基于《个人信息保护法》的企业个人信息保护合规风险控制验证框架1.0

CSA GCR cloud security GREATER CHINA REGION alliance ®

致 谢

云安全联盟大中华区（简称：CSA GCR）隐私与个人信息保护法律工作组在2021 年 4 月成立。由原浩、方婷担任工作组联席组长，工作组专家来自竹辉律师事务所、西北大学、恩智浦、中伦文德事务所、美柚、中国工商银行、绿盟科技、美云智数、上海 CA、上海网综所、埃森哲、亚萨合莱、360 政企安全、软通动力信息、艾贝链动等十多个单位。

本框架由 CSA 大中华区隐私与个人信息保护法律 工作组专家撰写，感谢以下专家的贡献：

联席组长：原浩、方婷

贡献者名单

原创作者：高健凯、胡恺健、赵晔、张元恺、曾令平、江澎、马宁、邢海韬、黄鹏华、夏巍、魏晓刚

审核专家：郭鹏程、姚凯

研究协调员：高健凯

贡献单位：绿盟科技集团股份有限公司、广东美云智数科技有限公司、北森云计算有限公司

（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。

如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正! 联系邮箱： research@c-csa.cn；云安全联盟 CSA 公众号：

目录

致 谢.....3

1.框架的结构及考虑.....5

1.1 原则和通用.....5

1.2 知情同意和处理规则.....6

1.3 对自动化决策的特别关注.....6

1.4 敏感个人信息的特别关注.....6

1.5 数据出境的统一考虑.....6

1.6 个人权利和对个人权利的回应.....7

1.7 在企业架构和制度中的体现.....7

1.8 记录和证据.....7

1.9 第三方和供应链.....7

2.框架的方法论.....8

2.1 高度概括合规要求（D 列）.....8

2.2 将合规要求做解读后对应到企业规范文件或产品呈现（F/G 列）.....8

2.3 从最普遍的标准切入企业控制措施（H/I 列）.....8

2.4 对措施的增强介绍或解释（J 列）.....9

2.5 对触发合规的最低时限或阶段要求.....9

3.框架的维护更新与其他声明.....9

4.附件（框架）.....9

基于《个人信息保护法》的企业个人信息保护合规

风险控制验证框架 1.0

说明文档

1. 框架的结构及考虑

控制框架从 10 个维度搭建，大部分的维度之间为独立关系，但部分维度具有包括关系。这主要是考虑到《个人信息保护法》的架构，以及对于原则、规则等本身既有概括性的必然。

目前围绕个人信息或隐私管理国内外有不同的框架工具，本框架可以作为：（1）基于最为通用的 ISO 2700x 细化的映射，实现对个人信息保护与管理的全面覆盖；（2）对于已经使用欧盟 GDPR 或者网信、工信部门的既有规范进行合规工作的符合性，提供额外的验证过程。

1.1 原则和通用

目前个人信息保护的主要原则可以概括是为：合法正当必要性原则、合理直接目的性原则、最小影响和最小范围原则。将这些确定为原则，主要原因是对必要性、合理性、最小化这些概念难以和缺少准确的衡量指标，且新技术、新应用又不断的冲击既有的量化标准。

由于这些原则具有在产品、服务设计中的普遍适用性，且在进行是否合规的“终极”判定时，或者在无其他明确法律依据支持佐证时，需要直接援引这些原则判断。因此，就其中最为基础的必要性原则，也称之为个人信息保护合规判定的“帝王原则”。

值得注意的是，这些原则判断的最终权，在监管机构（执法）和司法机关。合规工作虽然可以减轻或降低风险后果，但不能完全免责[1]。

1.2 知情同意和处理规则

将知情同意作为处理规则的起点，而不再作为合规的原则，主要是考虑到知情同意的各种实现是非常实务的运用，不像上述原则一样“抽象”，目前的合规起步主要的都是通过个人信息处理规则“呈现”完成，同时《个人信息保护法》对构筑知情同意列举了大量条款，需要相应的进行合规设计。

