|  |  |
| --- | --- |
| ICS | 35.030 |
| CCS | |  | | --- | |  |   L 80 |

团体标准

T/ZS XXXX—2024

个人信息跨境处理活动安全规范

Safety norms for cross-border processing activities of personal information

（征求意见稿）

2024-XX-XX发布

2024-XX-XX实施

浙江省产品与工程标准化协会  发布

目次

[前言 II](#_Toc6125)

[1 范围 1](#_Toc16552)

[2 规范性引用文件 1](#_Toc6879)

[3 术语和定义 1](#_Toc7346)

[4 基本要求 1](#_Toc31935)

[5 个人信息主体 2](#_Toc10041)

[6 组织管理 2](#_Toc5722)

[7 信息跨境处理 3](#_Toc20991)

[8 个人信息影响评估 3](#_Toc17896)

前言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件起草单位：连连数字科技股份有限公司、杭州市金融人才协会。

本文件主要起草人：应骏、汤怡、童将、初永光、虞群娥、叶嘉怡、金娟娟。

个人信息跨境处理活动安全规范

* 1. 范围

本文件规定了个人信息跨境处理活动安全的基本要求、个人信息主体、组织管理、信息跨境处理、个人信息影响评估等内容。

本文件适用于跨国企业、跨境电子商务平台、云服务提供商等涉及个人信息跨境处理活动的组织和企业。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T25069-2022 信息安全技术术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

