北京学而思教育科技有限公司
个人信息安全影响评估报告

2022 年 04 月 11 日

北京学而思教育科技有限公司

目录

1 项目概述

1.1 评估依据

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

1.2 评估价值

实施个人信息安全影响评估，能够有效加强对个人信息主体权益的保护，有利于组织对外展示其保护个人信息安全的努力，提升透明度，增进个人信息主体对其的信任。包括：

1) 在开展个人信息处理前，组织可通过影响评估，识别可能导致个人信息主体权益遭受损害的风险，并据此采用适当的个人信息安全控制措施。

2) 对于正在开展的个人信息处理，组织可通过影响评估，综合考虑内外部因素的变化情况，持续修正已采取的个人信息安全控制措施，确保对个人合法权益不利影响的风险处于总体可控的状态。

3) 个人信息安全影响评估及其形成的记录文档，可帮助组织在政府、相关机构或商业伙伴的调查、执法、合规性审计等中，证明其遵守了个人信息保护与数据安全等方面的法律、法规和标准的要求。

4）在发生个人信息安全事件时，个人信息安全影响评估及其形成的记录文档，可用于证明组织已经主动评估风险并采取一定的安全保护措施，有助于减轻、甚至免除组织相关责任和名誉损失。

5）组织可通过个人信息安全影响评估，加强对员工的个人信息安全教育。参与评估之中，员工能熟悉各种个人信息安全风险，增强处置风险的能力。

6）对合作伙伴，组织通过评估的实际行动表明其严肃对待个人信息安全保护，并引导其能够采取适当的安全控制措施，以达到同等或类似的安全保护水平。

1.3 评估责任主体

组织指定个人信息安全影响评估的责任部门或责任人员，由其负责个人信息安全影响评估工作流程的制定、实施、改进，并对个人信息安全影响评估工作结果的质量负责。该责任部门或人员具有独立性，不受到被评估方的影响。通常，组织内部牵头执行个人信息安全影响评估工作的部门为法务部门、合规部门或信息安全部门。

组织内的责任部门可根据部门的具体能力配备情况，选择自行开展个人信息安全影响评估工作，或聘请外部独立第三方来承担具体的个人信息安全影响评估工作。

对于具体的产品、服务或项目，由相应的产品、服务或项目负责人确保个人信息安全影响评估活动的开展和顺利进行，并给予相应支持。

当由组织自行进行个人信息安全影响评估时，主管监管部门和客户可要求独立审计来核证影响评估活动的合理性和完备性。同时，该组织允许主管监管部门对影响评估流程以及相关信息系统或程序进行取证。

1.4 评估流程

个人信息安全影响评估的基本原理如下图。

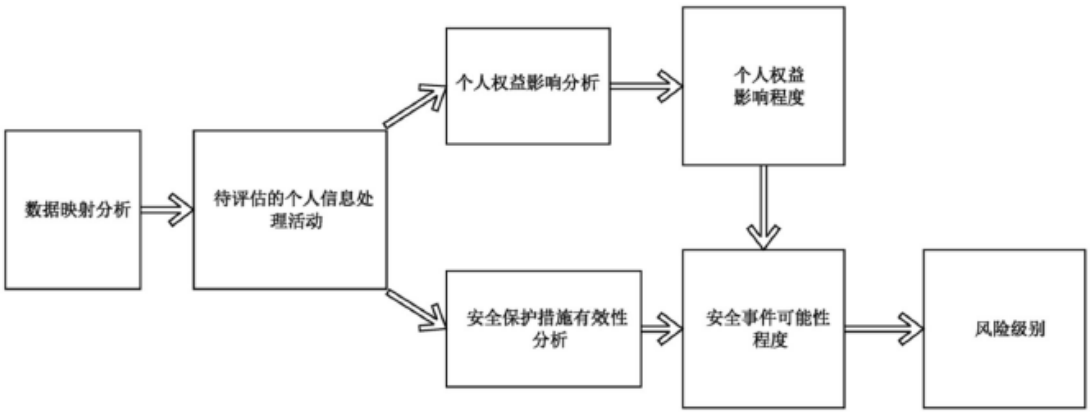

图 1　评估原理示意图

开展评估时，通过分析个人信息处理活动对个人信息主体的权益可能造成的影响及其程度，以及分析安全措施是否有效、是否会导致安全事件发生及其可能性，综合两方面结果得出个人信息处理活动的安全风险及风险等级，并提出相应的改进建议，形成评估报告。

