防和减少争议纠

			纷。
4.5-4	算法管理	加强用户模型和用户标签管理，完善记入用户模型的兴趣点规则和用户标签管理规则，不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息。	算法推荐服务提供者是算法安全的主体责任部门，应建立数据安全和个人信息保护、安全评估监测、安全事件应急处置等管理制度和技术措施，加强信息安全管理，加强用户模型和用户标签管理等，算法推荐服务提供者应采取有效的数据安全管理制度（如数据安全管理制度、数据安全应急响应制度、人员与技术管理制度、数据安全风险评估与监测制度等）和技术措施（如数据标签技术、数据脱敏技术、隐私数据保护技术等）
4.5-5	人工复核机制	向个人信息主体供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。	

4.6 个人信息跨境

4.6.1 个人信息出境合法情形

序号	合规要求	控制措施及规程说明	其他考虑
4.6-1	具备的合法性条件	个人信息处理者必须要清楚地一个前提是因业务等需要，确需境外提供个人信息的，需满足下列条件之一： 1）依照《个人信息保护法》第四十条的规定通	人类遗传资源信息出境，需经国务院科学技术行政部门批

		过国家网信部门组织的安全评估； 2）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； 3）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； 4）法律、行政法规或者国家网信部门规定的其他条件。	准（科学技术部备案、批准）。
4.6-2	处理外国司法或者执法机构请求	按中国缔结或参加的国际公约、协定等向境外提供个人信息时建议需考虑以下两个方面的要求： 1）按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求； 2）非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。	

4.6-3	个人信息主体知情同意	个人信息处理者在向境外提供个人信息前，应当告知与获得个人单独同意的，操作如下： 1）个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项： a） 境外接收方的名称或者姓名和联系方式； b） 个人信息的处理目的、处理方式，处理的个人信息种类、保存期限； c） 个人行使《个人信息保护法》规定权利的方式和程序； d） 法律、行政法规规定应当告知的其他事项。 2）基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。	

4.6.2 个人信息出境安全评估触发条件

序号	合规要求	控制措施及规程说明	其他考虑
4.6-4	关键信息基础设施运营者和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。	个人信息出境触发国家网信部门组织的安全评估的场景主要分为以下四类： 1）出境数据中包含重要数据。需要注意的是，本分类虽然讲述的是重要数据，但在具体实践过程中，部分行业已将一定数量的个人信息纳入重要数据范畴或等同于按照重要数据的保护要求进行管理；	涉及关键信息基础设施运营者的请参考《关键信息基础设施安全保护条例》所列明的八大行业。

		2）关键信息基础设施运营者； 3）处理个人信息达到一百万人的个人信息处理者； 4）累计向境外提供超过十万人个人信息或者一万人以上敏感个人信息的个人信息处理者； 5）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。	

4.6.3 向境外提供个人信息应当履行的义务

序号	合规要求	控制措施及规程说明	其他考虑
4.6-5	与影响评估报告的一致性	个人信息处理者在履行义务或向监管部门、个人信息主体展示评估报告时，需要提供充分的证据材料，证明其向境外提供数据与个人信息保护影响评估报告中的目的、范围、方式和数据类型、规模等内容是一致的。	
4.6-6	与安全评估时的一致性	个人信息处理者需要知道的是： 1）个人信息保护影响评估报告作为申请材料之一提交给网信部门进行安全评估，需要在报告中明确目的、范围、方式和数据类型、规模等信息； 2）申报书作为申请材料之一提交给网信部门进行安全评估，也需要明确出境目的、范围、方式和数据类型、规模等信息。 3）日常实践操作中是需要与影响评估报告、申报书所述内容保持一致的，并留存向境外提供数据时的证据材料（包括但不限于相关日志记录和数据出境审批记录、测试验证记录）三年以上。	《数据出境风险自评估报告》可理解为《个人信息保护影响评估》的一种。
4.6-7	采监督数据接收方按照双方约定	1）个人信息处理者需要与数据接收方签订服务合同、保密协议、安全承诺书等，管理部门和法务部门、审	