值得注意的是，知情同意构成了个人信息处理规则（无论是隐私政策、服务协议等等）贯穿始终的基准。

1.3 对自动化决策的特别关注

自动化决策是《个人信息保护法》中为数不多的涉及算法[2]、人工智能等相关的条款，其代表了未来监管所可能关注的增设、重要方面，因此本框架给与特别关注。

1.4 敏感个人信息的特别关注

一般个人信息和敏感个人信息是对个人信息的基本分类，也符合《数据安全法》对数据分类分级的一般要求。将个人信息做敏感和一般的分类（《个人信息保护法》做具体列举，是从分类而非分级的考虑），同时形成了个人信息分级的初始目的。敏感个人信息需要附加额外的控制措施，因此应特别关注。

1.5 数据出境的统一考虑

数据出境安全评估办法明确了对个人信息和重要数据适用统一的出境评估规则，对数据出境的合规尽管不是所有运营者、处理者都需要面对的问题，其

[1] 最高人民检察院在2021年发布《关于建立涉案企业合规第三方监督评估机制的指导意见（试行）》，对涉案企业合规不起诉模式正在进行持续探索。

[2] 《互联网信息服务算法推荐管理规定》已经通过实施，其对行业可能产生的影响尚有待进一步观察。

规则的要求也具有不同于个人信息的一般处理的要求，但由于出境选择的多样性和触发条件的不同，数据出境自身形成了相对独立的合规评价体系[3]。

1.6 个人权利和对个人权利的回应

虽然《个人信息保护法》将个人的权利作为专章规定，但从企业合规的角度对应的是对这些权利的响应。虽然企业从业务流程和个人信息生命周期已经涉及对个人权利的响应，但将其单独作为一个维度，有助于体系化的验证对个人信息响应和保护的程度。

1.7 在企业架构和制度中的体现

从组织架构和风险控制制度出发规范个人信息保护与合规，符合传统风险控制和管理的思路，也是本框架与既有的标准建立关联和匹配的基础，最终也是合规的形式化成果和验证依据。

1.8 记录和证据

本框架也突出了记录和证据的重要性。一方面是从《网络安全法》以来对记录、日志等已经提出了越来越多的要求，另一方面，从法律的角度考虑这些记录和证据，体现出本框架作为法律合规框架，而非其他框架的独有特点。毕竟，所有的日志、记录等等只有符合法律规定的形式和内容要求，才能成为企业合规和免责的依据[4]。

1.9 第三方和供应链

对第三方合作伙伴和从供应链角度考虑个人信息保护，为企业提供了外部性的多重视角，尽管供应链安全的最重要问题并非个人信息保护，但个人信息保护的重要方面涉及对与外部的合同、协议评价和在信息传递、转移中的大量处理行为的合规评价。特别是在数字经济的宏观背景和平台模式直接面对最终

[3] 公开信息显示，《数据出境安全评估办法（征求意见稿）》尝试进行统一的数据出境安排，但未来仍有可能就个人信息与重要数据出境分别设置不同的规则，因此征求意见稿的施行仍有不确定性。

[4] 对电子数据证据，应充分结合《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》《关于民事诉讼证据的若干规定》。任何合规框架不应代替对电子证据的过程化考虑，且企业应注意，对行政和刑事案件中，证据的收集、提取、固定、审查应主要属于侦察、检察机关的活动。

用户的微观场景下，传统信息安全标准的企业“内控”已经不能完全满足企业业务活动的需要，这就是为何供应链安全、BYOD、零信任等概念愈发受到重视的部分非技术原因。

2.框架的方法论

框架主要从法律规定出发，而非从单一的权利主体个人视角或者从监管角度、技术角度，尝试建立一个可自洽并周延的体系。为此主要使用了以下方法和逻辑：

2.1 高度概括合规要求（D 列）

将《个人信息保护法》的合规要求先做高度凝练，便于全文化和随机的检索。其优点是能够快速检索到关注的合规要求，缺点是可能因概括而导致信息缺失。

2.2 将合规要求做解读后对应到企业规范文件或产品呈现（F/G 列）

将合规要求适当展开，并落实到企业的产品、服务中，便于确认这些合规要求在企业层面的体现形式，例如哪些需要体现在个人信息处理规则（隐私政策展示、确认等）、哪些属于企业内部规章制度（访问控制规则、流程等）。

