CS 35. xxx
CCS Lxx

团　　体　　标　　准

T/ISC XXX—XXXX

未成年人个人信息合规审计标准

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国互联网协会　　发布

目　次

20xx-xx-xx 发布　　20xx-xx-xx 实施
x　x　x　x　x　发布

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这些专利的责任。

本文件由中国互联网协会归口。

本文件主要起草单位：

本文件主要起草人：

引　言

当前，互联网与经济社会深度融合，已成为未成年人了解世界、学习知识、休闲娱乐、交流交往的重要平台。然而，未成年人在心理与生理上尚未成熟，在自我防护、判断是非以及自我调控方面相较于成年人显得较为薄弱。对此，我国已经建立了一套较为完善的法律法规体系，包括《未成年人保护法》《网络安全法》《个人信息保护法》《儿童个人信息网络保护规定》《未成年人网络保护条例》等，旨在为未成年人个人信息提供全方位的法律保护。

本文件将落实法律法规的要求，提出未成年人个人信息合规审计标准，指导行业进行系统性的未成年人个人信息合规审计，细化并落实未成年人个人信息保护的义务和要求，助力企业开展未成年人个人信息合规审计工作。

未成年人个人信息合规审计标准

1 范围

本文件规定并提供了开展收集、存储、使用等未成年人个人信息处理活动应遵循的原则、安全要求以及合规审计要点。

本文件适用于指导未成年人个人信息处理者进行未成年人个人信息保护。

2 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（包括所有的修改版）适用于本文件。

GB/T 25069 信息安全技术术语

GB/T 35273 信息安全技术个人信息安全规范

3 术语和定义

GB/T 25069 和 GB/T 35273 界定的以及下列术语和定义适用于本文件。

3.1

未成年人 Minors

未满十八周岁的公民。

3.2

儿童 Children

不满十四周岁的未成年人。

3.3

未成年人个人信息 Personal Information of Minors

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未成年人身份或者反映特定未成年人活动情况的各种信息。

3.4

监护人 Guardian

对无民事行为能力人和限制民事行为能力人的人身、财产和其他一切合法权益负有监护和保护职责的人。

3.5

个人信息处理者 Personal Information Processor

有权决定个人信息处理目的、方式等的组织或个人。

3.6

未成年人个人信息处理者 Minors Personal Information Processor

有权决定未成年人个人信息处理目的、方式等的组织或个人。

4 审计方式

未成年人个人信息处理者应当自行或者委托专业机构对其处理未成年人个人信息遵守法律、行政法规的情况进行合规审计，并将审计情况及时报告网信等部门。

5 未成年人个人信息合规审计制度

5.1 未成年人个人信息合规审计基本要求

a） 法律法规及行业标准要求

个人信息处理者开展未成年人个人信息处理活动，除应满足《个人信息保护法》、《数据安全法》、《网络安全法》、《未成年人网络保护条例》以及《儿童个人信息网络保护规定》等法律规定外，还应遵循 GB/T 35273 信息安全技术 个人信息安全规范等相关规定。