2 评估实施

2.1 评估准备

2.1.1 评估团队

组织确认并任命负责进行个人信息安全影响评估的人员为许浩。此外，指定应用安全组负责人安亚龙负责签署评估报告。

2.1.2 评估计划

本次个人信息安全影响评估计划时间节点：2022 年 04 月 01 号—2022 年 04 月 11 号。

2.1.3 评估对象和范围

从以下三个方面描述评估的对象和范围：

1）系统基本信息，包括但不限于：

- 处理个人信息的目的和型；
- 对支撑当前或未来业务流程的信息系统的描述；
- 履行信息系统管理职责的部门或相关人员，以及其职责或履行水平，
- 关于个人信息处理方式、处理范围的说明、有权访问个人信息的角色等；

- 如预计委托第三方处理，或与第三方共享、转让信息系统的个人信息，说明上述第三方身份、第三方接人信息系统的情况等。

2）系统设计信息，包括但不限于：

- 功能（或逻辑）结构概览；
- 物理结构概览；
- 包含个人信息的信息系统数据库、表格和字段的清单和结构；
- 按组件和接口划分的数据流示意图；
- 个人信息生命周期的数据流示意图，例如个人信息的收集、存储、使用和共享等；
- 描述通知个人信息主体的时间节点以及取得个人信息主体同意的时间节点和工作流程图；
- 可对外传输个人信息的接口清单；
- 个人信息处理过程中的安全措施。

3）处理流程和程序信息，包括但不限于：

- 信息系统的身份与用户管理概念；
- 操作概念，包括信息系统或其中部分结构采用现场运行、外部托管，或云外包的方式；
- 支持概念，包括列示可访问个人信息的第三方范围、其所拥有的个人信息访问权限、其可访问个人信息的位置等；

- 记录概念，包括已登入信息的保存计划；
- 备份与恢复计划；
- 数据的保护与管理；
- 据保存与删除计划及存储介质的处置。

2.1.4 风险源识别

为进一步简化个人信息安全事件可能性的分析过程，将与个人信息安全事件可能性相关的要素归纳为以下四个方面：

1）网络环境和技术措施。评估时关注的要素包括但不限于：

- 处理个人信息的信息系统所处网络环境为内部网络还是互联网，不同的网络环境其面临的威胁源不同，连接互联网的信息系统面临的风险更高；
- 处理个人信息的信息系统与其他系统的交互方式，比如是否采用网络接口进行数据交互，是否嵌入可收集个人信息的第三方代码、插件等，通常情况下数据交互越多，需采取更加全面的安全措施防止信息泄露、窃取等风险；
- 个人信息处理过程中是否实施严格的身份鉴别、访问控制等措施；
- 是否在网络边界部署了边界防护设备，配置了严格的边界防护策略，实施了数据防泄露技术措施；

- 是否监测和记录网络运行状态，是否标记、分析个人信息在内部或与第三方交互时的状态，及时发现异常流量和违规使用情况；
- 是否采取了防范病毒和木马后门攻击、端口扫描、拒绝服务攻击等网络入侵行为的技术措施；
- 是否采用加密传输、加密存储等措施对个人敏感信息进行额外保护，
- 是否对个人信息收集、保存、传输、使用、共享等各阶段的个人信息处理活动进行审计，并对异常操作行为进行报警；
- 是否建立了完备的网络安全事件预警、应急处置、报告机制；
- 是否对信息系统进行定期安全检查、评估、渗透测试，并及时进行补丁更新和安全加固；
- 是否对数据存储介质加强安全管理，是否具备对数据进行备份和恢复的能力；
- 其他必要的网络安全技术保障措施。