2.3 从最普遍的标准切入企业控制措施（H/I 列）

本框架选取了业界认可度最高，并遵循技术中立性的 ISO 27001（及 27018）对企业合规的控制措施。一方面这符合目前主流的合规框架的方法论，例如 NIST 的关键基础设施框架也已穷尽对应更多的标准方法，另一方面 ISO 的上述标准不寻求特定技术，能够符合企业不同程度的匹配要求，并且 27018 等对个人信息保护进行了扩展控制建议，也符合本框架寻求可扩展的弹性要求。

当然受限于表格形式，企业需要对应 ISO 的具体文本。

2.4 对措施的增强介绍或解释（J 列）

除了对一般合规管理的标准描述，框架也尝试对可用的拓展的措施，包括安全技术措施做适当引介，这样企业可以快速的找到必要的措施以快速符合合规法律的技术要求，以应对技术发展变化的需求，因此此部分内容也将保持持续更新。

2.5 对触发合规的最低时限或阶段要求

对于不同的合规要求，企业实践中存在一个适用性、优先性，以及何时触发的判断。对应优先性，框架基于一般企业给出了排序的参考建议，这主要是结合了监管在一定时期内的关注、热点，因此也存在动态调整，并不同规模的企业其优先性考虑也有差异；对于触发问题，最典型的如数据出境，可能非普遍性义务，需要达到触发条件，且由于数据出境安全评估办法规定了一个累计、动态的衡量标准，需要企业持续对个人信息进行“监测”，以便在适当的时点启动合规。为此框架在后续版本中将考虑设定了一个触发合规的时点要求，将最迟、不晚于某个时点需要做相应合规动作进行原则性的设定。

3. 框架的维护更新与其他声明

本框架由云安全联盟大中华区“隐私与个人信息保护法律工作组”制定并维护。

对本框架的使用受限于云安全联盟大中华区及其网站的规则。请登录 CSA GCR 网站 https://www.c-csa.cn/获取更多信息。

4. 附件（框架）

（以下为附件）

基于《个人信息保护法》的企业个人信息保护风险控制合规验证框架

			合规要求（D）	法律依据（E）	条款解读/典型场景描述（F）	管理控制措施（G）	ISO 27001（H）	管理控制的描述（I）	增强的控制场景或措施（J）	备注（K）/优先性
CSA GCR 隐私与个人信息保护法律工作组维护，2021.12										
	区分不同的合规种类，便于识别企业行为		提炼合规要点，粒度在条款级别	此部分对应到《个人信息保护法》的具体条款，但不再援引全文；考虑到配套制度，也会就主要的配套法规、标准的条款做提示	解读法律规定的要旨，并尽可能列举法律风险（行为）；注意不同的风险行为可能对应于对同一合规要求的违反	列举主要的制度、技术措施，可用于判断现有措施的符合性；亦包括可用的整改机制	对应到 ISO 27001（含 27018，红色标识）的具体控制措施项下（需要特别说明的是，27 系列并非仅为个人信息保护设计，且其主要从企业风险角度出发，而非用户利益角度）	对标准应用的进一步描述和其他参考，整体上将个人的权利作为产品、服务设计和实现的功能部分，因此此部分主要的归入 A14	增加或补充描述一些可能实现的场景	就相关合规要求的风险程度、特别是已经普及的程度、监管关注程度、法律后果的严重性进行优先排序（更细粒度的量化应结合风险评估），但组织应考虑监管不同阶段的关注亦有变化；零就框架合规要求之间的关联进行识别和标注；其他备注
1	原则/通用	1	合法正当必要诚信	5	正向判定的基本依据是知情同意；反向还需判定是否通过误导、欺诈、胁迫等方式处理个人信息	个人信息处理规则；产品服务功能展示	A.5.1.1	应在信息安全策略和承诺中植入个人信息保护的基本原则	通过隐私政策和专门页面等组合方式呈现； 其中，必要性与最小化属于动态可量化机制	高
		2	明确合理直接关联目的	6	处理应与业务目的直接相关，应与产品服务类型直接相关	产品服务功能解释说明	A.14.1.1; A.14.2.1; A.14.2.8; A.14.2.9; A.6.1.5; A.3.1	是否符合目的性，作为系统（产品、服务）验收的依据之一 应在信息系统的开发需求阶段、开发过程阶段、测试验收阶段确认符合目的性原则		高
		3	个人权益影响最小的方式	6	这里的权益是《民法典》界定的各项经济权益与人格权益的统称	个人信息保护影响评估报告	A.12.1.1; A.14	应从对个人的（1）限制个人自主决定权；（2）不合理的差别待遇；（3）人身财产损失；（4）名誉权等人格损失或精神损失多角度评价影响		中
		4	实现产品服务目的最小范围	6	与产品服务的基本功能对应；必要功能对应必要收集（和处理）	产品服务功能解释说明	A.6.1.5; A.14.1; A.12.1.1； A.5	是否符合目的性和必要性原则，作为系统（产品、服务）验收的依据之一；应在产品、服务设计时考虑个人信息安全，并进行分析和规范化。最小化存储和删除数据文件，属于最小范围的考虑，并涉及用户删除权的行使（和验证）	产品服务的内容、范围变化，可能导致必要性和最小化原则的扩张、缩小或丧失	高