	履行数据安全保护义务	计部门等共同参与审查与数据接收方合作过程，监督数据接收方履行个人信息保护责任与义务，合同内容参照《数据出境安全评估办法》第九条 2）管理部门可以从事前、事中、事后对数据接收方的背景、个人信息保护安全管理和技术手段、操作行为等进行审查和监督。 法务部门（隐私官或法律顾问）可以审查合同、保密协议、安全承诺书等材料的合法合规性。 4） 审计部门可以审查数据接收方是否按照双方约定的目的、范围、方式使用数据，到期后是否履行数据删除义务等。	
4.6-8	需要承担的责任	数据出境对个人、组织合法权益或者公共利益造成损害的，数据处理者应当依法承担责任。 1）首先，个人信息处理者需要履行自身义务，包括制定内部管理制度和操作规程，对个人信息实行分类分级管理，组织开展安全教育培训，采取相应的加密、去标识化等安全技术措施，制定并组织实施个人信息安全事件应急预案等。 2）其次，针对个人信息出境场景组织开展个人信息保护影响评估工作，并按照相关要求提交年度报告给网信部门以及将报告（或个人信息保护社会责任报告）简化后向公众发布。 3）最后，其他履行义务的证明材料 参考以往司法判例过程中，如“数据出境对个人、组织合法权益或者公共利益造成损害的，个人信息处理者需依法承担责任”，这个责任不是无限大，不是要求数据发送方代接收方受过，但可通过以上自证方式证明尽到了对涉案信息的安全保护义务，以减轻需承担的责任。	

4.6-9	相关日记录的保存	存留相关日志记录和数据出境审批记录三年以上： 1）相关日志记录包括但不限于：系统日志、网络设备日志、接口日志、程序账号日志、操作行为日志； 2）个人信息出境审批记录包括但不限于：用户单独同意记录、与数据接收方的合同记录、与相关方的保密协议、承诺书等记录、内部审批记录、向网信部门申报记录以及相关申报材料。	
4.6-10	配合监管部门的检查	国家网信部门会同国务院有关部门核验向境外提供个人信息和重要数据的类型、范围时，数据处理者应当以明文、可读方式予以展示。 个人信息处理者配合监管部门提供如下材料，包括不限于： 1）以明文、可读的方式展示相关日志记录、个人信息出境审批记录等材料。 2）提供网络环境等实施技术测试的方式，展示向境外提供个人信息的类型、范围。	
4.6-11	数据出境范围动态调整	国家网信部门认定不得出境的，数据处理者应当停止数据出境，并采取有效措施对已出境数据的安全予以补救。 按照个人信息的类别级别可能因时间变化、政策变化、安全事件发生、不同业务场景的敏感性变化或相关行业规则不同而发生改变的特性，个人信息处理者应针对个人信息出境场景建立动态调整的策略，可从如下三方面考虑： 1）事前：向网信部门申报出境时，对需要出境数据的类型、级别以及是否会因上述原因发生变化进行详细说明。 2）事中：时刻监测出境个人信息的变化情况，按照相关要求及时向网信部门反馈。	

		3）事后：当存在不得出境的个人信息时，及时停止出境，按照应急预案（需设置此类应急场景）的方式及时处置，并要求数据接收方按照合同（需有写明此种例外情况）删除已接收的相关个人信息。	
4.6-12	个人信息出境再转移的特别约定	个人信息出境后确需再转移的，应当事先与个人约定再转移的条件，并明确数据接收方履行的安全保护义务。 1）个人信息处理者、数据接收方应当在合同中明确个人信息再转移事项，并在出境前征得个人单独同意时，一并将再转移条件征得个人同意。 2）与此同时，在编写年度数据出境安全报告时也需要写明个人信息出境后再转移的情况。	《数据出境安全评估办法》第九条（三）限制境外接收方将出境数据再转移给其他组织、个人的约束条款。
4.6-13	非经中华人民共和国主管机关批准，境内的个人、组织不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。	1） 对于境外的强制调取，个人信息处理者需要同时履行个人信息出境安全义务（无论是安全评估、合同等）和主管机关批准程序的要求。 2）对于主动、自愿、不受任何压力的外国司法或者执法机构提供个人信息的，个人信息处理者也应当遵守个人信息出境安全方面的要求，包括主动过滤、删减掉明文禁止出境的个人信息，对于未明文禁止出境的个人信息，进行出境安全评估。	

4.6.5 定期向监管机构定期汇报的要求

个人信息处理者需要明白，无论是认为不必进行出境评估的还是已获得网信部门申请出境评估的，只要涉及满足申报要求的个人信息出境都需要建立向网信部门的汇报机制，并在每年 1 月 31 日前编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况。