b） 审计原则

未成年人个人信息保护合规审计应遵循合法性、独立性、客观性、全面性、公正性、保密性原则。

c） 专项要求

未成年人个人信息处理者宜对其开展的未成年人个人信息处理活动进行单独审计。

未成年人个人信息处理者也可以在一般个人信息保护合规审计中纳入未成年人个人信息保护审计内容，但应当具有相对的独立性。

d） 审计周期

未成年人个人信息处理者应当每年对其开展的未成年个人信息处理活动进行审计工作。

5.2 未成年人个人信息合规审计流程

未成年人个人信息保护合规审计通常包括审计准备、审计实施、审计报告、问题整改、归档管理等阶段。

a） 审计准备阶段

审计准备阶段包括建立审计组、开展审前调查、确定审计方式方法、编制和评审审计方案等。

b） 审计实施阶段

审计实施阶段包括发送审计通知、收集审计证据、采信审计证据、撰写审计底稿和确认审计发现等。

c） 审计报告阶段

审计实施阶段包括异议解决、撰写审计报告、交付审计报告等。

d） 问题整改阶段

审计人员应对审计中发现的不合规项进行跟踪，督促被审计方在规定期限内整改。必要时，审计人员可对整改措施的完成情况及有效性进行跟踪审计。

e） 归档管理阶段

未成年人个人信息处理者和第三方专业机构应妥善保管个人信息保护合规审计底稿、报告等档案资料。

5.3 未成年人个人信息合规审计证据

未成年人个人信息处理者应保证提供的审计证据真实、完整、有效，并满足以下要求：

a） 管理文件应经过正当的起草或批准程序并生效实施；

b） 协议文件应获得协议各方的有效同意并实际生效和执行；

c） 纸质或者电子记录的工作档案应能够反映真实情况；

d） 访问日志、存储日志、传输日志、删除日志等网络日志应是未经篡改的原始记录；

e） 网络安全等级保护、个人信息保护认证、数据安全管理认证等证明应在有效期内；

f） 个人信息处理相关检测报告应加盖测试机构公章并对内容真实性做出负责任承诺。

6 基本原则

未成年人个人信息处理者开展未成年人个人信息处理活动除应遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息外，还应遵循如下原则，具体包括：

a） 专项保护原则——对未成年人个人信息开展专项保护，包括专人负责、针对性的保护措施与保护规则等，将未成年人权益作为优先保护事项。

b） 主动保护原则——发生或者可能发生未成年人个人信息泄露、篡改、丢失的，未成年人个人信息处理者应主动采取包括停止传输、删除、屏蔽、断开链接等手段。

c） 便捷使用原则——应设立未成年人模式，便于家长履行监护职责，并建立便捷的投诉、举报渠道，及时受理处置涉未成年人投诉举报，维护未成年人合法权益。

d） 适龄原则——应细分未成年人模式，并根据其身心发展特点，评估产品类型、内容与功能等要素，为不同年龄段未成年人提供不同的信息和服务。

e） 多方协作原则——未成年人个人信息处理者应与监护人、相关组织、机构以及政府部门协作开展未成年人信息保护工作，实现未成年人保护社会共治。

7 未成年人个人信息的收集

7.1 未成年人个人信息处理者对未成年人个人信息的收集

未成年人个人信息处理者需严格遵守相关法律法规收集未成年人的个人信息。对未成年人个人信息处理者的要求包括：

a） 应有效识别儿童/未成年人用户；

b） 区分儿童或未成年人进行告知；

c） 区分儿童或未成年人取得同意；

d） 收集儿童/未成年人个人信息应严格遵循最小必要原则。

7.2 对未成年人个人信息收集的审查事项

a） 对未成年人用户有效识别的审查事项

未成年人个人信息处理者处理未成年人个人信息的，应对未成年人个人信息处理者是否识别用户为未成年人进行审查，审查未成年人个人信息处理者是否根据差异化功能场景提供有效的识别措施。未成年人个人信息处理者应在注册和/或登录阶段采取下列措施之一对未成年人进行识别：年龄段选择下拉菜单；输入出生日期；输入身份证号进行实名认证；进行人脸识别验证；其他可以有效识别未成年人的措施。

b） 对未成年人及其监护人告知的审查事项

处理未成年人个人信息的，宜制定专门的未成年人/儿童个人信息处理规则，并对未成年人个人信息处理者是否履行下列告知要求进行审查：

1） 应通过至少一种显著方式向未成年人及其监护人告知未成年人个人信息处理规则。根据业务需要，网络服务提供者还应就儿童个人信息处理规则进行单独告知，显著方式包括：单独的勾选框；单独弹窗提示；单独引导页面；语音播放；其他可以有效告知的措施。