* 1. 术语和定义

GB/T25069-2022、GB/T 35273-2020界定的以及下列定义或术语适用于本标准。

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，不包括匿名化处理后的信息。

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

* + 1. 境外接收方 outland receiver

位于中华人民共和国境外并自个人信息处理者处接收个人信息的组织或个人。

* + 1. 个人信息处理者 personal information

在个人信息处理活动中自主决定处理目的、处理方式的组织或个人。

* 1. 基本要求

开展个人信息跨境处理活动的个人信息处理者和境外接收方应签订具有法律约束力和可执行的合同；合同内容应包含但不限于以下内容：

* 1. 个人信息处理者和境外接收方的名称、地址、联系人姓名、联系方式等基本信息；
  2. 个人信息跨境处理的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点等；
  3. 个人信息处理者和境外接收方保护个人信息的责任与义务；
  4. 个人信息跨境处理可能带来安全风险所采取的技术和应对措施等；
  5. 个人信息主体的权利，以及保障个人信息主体权利的途径和方式；
  6. 合同解除、违约责任、争议等解决办法；
  7. 处理过程中的数据加密、访问控制、监控和日志记录等技术措施；
  8. 具体的数据泄露应急预案和恢复计划；
  9. 各方应遵守的法律、行政法规规定的义务。
  10. 个人信息主体
      1. 主体义务
         1. 个人信息主体应仔细阅读并理解个人信息跨境处理的相关条款和条件，包括目的、范围、处理方式以及可能的风险。
         2. 人信息主体应确保提供的个人信息是准确、完整和最新的。
         3. 如果发现任何可疑活动或未经授权的访问，应立即报告给相关的个人信息处理者或数据保护机构。
      2. 主体权利
         1. 个人信息主体有权了解其个人信息被收集、使用、处理、存储和传输的具体情况，以及参与相关决策的权利。
         2. 如果个人信息主体发现其个人信息在跨境处理过程中存在错误或不完整，有权要求更正或删除。
         3. 如果个人信息主体因个人信息跨境处理活动受到损害，有权要求相应的赔偿。
         4. 个人信息主体有权直接向境外接收方提出请求。
         5. 个人信息主体有权选择是否允许其个人信息被跨境处理，以及在何种情况下允许跨境处理。个人信息主体有权根据相关法律法规要求查阅、更正、删除或转移其个人信息。
         6. 个人信息主体可以通过提交书面申请、在线表单或客服热线等方式行使其权利。个人信息处理者应在收到申请后的30个工作日内予以回复。
  11. 组织管理
      1. 信息保护负责人
         1. 开展个人信息跨境处理活动的个人信息处理者和境外接收方均应指定个人信息保护负责人。
         2. 应具备个人信息保护专业知识和相关管理工作经历。
         3. 应明确个人信息保护工作的主要目标、基本要求、工作任务、保护措施。
         4. 应指导、支持相关人员开展本组织的个人信息保护工作，确保个人信息保护工作达到预期目标。
         5. 应定期向高层管理人员汇报个人信息保护工作的进展和存在的问题，并提出改进建议。
      2. 信息保护机构
         1. 开展个人信息跨境处理活动的个人信息处理者和境外接收方均应设立个人信息保护机构。
         2. 应履行个人信息保护义务，保障个人信息安全，防止未经授权的访问以及个人信息泄露、篡改、丢失等。
         3. 应依法制定并实施个人信息跨境处理活动计划。
         4. 应定期组织开展个人信息保护影响评估。
         5. 应接受和处理个人信息主体的请求和投诉。
         6. 应接受认证机构对个人信息跨境处理活动的持续监督，包括复询问、配合检查等。
         7. 应每年至少进行一次内部数据保护审计，确保个人信息保护措施的有效性和合规性。
      3. 境外接收方
         1. 应确保处理个人信息的活动达到中国相关法律法规规定的个人信息保护标准。
         2. 应按照与个人信息处理者签订的合同或协议中的约定，处理个人信息。
         3. 境外接收方应尊重并保障个人信息主体的合法权益，如知情权、同意权、访问权、更正权、删除权等。
         4. 应保障个人信息的质量，包括信息的准确性、完整性、可用性等。
         5. 在需要进行数据出境安全评估的情况下，境外接收方应配合个人信息处理者完成相关评估工作，提供必要的资料和信息。
         6. 应承诺不将所接收的个人信息提供给第三方；如确需提供的，应满足中华人民共和国有关法律、行政法规要求。
         7. 当出现难以保证个人信息安全的情况时，应及时停止跨境处理个人信息，并通知个人信息主体。
         8. 发生或者可能发生个人信息泄露、篡改、丢失的情况下，应立即采取补救措施，并通知个人信息主体。
  12. 信息跨境处理
      1. 处理条件
         1. 个人信息跨境处理活动应通过国家网信部门组织的安全评估。
         2. 应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. 应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。
      2. 处理规则
         1. 应明确跨境处理个人信息的目的、方式和范围。
         2. 应明确跨境处理个人信息的基本情况，包括个人信息数量、范围、种类、感程度等。
         3. 应明确个人信息境外存储的起止时间及期满后的处理方式。
         4. 应明确跨境处理个人信息需要中转的国家或者地区。
         5. 应保障个人信息主体权益所需资源及明确需采取的措施。
         6. 应明确个人信息安全事件的赔偿、处置规则。
  13. 个人信息影响评估
      1. 评估内容
         1. 应分析个人信息的内容，确定其价值和敏感程度。
         2. 应明确个人信息的流动路径和流通渠道，评估其安全性和可信度。
         3. 应根据信息流动的路径和渠道，识别可能存在的威胁和漏洞，如数据传输中的安全漏洞、存储系统的安全性、第三方服务提供商的可信度等。
         4. 应评估境外接收方在个人信息保护方面的承诺和履行能力，包括其管理措施、技术措施、安全保障能力等。
         5. 应分析个人信息跨境处理活动可能涉及的国家安全和政治风险，评估其对国家安全和社会公共利益的影响。
         6. 宜采用定量和定性相结合的评估方法，利用风险评估矩阵、态势分析法（SWOT分析）等工具进行全面评估。
      2. 评估报告
         1. 个人信息处理者应对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估,并形成个人信息保护影响评估报告。
         2. 评估报告应保存3年及以上。
         3. 评估报告应包含但不限于以下内容：
  14. 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；
  15. 跨境处理个人信息的规模、范围、类型、敏感程度、频率；
  16. 个人信息跨境处理可能对个人信息权益带来的风险；
  17. 境外接收方承诺承担的责任义务、技术措施、保障能力等；
  18. 维护个人信息权益的渠道及潜存风险；
  19. 境外接收方所在国家或地区的相关法律法规、处理经验、监督机制等信息；
  20. 其他可能影响个人信息跨境处理安全的事项。