序号	合规要求	控制措施及规程说明	其他考虑
4.6-14	全部数据接收方名称、联系方式	与 4.6-3 中提到的“向个人告知境外接收方的名称或者姓名和联系方式”以及其他几种表现形态的报告所描述内容均要一致。	

4.6-15	出境数据的类型、数量及目的	与 4.6-3 中提到的“向个人告知出境数据的类型、数量及目的”以及其他几种表现形态的报告所描述内容均要一致。	建议在此处需进一步对上一年度的数据出境活动的数据类型、数据、目的、频次、敏感程度等内容进行详细说明。
4.6-16	数据在境外的存放地点、存储期限、使用范围和方式	1）个人信息处理者需要清楚知道的是：只要在中国处理的个人信息随后在另一个国家/地区处理，就会发生个人信息的跨境“提供”。而通常理解的情形是个人信息处理者将数据转移至中国境外的地方。例如，基于某项业务需求，个人信息处理者主动将在中国境内处理的个人信息随后提供给境外某一个国家/地区。但还有一种情形是个人信息并未转移至境外，而依旧存储在境内，不过个人信息处理者将境内数据库的访问登录信息或接口提供给境外主体，以便后者可以在境外远程访问查看。例如，当个人信息处理者允许在 A 国设立的接收方远程访问存储在中国的个人信息，鉴于远程访问情形也会对境内存储的个人信息构成一定风险威胁，从数据跨境流动安全管理的角度来看，其理论上也属于“数据出境”。 2）本条内容中涉及的存放地点既可以是境内也可能是境外（一个或多个）；同时个人信息处理者也需要对存储期限、使用范围和方式进行详细描述，其中对于存储期限需要根据法律法规、行业要求以及合同内容进行梳理，如反洗钱法。	
4.6-17	涉及向境外提供数据的用户投诉及处理情况	本条内容需统计上一年度涉及个人信息出境相关投诉，可结合日常投诉及处理流程相关内容进行描述。	

4.6-18	发生的数据安全事件及其处置情况	本条内容的编写可参照个人信息安全事件调查评估报告的内容，并将后期具体的处置情况（涵盖监管部门的处置意见、个人信息主体相关意见等）等内容加以描述。	
4.6-19	数据出境后再转移的情况	本条内容需针对合同中约定的再转移场景进行调查说明，调查内容包括但不限于是否与约定的一致、是否执行相应的保护措施、是否前一个转移方的个人信息进行删除。	
4.6-20	国家网信部门明确向境外提供数据需要报告的其他事项	本条内容遵循当年国家网信部门的监管要求，提供其他需要报告的内容和材料。	

4.6.6 从事跨境个人信息数据活动的被安全监管与建立技术与管理措施的义务

序号	合规要求	控制措施及规程说明	其他考虑
4.6-21	**建立健全相关技术和管理措施，**此控制措施其实也包括了跨境个人信息传输方面的技术要求	如何建立健全相关技术和管理措施，就目前行业实践看，更多的是围绕个人信息采集、传输、存储、使用、共享、销毁等生命周期各环节实施安全保护，包括数据加解密、数据脱敏、备份与恢复、安全审计、数据水印、数据销毁、完整性验证等个人信息保护技术研发及应用，而在落实相关技术和管理措施时，需注意以下几方面： 1）遵循在中国境内收集和产生的个人信息存储在境内的法律要求，个人信息处理者涉及的相关服务器和存储设备必须存放在中国境内，例如苹果中国数据中心部署在贵州。 2）不得滥用个人信息保护技术对个人信息主体进行监控，非法采集公民个人信息，破坏个人信息的完整性、可用性、保密性。	

		3） 涉及使用或者提供的网络产品和服务时，需设立流程、程序和系统评估个人信息保护缺陷、漏洞等风险情况。 4）持续改进技术手段，提升技术互操作性，令数据提供方和数据接收方在不同系统之间能够共享和使用个人信息。例如，尝试区块链技术特有的不可篡改特性，提升个人信息保护、增强数据供应链透明度。	