2） 应使用清晰易懂的文字向未成年人及其监护人说明收集个人信息的具体目的和必要性。

3） 处理敏感个人信息的，应当向监护人告知处理敏感个人信息的必要性以及对未成年人权益的影响。

4） 应确保告知个人信息处理规则对残疾人无障碍，如提供易读的文本格式、提供语音提示功能、提供视觉辅助功能以及提供其他辅助功能。

c） 未成年人及其监护人同意的审查事项

未成年人个人信息处理者处理儿童个人信息的，应对其是否取得未成年人的父母或者其他监护人的单独同意进行审查，审查事项包括：

1） 应取得儿童监护人单独同意，不应一次性针对多项儿童个人信息或多种处理活动取得同意；

2） 取得儿童监护人单独同意时，处理个人信息的同意期限不应设置为“始终允许”或“永久”；

3） 不应以改善服务质量、提升用户体验以及研发新产品等为目的收集儿童个人信息。

d） 收集未成年人个人信息最小必要的审查事项

对未成年人个人信息处理者收集未成年人个人信息的最小必要审查事项包括：

1） 收集儿童的生物识别、身份相关等个人信息具有充分的必要性；

2） 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；

3) 对提供产品或服务所需的未成年人个人信息分为必要和非必要两类，并在处理规则中进行充分告知。

8 未成年人个人信息的使用

8.1 未成年人个人信息处理者对未成年人个人信息的使用

未成年人个人信息处理者需严格遵守相关法律法规处理未成年人的个人信息。对未成年人个人信息处理者的要求包括：

a） 应采取安全技术措施；

b） 应减少使用自动化决策处理未成年人个人信息；

c） 应进行权限管控及审批记录；

d） 应建立未成年人真实身份信息动态识别机制；

e) 应对识别为疑似未成年人的用户进行动态核验。

8.2 对未成年人个人信息使用的审查事项

a) 安全技术措施

未成年人个人信息处理者使用未成年人个人信息的，应对未成年人个人信息处理者是否采取加密、去标识化等安全技术措施进行审查，确保未成年人个人信息处理者在不借助额外信息的情况下，消除或者降低个人信息的可识别性。

b) 自动化决策

未成年人个人信息自动化决策处理的审查事项包括：

1) 除对未成年人身份进行动态核验及适龄化推送目的以外，原则上未成年人个人信息处理者应默认关闭使用群体画像并需经监护人同意再开启；

2) 使用自动化决策处理未成年人个人信息的应事前告知处理未成年人个人信息的种类、涉及的场景及可能带来的影响；

3) 不得通过自动化决策方式向未成年人进行商业营销。

c) 权限管控及审批记录

未成年人个人信息处理的权限管控及审批记录审查事项包括：

1) 针对未成年人个人信息的访问应制定严格信息访问权限，控制未成年人个人信息的内部访问范围。

2) 确有必要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。

d) 动态识别机制

未成年人个人信息处理者依法应对用户是否为未成年人进行动态识别的，具体审查事项包括：

1) 应建立相关管理制度及技术手段，根据用户使用习惯（登陆时间、使用时长）、发布内容等，依据具体制度与自动化决策对用户进行动态识别，尽到合理注意义务；

2) 对未成年人动态识别机制向未成年人及其监护人进行告知。

e) 动态核验机制

若用户被识别为疑似未成年人的，未成年人个人信息处理者应对该用户是否为未成年人进行动态核验，具体审查事项包括：

1) 未成年人个人信息处理者应根据差异化功能场景，提供不同的动态核验措施，具体核验措施包括但不限于：身份证认证、人脸识别、监护人认证以及符合法律、行政法规或者国家网信部门规定的其他验证方法。

***注：**监护人认证的具体措施包括但不限于，要求用户提供其监护人的联络方式，再通过短信、电话、邮箱等方式进行监护人身份鉴别；要求监护人拨打免费号码与经过相关知识培训的人员通话；要求监护人签署动态验证表格，并通过邮箱或电子扫描方式等邮寄；要求用户提供其与监护人手持身份证照片以证明其监护人已明确知晓未成年人个人信息处理规则并作出单独同意；要求用户提供其家庭户口本等信息以证明作出单独同意的个人为其合法的监护人。

2) 对未成年人动态核验机制向未成年人及其监护人进行告知。

9 未成年人个人信息转移

9.1 未成年人个人信息处理者对未成年人个人信息的转移

未成年人个人信息处理者需严格遵守相关法律法规转移未成年人的个人信息。对未成年人个人信息处理者的要求包括：

a) 应根据接收方进行告知；

b) 应根据自身的用户群体取得同意；

c) 应根据自身的用户群体自行或者委托第三方机构进行影响评估。

9.2 对未成年人个人信息转移的审查事项

a) 告知义务

应向未成年人告知接收方的名称或者姓名和联系方式；用户为儿童的，应同时向其监护人告知。

b) 同意义务

接收方变更原先处理目的、处理方式的，是否依照法律、行政法规有关规定重新取得个人同意；用户为儿童的，应同时取得监护人的同意。

c) 影响评估/安全评估

向第三方转移未成年人个人信息的，应当自行或者委托第三方机构进行影响评估/安全评估；向第三方转移儿童个人信息的，应当自行或者委托第三方机构进行影响评估/安全评估。

10 未成年人个人信息的存储

10.1 未成年人个人信息处理者对未成年人个人信息的存储

未成年人个人信息处理者需严格遵守相关法律法规存储未成年人的个人信息，应建立未成年人个人信息存储机制。

10.2 对未成年人个人信息存储的审查事项

a) 应明确评估具体存储期限，并将该存储期限向未成年人及其监护人进行告知。若存储期限评估确有困难，应在处理规则中明确存储期限为实现处理目的的最小必要期限，并在达成目的后立即删除。如存在法律行政法规规定的其他情形，可以延长未成年人个人信息的存储时间。