2）个人信息处理流程。评估时关注的要素包括但不限于：

- 个人敏感信息的判定是否准确；
- 收集个人信息的目的是否正当、合法；
- 从第三方获得的数据是否得到正式的处理授权；

- 告知方式和告知的内容是否友好可达，是否所有的处理活动都征得了用户同意；
- 是否定义了个人信息最小元素集，是否超范围收集了个人信息；
- 变更个人信息使用目的是否对个人信息主体产生影响；
- 是否提供便捷有效的个体参与的机制，包括查询、更正、删除、撤回同意、注销账号等；
- 接收个人信息的第三方是否会变更目的使用个人信息；
- 个人信息的保存时间是否最小化，超出期限的删除等机制是否合理；
- 是否对用户画像机制进行限制，避免精确定位到特定个人；
- 是否为个性化展示提供用户可控制、可退出或关闭的机制；
- 匿名化机制是否有效，去标识化后的个人信息是否能够被关联分析等，导致可重新识别个人信息主体身份；
- 是否提供及时有效的安全事件通知机制和应急处置机制；
- 是否提供有效的投诉和维权渠道等；
- 是否未经用户同意向第三方共享、转让个人信息；
- 是否散播不准确的数据或不完整的误导性数据；
- 是否诱导或强迫个人提供过多个人信息；

- 是否过多地追踪或监视个人行为；
- 是否无根据地限制个人控制其个人信息的行为等；
- 其他个人信息处理流程的规范性。

3）参与人员与第三方。评估时关注的要素包括但不限于：

- 是否任命个人信息保护负责人或个人信息保护工作机构，个人信息保护负责人是否由具有相关管理工作经历和个人信息保护专业知识的人员担任；
- 是否依据业务安全需求，制定并执行个人信息安全管理的方针和策略；
- 是否制定涉及个人信息处理各环节的安全管理制度，并提出具体的安全管理要求；
- 是否与从事个人信息处理岗位上的相关人员签署保密协议，并对大量接触个人敏感信息的人员进行背景审查；
- 是否明确内部涉及个人信息处理不同岗位的安全职责，并建立发生安全事件的处罚、问责机制；
- 是否对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，并确保相关人员熟练掌握隐私政策和相关规程；
- 是否明确可能访问个人信息的外部服务人员需遵守的个人信息安全要求，并进行监督；

- 是否与第三方签署有约束力的合同等文件，约定个人信息传输至第三方后的处理目的、方式、数据留存期限、超出期限后的处理方式；
- 是否对第三方处理个人信息的行为进行定期检查、审计，确保其严格执行合同等约定；
- 其他方面的必要措施。

4）业务特点和规模及安全态势。关注的要素包括但不限于：

- 业务对个人信息处理的依赖性；
- 业务处理或可能处理个人信息的数量、频率、用户规模、用户峰值等；
- 是否曾经发生过个人信息泄露、篡改、毁损、丢失等事件；
- 个人信息保护相关执法监管动态；
- 近期内遭受网络攻击或发生安全事件的情况；
- 近期收到过或公开发布的安全相关的警示信息。

2.1.5 个人权益影响分析

1）个人权益维度

个人权益影响分析指分析特定的个人信息处理活动是否会对个人信息主体合法权益产生影响，以及可能产生何种影响。个人权益影响概括可分为“限制个人自主决定权”“引发差别性待遇”“个人名誉受损或遭受精神压力”“人身财产受损”四个维度：

- 限制个人自主决定权，例如被强迫执行不愿执行的操作、缺乏相关知识或缺少相关渠道更正个人信息、无法选择拒绝个性化广告的推送、被蓄意推送影响个人价值观判断的资讯等；
- 引发差别性待遇，例如因疾病、婚史、学籍等信息泄露造成的针对个人权利的歧视，因个人消费习惯等信息的滥用而对个人公平交易权造成损害等；
- 个人名誉受损或遭受精神压力，例如被他人冒用身份、公开不愿为人知的习惯、经历等，被频繁骚扰、监视追踪等；
- 人身财产受损，例如引发人身伤害、资金账户被盗、遭受诈骗、勒索等。

2）个人权益影响分析过程

组织可根据数据映射分析结果及确定需要评估的个人信息处理活动，结合相关法律、法规、标准的要求或组织自定义的个人信息安全目标，分析个人信息处理活动全生命周期或特定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，以审视是否存在侵害个人信息主体权益的风险。