4.6.7 个人信息出境安全评估实施流程

序号	合规要求	控制措施及规程说明	其他考虑
4.6-22	自评估	个人信息处理者在提交个人信息出境申请前，应先开展自评估，并形成《数据出境风险自评估报告》，主要包括以下事项： 1）数据出境的目的、范围、方式等的合法性、正当性、必要性； 2）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求； 3）出境数据的规模、范围、种类、敏感程度，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； 4）数据安全和个人信息权益是否能够得到充分有效保障； 5）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务； 6）遵守中国法律、行政法规、部门规章情况；	《数据出境风险自评估报告》的模板请参见数据出境安全评估申报指南（第一版）

		7）国家网信部门认为需要评估的其他事项。	
4.6-23	准备申报材料	申报数据出境安全评估，应当提交以下材料： 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	数据出境安全评估申报指南（第一版）
4.6-24	提交申报材料：申报渠道	个人信息处理者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。	数据出境安全评估申报指南（第一版）
4.6-25	申请材料评估：评估期间主要时间节点	在本阶段，个人信息处理者需要注意三个通知时间节点： **（一）省级网信办通知时间节点：**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。 **（二）国家网信办通知时间节点：**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。 **（三）个人信息处理者更正时间节点：**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。	
4.6-26	申报通过后：持续监督	个人信息出境评估结果有效期为二年，有效期内若评估内容发生变化或超过有效期，个人信息处理者则应立即停止相关个人信息出境活动直至新的个人信息据出境评估结果通过。	

5 合规监测改进

5.1 个人信息安全影响评估

5.1.1 个人信息安全影响评估的适用情形

序号	合规要求	控制措施及规程说明	其他考虑
5.1-1	适用情形	满足以下情形需开展个人信息安全影响评估： 1）处理敏感个人信息； 2）利用个人信息进行自动化决策； 3）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息； 4）向境外提供个人信息； 5）其他对个人权益有重大影响的个人信息处理活动。	在以下情形时建议开展个人信息安全影响评估： 1）在产品或服务发布前，或业务功能发生重大变化时； 2）在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时； 3）基于不同业务目的所收集个人信息产生汇聚融合时。

5.1.2 个人信息安全影响评估实施流程

序号	合规要求	控制措施及规程说明	其他考虑
5.2-1	组建评估团队	1）在评估计划启动前应首先任命评估负责人和确认评估报告签署人，组建合适的评估团队；	应确认评估团队人员构成的合理性；
5.2-2	确定评估对象和范围	1）应确认处理个人信息的系统、网络、业务服务范围； 2）涉及委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息的，还应确认以上个人信息的范围、处理目的和涉及的主体范围；	
5.2-3	制定评估计划	1）应制定评估计划表，清楚规定完成个人信息安全	评估计划的制定应考虑以

		影响评估报告须进行的工作、相关工作具体由评估团队中的哪些成员负责、时间安排等信息	下因素： 1）人员、技能、经验及能力的综合调配； 2）执行各项任务所需时间； 3)进行评估每一步骤所需资源，如自动化的评估工具等。
5.2-4	制定可能的咨询计划	必要时，应向处理个人信息的相关方进行咨询，包括但不限于：供应商、合作伙伴等。 咨询范围可包括个人信息处理过程的安全技术措施、安全管理措施、对相关措施的评价等。	应根据个人信息处理的影响范围、程度等确定相关方范围，必要时可组织用户访谈或咨询内外部的专门组织的意见。
5.2-5	个人信息梳理准备	根据评估对象和范围详细梳理相关个人信息处理过程，形成清晰的数据清单及数据映射图表，梳理过程应包括： 1）根据产品、业务、某项具体合作确认数据项；2）根据数据生命周期确认数据流转过程、数据处理目的、方式、安全技术措施、安全管理措施等； 3）根据数据处理涉及的网络、系统、工具、操作流程确认相关安全技术措施、安全管理措施等； 4）确认相关方的安全保护措施等。	数据映射图表涵盖的维度应包括：个人信息的类型、敏感程度、收集场景、处理方式、涉及相关方等要素，便于后续分类后进行影响分析和风险评价。
5.2-6	风险识别	对梳理到的个人信息项按照以下维度进行风险识别，确认数据处理个人信息处理的目的、处理方式等是否合法正当必要： 1）数据处理生命周期； 2）所处系统、网络环境，使用的工具等； 3）处理个人信息的人员和操作审批流程等； 4）业务内外部风险趋势。	