		5	产品服务必需功能	16；《常见类型移动互联网应用程序必要个人信息范围规定》	与产品服务的基本功能对应；必要功能对应必要收集	产品服务功能解释说明；实名制注册是所有产品、服务的必需功能	A.14.1; A.14.2.1; A.14.2.8; A.14.2.9; A.12.1.1	是否符合目的性和必要性原则，作为系统（产品、服务）验收的依据之一 应在信息系统的开发需求阶段、开发过程阶段、测试验收阶段确认收集的信息都为功能所必须		高
		6	公开透明	7	个人信息处理规则公开；处理过程（目的、方式与范围）透明；算法可解释	个人信息处理规则	A.5.1.1	应在信息安全策略中明确个人信息处理规则	透明度与算法等知识产权有关，应综合监管机构的具体要求，确定透明度。部分年度透明度报告可参考	低
		7	数据质量	8；《数据安全法》	避免因个人信息不准确、不完整对个人权益造成不利影响；但并不意味着企业可以强制要求个人补充和完善（对应产品功能非必要的）个人信息		A.12.3; A.14	备份是常规控制机制之一；完整性考虑应在产品、服务设计中考虑和增加实现、验证机制	在某些合同场景下，可对个人提供的数据质量提出要求和义务，但前提还应包括适当的对价	低
		8	明示处理的目的方式和范围	7	个人信息处理规则公开；处理过程（目的、方式与范围）透明；算法可解释	个人信息处理规则	A.6.1.5; A.14.1.1; A.14.2.1; A.14.2.8; A.14.2.9	应在信息系统的开发需求阶段、开发过程阶段、测试验收阶段确保系统有明确功能实现明示处理目的	应在产品、服务设计过程中，加入个人信息收集的明示	中
2	知情同意和处理规则	9	知情同意（起点）	13.1；14	自愿和明确做出，且提供和撤回同意的方式。格式条款和默认选定可能会认为非自愿、不明确。	个人信息处理规则和对规则的选择、记录过程（例如点击、勾选）	A.9.2; A.9.3; A.14.1; A.14.2.1; A.14.2.8; A.14.2.9; A.12.1.1	将个人信息安全植入开发过程；知情同意为注册和对企业产品、服务的访问的前提条件	应在产品、服务设计过程中，加入数据收集点的相关同意记录，并由用户通过逐项勾选个人信息、弹窗确认等方式完成每项个人信息的同意确认	中
		10	个人信息处理规则的设计和告知	17	名称、联系方式、处理目的、方式、个人信息种类、保存期限、个人权利。个人对处理规则的同意，为开启使用的前提	个人信息处理规则	A.5.1.1; A.14.1.1; A.14.2.1; A.14.2.8; A.14.2.9; A.18.1	应在产品、服务设计过程中，加入数据收集点的相关同意记录，并由用户通过逐项勾选个人信息、弹窗确认等方式完成每项个人信息的同意确认	可考虑采用层次化的隐私政策展现个人信息处理的相关规则。采用 1 个静态隐私政策文本+1 个首页横幅+N 个单独同意的精简弹窗告知	中
		11	无需同意的告知	13.2	应区分事先和事后告知的具体场景，例如履行监督职能和公共安全的，告知时点不同			告知并不一定意味着需要同意，例如基于公共利益的考虑		低
		12	重新同意	14	处理目的、种类、方式变更，意味着原有同意失效，需重新同意；不同系统下的同一应用，应视为需重新同意	个人信息处理规则和对规则的选择、记录过程（例如点击、勾选）	A.9.2.1; A.9.2.2; A.9.2.6; A.12.1.2; A.14.1.1; A.14.2.1; A.14.2.8; A.14.2.9;	重新同意可能意味着连续使用（以前的数据有效），也可能为从零开始使用	应在产品、服务设计过程中，提供因个人信息处理活动变更时的站内信、弹框等重新告知和取得同意的功能	中
		13	撤回同意	15	自愿和明确做出，且提供和撤回同意的方式	个人信息处理规则和对规则的选择、记录过程（例如点击、勾选）	A.9.2.1; A.9.2.5; A.9.2.6; A.9.3; A.14.1.1; A.14.2.1; A.14.2.8; A.14.2.9	在提供撤回选择时，个人也应当了解撤回的后果 企业应评估如何处理撤回范围之外的个人信息	分别针对 APP 功能、SDK、Cookie 等提供	中
		14	撤销同意		参照删除处理		A.9.2.1; A.9.2.6			中
		15	个人信息处理规则版本更新的告知	17	版本更新应告知，并公开；对涉及用户权益的规则，应重新取得同意	个人信息处理规则	A.12.1.1; A.12.1.2; A.14.2.2; A.18.1	在变更管理中考虑规则变更、个人信息主体同意拒绝的变更等。规则版本的任何变动，应体现法律和政策的变化		中