b) 应存储于中华人民共和国境内。

c) 应采取去标识化、加密存储等技术手段保证信息安全。

11 未成年人个人信息的删除

11.1 未成年人个人信息处理者对未成年人个人信息的删除

未成年人个人信息处理者需严格遵守相关法律法规删除未成年人的个人信息，应建立未成年人个人信息删除机制。

11.2 对未成年人个人信息删除的审查事项

a) 应在制度层面建立未成年人个人信息删除或匿名化机制；

b) 超出未成年人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，或者依法停止除存储和采取必要的安全保障措施之外的处理；

c) 未成年人个人信息处理目的已实现、无法实现或者为实现处理目的不再必要，应删除或匿名化处理个人信息，或者依法停止除存储和采取必要的安全保障措施之外的处理；

d) 个人撤回同意的，应对个人信息进行删除或匿名化处理，或者依法停止除存储和采取必要的安全保障措施之外的处理。

12 未成年人个人信息主体的权利

12.1 未成年人个人信息主体的权利

未成年人个人信息处理者需严格保障法律赋予未成年人的知情、查阅、更正、删除、撤回同意、注销账户、获取个人信息副本等个人信息主体权利，并便捷的支持未成年人或者其监护人行使。

12.2 对未成年人个人信息主体权利的审查事项

a) 应为未成年人及其监护人提供便捷的查阅、复制和删除等个人信息管理功能，不得限制未成年人或者其监护人的合理请求，或者设置不合理的条件；

b) 应保障未成年人及其监护人有权通过电话或在线平台等便捷方式行使权利，并指定专人及时处理；

c) 应在接到权利人申请后 15 个工作日内处理完成，并对处理过程以及处理结果进行完整记录；

d) 拒绝未成年人或其监护人权利请求的，应书面告知申请人并说明理由。

13 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者

若未成年人个人信息处理者属于提供重要互联网平台服务、用户数量巨大、业务类型复杂的，应当履行以下义务：

a） 按照国家规定建立健全未成年人个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对未成年人个人信息保护情况进行监督；

b） 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；

c） 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；

d） 定期发布个人信息保护社会责任报告，接受社会监督。

14 个人信息安全事件处置

14.1 个人信息安全事件处置基本要求

发生或者可能发生未成年人个人信息泄露、篡改、丢失的，未成年人个人信息处理者应当立即启动个人信息安全事件应急预案，采取补救措施，及时向网信等部门报告，并按照国家有关规定将事件情况以邮件、信函、电话、信息推送等方式告知受影响的未成年人及其监护人。

14.2 个人信息安全事件处置审查事项

发生或者可能发生未成年人个人信息泄露、篡改、丢失的，应当审查未成年人个人信息处理者是否遵循了下列未成年人个人信息安全事件处置的要求。

a) 主动通知

未成年人个人信息处理者发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，应及时将未成年人个人信息安全事件相关情况通过邮件、推送通知、公告等方式告知受影响的个人信息主体及其监护人，并向有关主管部门报告。

b) 防止扩散

未成年人个人信息处理者发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，应当及时提示，并采取停止传输等必要保护措施，防止信息扩散。

c) 主动报告

未成年人个人信息处理者通过未成年人发布的私密信息发现未成年人可能遭受侵害的，应当立即采取必要措施保存有关记录，并向公安机关报告。

15 监护人服务平台

15.1 监护人服务平台的基本要求

鼓励未成年人个人信息处理者根据差异化功能场景，设置监护人服务平台，协助监护人做好未成年人网络保护工作，维护未成年人合法权益。对监护人服务平台的要求包括：

a） 监护人可以通过监护人服务平台代为行使未成年人各项个人信息权利；

b） 监护人可以通过监护人服务平台代为行使的权利包括知情、查阅、更正、删除、撤回

同意、获取个人信息副本等。

15.2 对监护人服务平台的审查事项

若未成年人个人信息处理者设置监护人服务平台，应提供相应的支持和服务，并对监护人服务平台是否履行下列义务进行审查：

a) 监护人服务平台应具有独立页面（如网站、移动互联网应用程序、客户端软件等）向监护人提供产品或服务，可以设置便捷的交互式页面便于监护人代为行使知情、查阅、更正、删除、撤回同意、获取个人信息副本等权利；

b) 监护人服务平台收集个人信息，应具有独立的处理规则向监护人告知处理个人信息的目的、方式和范围等，并获得监护人的授权同意；

c) 监护人服务平台应保证处理个人信息的目的、方式、范围与告知的个人信息处理规则一致。