5.2-7	个人权益影响分析	应结合相关法律法规与政策标准的要求或组织自定义的个人信息安全目标，分析个人信息处理行为对个人权益可能产生的影响，以及个人信息泄露、毁损、丢失、滥用等对个人权益可能产生的影响，审视是否存在侵害个人信息主体权益的风险。	个人权益影响概括可分为“影响个人自主决定权”“引发差别性待遇”“个人名誉受损或遭受精神压力”“个人财产受损”四个维度。
5.2-8	安全风险分析	应结合个人信息处理活动特点、已实施的安全措施、相关方、处理规模等要素，同时考虑具备的事件处置经验、用户习惯、预防性措施、相应整改措施等，评价安全风险程度。	
5.2-9	保护措施合法、有效、适应性分析	综合个人权益影响分析和安全风险分析评估所采取的相应保护措施，与经整改后的风险和影响程度相适应，不应超过法律法规和标准规定的阈值。	
5.2-10	形成评估报告	评估报告内容应包括：个人信息保护评估人员的审批页面、评估报告适用范围、实施评估及撰写报告的人员信息、参考的法律、法规和标准、个人信息影响评估对象（应明确涉及的个人敏感信息）、评估内容、涉及的相关方等，以及个人权益影响分析结果，安全保护措施分析结果、安全事件发生的可能性分析结果、风险判定的准则、合规性分析结果、风险分析过程及结果，风险处置建议等。	
5.2-11	相关报告和处理情况保存	个人信息保护影响评估报告和处理情况记录应当至少保存三年。	

5.2 个人信息安全合规审计

序号	合规要求	控制措施及规程说明	其他考虑
5.2-1	适用情形	个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。	审计周期最长为一年，可根据内外部的合规环境动

			态调整周期
5.2-2	维护合规清单	1）维护合规清单主要包括以下内容： 2）梳理业务模式，识别合规需求； 3）根据合规需求建立合规清单； 4）追踪外部的法律需求和外部相关的合规事件情况更新和维护事件清单；	
5.2-3	合规基线的设置	结合各类业务的清单，进行合规基线的裁剪和说明，告知具体的业务相关方	
5.2-4	合规审计报告	合规审计报告应当满足以下条件： 1）至少由法务部门、安全部门协同开展，业务部门积极配合； 2）包含对不合规事项对处置建议（例如相关业务关停等），并将审计结果上报至管理层；	由于合规的重要性，建议将合规结果与绩效关联

附录 1 条款与法律法规映射

序号	本文章节号	依据法律法规及条款号	依据文件类别	合规遵循程度
1	2-1	《个人信息保护法》第五十一条（二）	国家法律	严格遵循
2	2-2	《个人信息保护法》第四条	国家法律	严格遵循
3	2-3	《个人信息保护法》第二十八条	国家法律	严格遵循
4	2-4	《个人信息保护法》第四条	国家法律	严格遵循
5	3.1-1	/	最佳实践	建议遵循
6	3.1-2	/	最佳实践	建议遵循
7	3.1-3	/	最佳实践	建议遵循
8	3.1-4	《个人信息保护法》第五十二条	国家法律	严格遵循
9	3.1-5	《个人信息保护法》第五十八条	国家法律	严格遵循
10	3.1-6	《个人信息保护法》第五十三条	国家法律	严格遵循
11	3.1-7	《儿童个人信息保护规定》第八条	行政法规	严格遵循
12	3.2-1	GB/T 35273-2020 《信息安全技术 个人信息安全规范》8.8	推荐性国家标准	严格遵循
13	3.2-2	《个人信息保护法》第四十四条	国家法律	严格遵循
14	3.2-3	《个人信息保护法》第四十五条	国家法律	严格遵循
15	3.2-4	《个人信息保护法》第四十六条	国家法律	严格遵循
16	3.2-5	《个人信息保护法》第四十七条	国家法律	严格遵循
17	3.2-6	《个人信息保护法》第四十八条	国家法律	严格遵循
18	3.2-7	《个人信息保护法》第四十九条	国家法律	严格遵循
19	3.3-1	《个人信息保护法》第五条	国家法律	严格遵循
20	3.3-2	《个人信息保护法》第六条	国家法律	严格遵循
21	3.3-3	《个人信息保护法》第八条	国家法律	严格遵循
22	3.3-4	《个人信息保护法》第二十六条	国家法律	严格遵循
23	3.3-5	《个人信息保护法》第五十一条	国家法律	严格遵循