		16	实现处理目的所必要的最短保存期限	19	以交易完成作为保存期限的基础；如延长保存期限，需要有相应的处理目的支持。匿名化为从个人信息转化为企业信息的前提	个人信息处理规则的目的描述；存储期限的比对	A.14.1.1; A.14.2.1; A.14.2.8; A.12.3	应在信息系统的开发需求阶段、开发过程阶段、测试验收阶段确保系统中收集的信息保存期限合规，到期删除。同时控制生产数据中个人信息在测试环境中的使用。	应通过时间戳、过期提醒等方式建立触发期限的机制	高
		17	转移、共享、提供的告知	22；23	应在个人信息处理规则（隐私政策、用户指南等）中告知个人信息向特定方转移、提供、共享，并取得同意	个人信息处理规则	A.5.1.1; A.13.2; A.18.1; A.8.1			高
		18	单独同意：转让个人信息	23	由于处理者主体变化，应取得个人单独同意	转让协议	A.13.2; A.18.1	应在隐私政策中明确转让的第三方信息，概括转让不视为符合		高
3	自动化决策	19	自动化决策的透明度	24	进行算法机制、机理审核：定期审核、评估、验证算法机制机理、模型、数据和应用结果	个人信息处理规则（专章）	A.5.1.1	公开透明原则在自动化决策中的体现		高
		20	用于推送和营销的自动化决策的选项填充	24	通过“内容去重、打散干预”等方式，提供不针对其个人特征的选项，或者提供便捷的拒绝方式	个人信息处理规则（专章）	A.14.1.1; A.14.2.1; A.14.2.9; A.3.2	营销目的的使用，应经用户明确同意，并可随时拒绝同意	APP 开发者应考虑操作系统对营销、广告等活动的技术限制	高
		21	自动化决策的解释说明	24	公示算法推荐服务的基本原理、目的意图、运行机制等	个人信息处理规则（专章）	A.14.1.1; A.14.2.1; A.14.2.9; A.18.1			中
		22	算法规范	《互联网信息服务算法推荐管理规定》	对算法增加考虑分类分级、日志留存、安全评估	个人信息处理规则（专章）；算法机制	A.5.1.1; A.14.1.1; A.14.2.1; A.14.2.9; A.18.1	应首先在《互联网信息服务算法推荐管理规定》下确定企业所涉及算法的归类，以及是否备案等基本问题	应区分自动化决策的解释性，与算法的可解释性。前者是过程描述 并非所有的算法都归入《互联网信息服务算法推荐管理规定》所界定的“算法”	中
4	个人信息的公开及可能的公共数据	23	单独同意：公开个人信息	25; 26; 《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》	公开个人信息，或公共安全目的获取的个人信息用于其他用途，应取得个人单独同意	单独的书面（电子化）通知请求	A.13.2; A.18.1			中
		24	已公开信息的处理	27	个人有后续拒绝权		A.13.2; A.18.1		例如：考虑通过企业信息公示系统、裁判文书、媒体公开报道等形式公开后的个人信息使用范围	低
5	敏感个人信息	25	特定的目的和充分必要性	28	个人信息分类分级，应就敏感个人信息（第 28 条）单独收集；已收集的单独识别；已识别的单独处理	个人信息处理规则（专章）		在一般个人信息基础上的附加考虑	不可分的应按照就高不就低原则处理	高
		26	单独同意：敏感个人信息	29	基于告知——（单独）同意规则	个人信息处理规则（专章）	A.13.2; A.18.1			高
6	出境	27	单独同意：出境个人信息	39	基于告知——（单独）同意规则	企业业务合同；个人信息处理规则	A.13.2; A.18.1; A.12.3.1			中
		28	自评估							高