24	3.3-6	《个人信息保护法》第五十一条	国家法律	严格遵循
25	3.3-7	《个人信息保护法》第五十一条	国家法律	严格遵循
26	3.3-8	《个人信息保护法》第十九条、第四十七条	国家法律	严格遵循
27	3.3-9	《个人信息保护法》第十九条、第四十七条	国家法律	严格遵循
28	3.3-10	《个人信息保护法》第十九条、第四十七条	国家法律	严格遵循
29	3.3-11	《互联网个人信息安全保护指南》5.2.3.2	国家标准	建议遵循
30	3.3-12	《个人信息保护法》第五十一条 GB/T 41479-2022 《信息安全技术 网络数据处理安全要求》7.2 GB/T 37964-2019《信息安全技术个人信息去标识化指南》附录 A	国家标准	建议遵循
31	3.3-13	GB/T 35273-2020 《信息安全技术 个人信息安全规范》7.4	国家标准	建议遵循
32	3.3-14	GB/T 37988-2019 《信息安全技术 数据安全能力成熟度模型》9.2	国家标准	建议遵循
33	3.3-15	《网络数据安全管理条例》（征求意见稿）第二十五条	行政法规	建议遵循
34	3.3-16	《个人信息保护法》第十条	国家法律	严格遵循
35	3.3-17	《个人信息保护法》第二十三条	国家法律	严格遵循
36	3.3-18	GB/T 35273-2020 《信息安全技术 个人信息安全规范》9.4 《儿童个人信息网络保护规定》第十八条	国家标准	建议遵循
37	3.3-19	GB/T 37988-2019 《信息安全技术 数据安全能力成熟度模型》10	国家标准	建议遵循
38	3.3-20	《互联网个人信息安全保护指南》	国家标准	建议遵循
39	3.3-21	GB/T 41479-2022 《信息安全技术 网络数据处理安全要求》5.13	国家标准	建议遵循

40	4.1-1	《个人信息保护法》第二十八条	国家法律	严格遵循
41	4.1-2	《个人信息保护法》第二十九条	国家法律	严格遵循
42	4.1-3	《个人信息保护法》第三十条	国家法律	严格遵循
43	4.1-4	GB/T 35273-2020 《信息安全技术 个人信息安全规范》5.4 GB/T36651—2018《信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架》	国家标准	建议遵循
44	4.1-5	GB/T 35273-2020 《信息安全技术 个人信息安全规范》6.3	推荐性国家标准	建议遵循
45	4.1-6	GB/T 35273-2020 《信息安全技术 个人信息安全规范》6.3	推荐性国家标准	建议遵循
46	4.2-1	《个人信息保护法》第三十一条	国家法律	严格遵循
47	4.2-2	《儿童个人信息网络保护规定》第八条、第九条、第十条	行政法规	严格遵循
48	4.2-3	未成年人网络保护条例（征求意见稿）第三十七条	行政法规	严格遵循
49	4.2-4	未成年人网络保护条例（征求意见稿）第四十二条	行政法规	严格遵循
50	4.3-1	/	最佳实践	建议遵循
51	4.3-2	/	最佳实践	建议遵循
52	4.3-3	/	最佳实践	建议遵循
53	4.3-4	/	最佳实践	建议遵循
54	4.4-1	《个人信息保护法》第二十一条	国家法律	严格遵循
55	4.4-2	《个人信息保护法》第二十一条	国家法律	严格遵循
56	4.4-3	/	最佳实践	建议遵循
57	4.4-4	/	最佳实践	建议遵循
58	4.4-5	/	最佳实践	建议遵循