		29	安全评估	《数据出境安全评估办法（征求意见稿）》	CII和达标数量的企业，应进行安全评估	安全评估报告	A.18.1; A.11.11	主要涉及触发安全评估的条件判断	《数据出境安全评估办法（征求意见稿）》扩大了安全评估的使用范围	高
		30	保护认证	38	细则待定	认证过程和结果（证书）		择一适用；认证的有效期应考虑		中
		31	标准合同	38	细则待定（GDPR）版本的法律冲突和优先适用问题应考虑	企业业务合同；个人信息处理规则	A.18.1; A.11.11	择一适用；标准合同条款的部分引用，不适为采用了标准合同模式		中
7	对个人权利请求的回应	32	知情权	44	知情体现在个人信息收集、使用，直至删除的全生命周期	个人信息处理规则	A.9.2.2; A.9.2.3; A.9.2.5; A.9.2.6; A.9.3 A.2.1	将用户设置或配置账户信息和保护口令信息的义务部分转移至用户个人；并应系统的描述用户自身的义务和责任（不局限于9.3对员工的用户责任描述）。整体上而言，对个人用户权利的回应应在协议、规则中做出，并相关技术措施也需在协议中进行明确。	应区分个人信息的性质，分别采用结构化查询和非结构化查询的方式分别符合	中
		33	决定权	44	有权提供、限制或者拒绝他人对其个人信息进行处理	个人信息处理规则	A.9.2; A.14.1.1; A.14.2.1; A.14.2.9	用户决定权取决于对其访问控制的配置与控制	应在产品、服务设计中加入隐私偏好中心，为用户提供拒绝个人信息处理的能力	中
		34	拒绝权	45	拒绝权包括未收集的拒绝，已收集的删除	个人信息处理规则	A.14.1.1; A.14.2.1; A.14.2.9		应符合监管机构处理时限的要求（15工作日）	中
		35	查阅权	45	已可辨识、可读（结构化）的方式；可按照个人请求查阅的范围精确提供，但如个人要求全部查阅的，则应全部呈现	个人信息处理规则	A.13.2			中
		36	复制权	45	对查阅信息的复制和获取	个人信息处理规则	A.13.2		查阅与复制的区别，以及重复查阅、复制所可能产生的费用列明	中
		37	可携带权	45	权利的提出应符合法定条件（网信待定）和可携带性（如类似应用）	个人信息处理规则	A.13.2	符合下列条件的个人信息转移请求，数据处理者应当为个人指定的其他数据处理者访问、获取其个人信息提供转移服务：（1）请求转移的个人信息是基于同意或者订立、履行合同所必需而收集的个人信息；（2）请求转移的个人信息是本人信息或者请求人合法获得且不违背他人意愿的他人信息；（3）能够验证请求人的合法身份。	可携带权将导致企业产生额外成本，应进行费用列明	低
		38	更正权	46	为个人权利；如果企业为数据质量的，则应请求个人更正和补充	个人信息处理规则	A.9.2.5; A.9.2.6	企业对发生的个人信息错误，不应主动更正，但影响业务运行的，应以通知方式告知	错误信息导致业务无法运行的，结合数据质量和“删除权”	中
		39	删除权	47	处理目的、留存期限等	个人信息处理规则	A.9.2.6; A.11.2.5; A.11.2.7; A.12.3; A.11.3	对备份信息的删除应在协议中考虑，例如自动化备份，以及为争议解决的备份。对已删除数据的恢复，应考虑对删除权的影响。	删除与账户注销应关联考虑	高
		40	解释权	48	有权要求企业对个人信息处理规则进行解释说明	个人信息处理规则	A.13.2; A.18.1		自动化决策、算法	中

		41	继承权	49	涉及近亲属利益的可继承性，企业需对其身份（近亲属）和其利益（正当性）进行判定	个人信息处理规则	A.13.2; A.18.1			中
		42	救济权	50	建立便捷的个人行使权利的申请受理和处理机制，包括联系方式、智能和人工应答等；诉讼	应用交互页面；外部链接	A.13.2; A.18.1			低
8	管理制度和合规架构	43	规章制度	51	应在等级保护制度、资产管理、访问控制、业务流程、员工手册等具体规章制度中体现个人信息保护	网络安全管理制度（人力、资源、访问）	A.5.1; A.6.1; A.13.2; A.11.11	应在信息安全策略文件和承诺中增加体现个人信息保护。应考虑协议于规章制度的契合度。		高
		44	操作规程	51	针对个人信息处理过程的操作规程，应与企业业务流程的操作相匹配	业务流程文件	A.6.1.5; A.9.2; A.10.1.2; A.13.2; A.12.4.1; A.8.1.3; A.8.1.4; A.8.2.3; A.8.3.3; A.8.3.2; A.12.1.1; A.12.1.2	授权过程中体现对个人信息的访问权限; 应能识别外部第三方对企业资产、数据的访问，并符合企业的网络安全要求; 将个人信息，及企业在去标识化、匿名化后形成的数据，分别识别和建立资产清单和管理制度		高
		45	分类分级	51	数据分类分级在个人信息保护领域中的体现，敏感和一般为典型的分级，第 28 条提供了敏感个人信息的分类示范	资产管理制度	A.8.2	应在信息资产的分类分级中考虑个人信息；以及个人信息在何种情况下可能成为重要数据	例如《金融数据安全数据安全分级指南》给出了行业分类的参照	高
		46	加密	51	包括对存储和传输的个人信息加密	传统的加密机制和策略	A.9.4.1; A.9.4.2; A.10.1; A.11.5; A.11.6	不使用无加密的移动介质，以及 HTTPS 默认加密	国密系列算法，以及同态加密、安全多方计算等提供了加密在特定场景中的部分方案	高
		47	去标识化	51	以降低个人信息的敏感程度	典型的去标识化工具，及隐私计算工具	A.18.2.3		主流的隐私计算技术提供了实现去标识化的部分功能，但去标识化与匿名化不应等同	高
		48	物理访问控制				A.6.2; A.11	特别的，应对设备进出和转移进行控制和授权		中
		49	系统与网络访问控制				A.9; A.11.2; A.11.7; A.11.8	访问控制应该是所有用户创建和使用产品、服务的基础，ID 管理和用户权限是访问控制的基础动作		高
		50	从业人员管理	51	人员角色、职责和责任的宣贯培训、访问策略配置	配置策略、访问控制策略、员工手册	A.6.1.2; A6.2; A.7	有关人员自带设备（BYOD）同时涉及的物理、逻辑和人员控制，可进一步参考 BYOD 指南或其他文件		高
		51	应急预案	51	在网络安全应急预案中体现个人信息保护	网络安全应急预案	A.16	将个人信息安全事件管理纳入应急预案并给与响应		中
		52	个人信息保护负责人	52	在管理层设定个人信息保护的角色	章程、董事会决议、（总）经理任命职责	A.6.1.1	应在信息安全责任划分中增加和突出负责人角色		高
		53	保护负责机构	52	在内部控制等既有机构中，或单独设置个人信息保护的负责机构；头部企业应履行备案义务	公司治理的管理层、组织架构	A.6.1.1	一般涉及两个层面，包括管理层（董事会）内设机构，以及组织架构的特定角色机构与人员		高
		54	审计	54	主动发起审计（在 IT 审计中包括个人信息审计）	IT 审计等	A.18.2.1; A.12.7	应以独立性为前提进行必要的个人信息安全审计		中
		55	接受审计		接受网信部门审计		N/A			中