59	4.4-6	/	最佳实践	建议遵循
60	4.4-7	/	最佳实践	建议遵循
61	4.5-1	《个人信息保护法》第二十四条	国家法律	严格遵循
62	4.5-2	《个人信息保护法》第二十四条	国家法律	严格遵循
63	4.5-3	《个人信息保护法》第二十四条	国家法律	严格遵循
64	4.5-4	《互联网信息服务法推荐管理规定》第十条	行政法规	严格遵循
65	4.5-5	GB/T 35273-2020 《信息安全技术 个人信息安全规范》7.7	推荐性国家标准	建议遵循
66	4.6-1	《个人信息保护法》第三十八条	国家法律	严格遵循
67	4.6-2	《个人信息保护法》第四十一条	国家法律	严格遵循
68	4.6-3	《个人信息保护法》第三十九条	国家法律	严格遵循
69	4.6-4	《数据出境安全评估办法》第四条 《个人信息和重要数据出境安全评估办法 》（征求意见稿）第八条	行政法规	严格遵循
70	4.6-5	《数据出境安全评估办法》第三条 网络数据安全管理条例》（征求意见稿）第三十九条	行政法规	严格遵循
71	4.6-6	《数据出境安全评估办法》第三条 网络数据安全管理条例》（征求意见稿）第三十九条	行政法规	严格遵循
72	4.6-7	《数据出境安全评估办法》第三条、第九条	行政法规	严格遵循
73	4.6-8	/	最佳实践	建议遵循
74	4.6-9	《网络数据安全管理条例》（征求意见稿）第三十九条	行政法规	严格遵循
75	4.6-10	《网络数据安全管理条例》（征求意见稿）第三十九条	行政法规	严格遵循
76	4.6-11	《网络数据安全管理条例》（征求意见稿）第三十九条	行政法规	严格遵循

77	4.6-12	《网络数据安全管理条例》（征求意见稿）第三十九条	行政法规	严格遵循
78	4.6-13	《网络数据安全管理条例》（征求意见稿）第三十九条	行政法规	严格遵循
79	4.6-14	《网络数据安全管理条例》（征求意见稿）第四十条	行政法规	严格遵循
80	4.6-15	《网络数据安全管理条例》（征求意见稿）第四十条	行政法规	严格遵循
81	4.6-16	《网络数据安全管理条例》（征求意见稿）第四十条	行政法规	严格遵循
82	4.6-17	《网络数据安全管理条例》（征求意见稿）第四十条	行政法规	严格遵循
83	4.6-18	《网络数据安全管理条例》（征求意见稿）第四十条	行政法规	严格遵循
84	4.6-19	《网络数据安全管理条例》（征求意见稿）第四十条	行政法规	严格遵循
85	4.6-20	《网络数据安全管理条例》（征求意见稿）第四十条	行政法规	严格遵循
86	4.6-21	《个人信息保护法》第三十八条	国家法律	严格遵循
87	4.6-22	《数据出境安全评估办法》第六条 《数据出境安全评估申报指南》（第一版）	行政法规	严格遵循
88	4.6-23	《数据出境安全评估办法》第六条 《数据出境安全评估申报指南》（第一版）	行政法规	严格遵循
89	4.6-24	《数据出境安全评估办法》第四条	行政法规	严格遵循
90	4.6-25	《数据出境安全评估申报指南》（第一版）	行政法规	严格遵循

91	4.6-26	《数据出境安全评估办法》第十二条	行政法规	严格遵循
92	5.1-1	《个人信息保护法》第五十五条	法律法规	严格遵循
93	5.2-1	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
94	5.2-2	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
95	5.2-3	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
94	5.2-4	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
97	5.2-5	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
98	5.2-6	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
99	5.2-7	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
100	5.2-8	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
101	5.2-9	GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》	推荐性国家标准	建议遵循
102	5.2-10	《个人信息保护法》第五十六条	法律法规	严格遵循
103	5.2-11	《个人信息保护法》第五十六条	法律法规	严格遵循
104	5.2-1	《个人信息保护法》第五十四条	法律法规	严格遵循
105	5.2-2	/	最佳实践	建议遵循
106	5.2-2	/	最佳实践	建议遵循

附录2供应商服务类别及主要涉及服务对象

对于供应商的数据合规的管理，首先是要识别是哪些类别的供应商会涉及个人数据合规的要求或问题，其次是对供应商如何管理或处理个人数据的工作进行识别。通常而言，主要有如下供应商类别会涉及个人数据的处理。

序号	供应商服务类别	主要涉及的服务事项
1	云服务商	指的是基于云计算的技术架构支撑下对外提供按需分配、可计量的 IT 服务的供应商：云服务商管理、运营、支撑云计算的基础设施及软件，通过网络交付云计算的资源
2	技术服务商	指为企业提供信息系统、软硬件等开发、测试、集成、测评。运维以及日常安全管理的机构
3	数据受托处理者	指接受企业委托，按照企业要求的目的和方式开展企业数据处理活动的机构
4	数据提供方	指为企业运营提供各类数据资源的个人或机构，此处的“提供”包含“共享”和“转让”两种情形
5	数据接收方	指从企业接收各类数据资源的个人或机构
6	第三方 SDK 运营者	SDK 是指协助软件开发的相关一进制文件、文档、范例和工具的集合，而第三方 SDK 运营者是指非 APP 运营方或其关联机构的外部第三方 SDK 运营机构
7	数据交易服务机构	指在数据交易活动中提供数据资产、数据合规性、数据质量等第三方评估以及交易撮合、交易代理、专业咨询、数据经纪、数据交付等专业服务的机构
8	金融保险服务	为组织人员（包括但不限于员工/客户/用户/实习生等）提供金融保险服务业务（包括但不限于商业保险/意外险/综合险/特定人群或目标的融资贷款等服务）
9	人力资源招聘服务	为组织提供招聘及其周边服务（包括但不限于猎头、招聘合作、职位发布及信息收集网站、PDP 等性格测评工具）
10	人力资源外包服务	为组织提供人员的长期外包（包括但不限于工厂辅工、高峰期临时需求、工程建设项目等）
11	人员租赁服务	为组织提供人员的短期租赁（包括但不限于专项活动、特定时期或周期性的短期人员需求等）
12	公共关系（PR）服务	为组织提供与公共关系相关的服务（包括但不限于自有媒体、传统媒体以及自媒体等各种媒体、传媒平台的合作）

13	业务/流程服务委外	为组织提供与其业务及业务管理流程相关的服务（包括但不限于快递物流、内外部培训、流程管理、项目管理等）
14	市场营销&促销	为组织提供市场营销、零售促销等活动相关的服务（包括但不限于长期的促销人员、短期如节假日或特定地点促销活动等的销售端的人力服务）
15	软件开发外包	为组织提供软件开发相关的服务（包括但不限于管理类或涉及大量个人信息的公共服务类软件等开发外包）
16	定制类数据服务	为组织提供各种定制的数据相关服务（包括但不限于各类舆情或特定/不定主题的数据相关服务，如自采数据、数据采集或分析、数据采购等）

附录 3 供应商提供/处理数据时对应的合规评审要求

对于供应商提供或处理的隐私数据中，应重点关注以下几类数据及其相应的合规评审要求：

序号	数据类别	数据信息描述	合规要点
1	通信类	邮件、短信、聊天记录、通话记录等	依照法规要求不得采购或提供此类数据
2	图片类	身份证、银行卡、护照等个人证据	依照法规要求不得采购或提供此类数据
3	图片类	机票/火车票等	鉴于难以保证信息合法性，不建议采购或提供此类数据；
4	图片/视频类	公共道路交通相关	公共监控类视频不得采购或提供 供应商自行采集的，应要求对人脸和车牌等可识别个人的信息匿名化处理，环境模糊化 供应商获取的第三方图片/视频，应获得允许本组织使用的授权 组织不得对供应商提供此类信息

5	图片/视频类	包含人脸的图片/视频	1）需获得被拍摄人对使用其人脸特征的授权和同意方可采购或提供 2）涉及未成年人的，应获取其监护人的同意或明示同意 3）从第三方获得的，需有允许组织或其他方使用的授权 4） 不得含有非法信息
6	图片/视频类	名片/票据（含购物小票等）	1） 需确保来源合法并有权提供给第三方使用 2）对于不需要个人信息或企业商业信息的，应予以匿名化处理 3）对于需要其中个人信息或企业商业信息的，应得到授权或同意
7	图片/视频类	翻拍或扫描的文档	1）信息应不得含有涉及国家秘密、侵害他人商业秘密或侵犯知识产权的内容 2）不得含有个人信息，除非获得了相关信息主体的明确同意和授权
8	公开数据	通过爬虫爬取网络上公开的文本、图片和视频	对供应商爬取数据时应提出要求： 1）只能爬取公开数据 2）不能绕过技术限制（如 ROBOT 协议、密码鉴权等） 3）遵守已签署的用户协议 4）不能给网站造成额外的资源影响 5）在网站通知停止时应停止爬取 6）控制使用目的（避免不正当竞争） 7）不侵犯知识产权 8）爬取的信息不属于非法信息

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