		56	个人信息保护影响评估	55；《GBT 39335-2020》	评估报告和处理情况记录的保存应符合《民法典》诉讼时效的规定	评估报告	A.18.2.1；A.18.2.2	《GBT 39335-2020》		高
		57	通知	57	向网信部门和受影响的个人通知	符合内容和形式要求的电子化（书面）通知	A.13.2；A.14.1；A.6.1；A.10.1		通知应符合时效性和形式要求；应考虑时间戳、回执等以确定和保存通知的送达	高
		58	外部监督机构	58	对大型平台的“守门人”义务要求					低
		59	平台规则	58	对大型平台的“守门人”义务要求					低
		60	通知——停止规则	58	对大型平台的“守门人”义务要求				应注意与传统的避风港原则的异同	低
		61	社会责任报告	58	对大型平台的“守门人”义务要求					低
		62	接受测评	61.3	测评对象是企业的产品、服务	测评报告	A.6.1.3	应与网信部门、公安部门、工信部门、市监部门等建立适当联系		中
		63	接受检查	63	检查对象是企业自身（的生产运营）	检查结论、整改记录	A.6.1.3；A.14；A.17	极端情况下，个人信息保护的违规，可能导致停业整顿等业务业务连续性的风险		高
		64	执法协助	《网络安全法》第28条	协助提供数据、记录，权限及必要的设施设备	保留协助记录		系统文件的必要保护作为合规遵从的依据之一		中
9	记录与证据	65	日志的时限		网络日志及留存应符合《网络安全法》时限要求	留存期限和可审计	A.12.4；A.18.1.3；A.18.2	应部署自动化日志工具，并考虑审计必要性		高
		66	日志的时效		网络日志及留存应符合诉讼时效的时限要求	留存期限和可审计	A.12.4；A.18.1.3；A.18.2	考虑法定与约定留存时限发生冲突时的处理		高
		67	记录		记录应符合网络数据的三性要求，并在验证是否符合网络安全保护义务、个人信息保护义务时以“电子数据证据”的形式提供		A.18.1.3；A.18.2；A.16.1.7；A.6.2	应区分日志、记录和数据、事件		高
		68	电子数据证据	《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》			A.18.1	应从证据的生命周期考虑可靠的证据链实现		高
10	第三方与供应链	69	管理供应商与供应链安全		与供应商的协议	协议审查；权限配置；过程检查	A.6.1.4；A 6.1.5；A.14.2.7；A.15；A.11.12	应通过尽职调查等对外包方进行必要的识别和审查；并在开发外包中关注个人信息保护		高
		70	向客户提供产品服务中的个人信息保护		与客户方的协议	协议审查；权限配置；过程检查	A.6.1.4；A 6.1.5；A.14.2.7；A.15	对获取的客户信息、最终用户信息，应考虑协议明确各方权利义务的边界	委托协议在《个人信息保护法》下具有合同相对性的基本功能，应考虑在协议中体现委托关系（如适用）；GDPR 的数据控制者与数据处理者区分具有参考意义，但不完全适用于境内	高
		71			保密协议		A.13.2.4	包括员工保密协议和对第三方的保密义务，以及要求第三方保密的义务		中
		72			第三方开放工具接口等（SDK）	协议中披露 SDK 主体和功能		在隐私政策中列明，并结合个人撤回同意的考虑		高