个人权益影响分析过程一般包含对个人信息敏感程度分析、个人信息处理活动特点分析、个人信息处理活动问题分析以及影响程度分析四个阶段：

- 在个人信息敏感程度分析阶段，组织可参照国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息的敏感程度对个人权益可能产生的影响，例如健康生理信息的泄露、滥用等可能会对个人生理、心理产生较严重的影响；
- 在个人信息处理活动特点分析阶段，组织可参照与国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息处理活动是否涉及限制个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、人身财产受损等，例如公开披露个人经历的行为可能会对个人声誉产生影响；
- 在个人信息处理活动问题分析阶段，组织可参照与国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息处理活动可能存在的弱点、差距和问题，其中对个人信息流程规范性的分析结果可以支撑该阶段的分析过程，对问题严重程度的分析有助于分析个人权益的影响程度；
- 在个人权益影响程度分析阶段，组织可结合前几个阶段的分析结果，综合分析个人信息处理活动对个人权益可能造成的影响，及其严重程度。

2.2 评估原则

2.2.1 标准性原则

风险评估工作的指导性原则，指按照 GB/T 20984-2007 中规定的评估流程实施，对各个阶段的工作进行评估。

2.2.2 可控性原则

在评估过程中，应保证参与评估的人员、使用的技术和工具、评估过程都是可控的。

2.2.3 完备性原则

严格按照被评估方提供的评估范围进行全面的评估。

2.2.4 最小影响原则

从项目管理层面和工具技术层面，将评估工作对业务相关网络、系统正常运行的可能影响降低到最低限度，以免对被评估网络上的业务运行产生显著影响。

2.2.5 保密原则

评估方应与被评估方的负责人签署相关的保密协议，以保障被评估方的利益。

2.3 数据映射分析

针对个人信息处理过程进行全面的调研后，形成清晰的数据清单及数据映射图表。

数据映射分析阶段需结合个人信息处理的具体场景。调研内容包括个人信息收集、存储、使用、转让、共享、删除等环节涉及的个人信息类型、处理目的、具体实现方式等，以及个人信息处理过程涉及的资源和相关方。调研过程中尽可能考虑已下线系统、系统数据合并、企业收购、并购及全球化扩张等情况。

梳理数据映射分析的结果时，根据个人信息的类型、敏感程度、收集场景、处理方式、涉及相关方等要素，对个人信息处理活动进行分类，并描述每类个人信息处理活动的具体情形，便于后续分类进行影响分析和风险评价。

2.4 安全事件可能性等级判定准则

可能性描述	可能性等级
采取的措施严重不足，个人信息处理行为极不规范，安全事件的发生几乎不可避免	很高
采取的措施存在不足，个人信息处理行为不规范，安全事件曾经发生过或已经在类似场景下被证实发生过	高
采取了一定的措施，个人信息处理行为遵循了基本的规范性原则，安全事件在同行业、领域被证实发生过	中
采取了较有效的措施，个人信息处理行为遵循了规范性最佳实践，安全事件还未被证实发生过	低

2.5 可能性判定表

可能性描述	可能性等级
网络环境与互联网及大量信息系统有交互现象，基本上未采取安全措施保护个人信息安全	很高
该个人信息处理行为为常态、不间断的业务行为，该行为已经对个人主体的权益造成了影响，或收到了大量相关的投诉，并引起了社会关注	
任意人员可接触到个人信息，对第三方处理个人信息的范围无任何限制，或已出现第三方滥用个人信息的情形	
威胁引发的相关安全事件已经被本组织发现，或已收到监管部门发出的相关风险警报	
网络环境与互联网及其他信息系统有较多交互现象，采取的安全措施不够全面	高
该个人信息处理行为为常态、不间断的业务行为，个人信息处理行为不规范，且收到了相关的投诉	
对处理个人信息相关人员的管理松散，管理制度无落实的记录，未对第三方处理个人信息的范围提出相关要求	
威胁引发的相关安全事件曾经在组织内部发生过，或已在合作方中发生，或收到过权威组织发出的相关风险预警信息，或处理个人信息的规模超过 1 000 万人	
网络环境与互联网及其他信息系统有交互现象，采取了一定的安全措施	中
该个人信息处理行为为常态业务行为，个人信息处理行为规范性欠缺，且，合作伙伴或同领域其他组织收到过相关的投诉	
有相关的管理制度，对人员提出了管理要求，对第三方处理个人信息的范围提出限制条件，但相应的管理和监督效果不明	
威胁引发的相关安全事件已经被同领域其他组织发现，或在专业组织相关报告中被证实已出现，或处理个人信息的规模超过 100 万人	
网络环境比较独立，交互少，或采取了有效的措施保护个人信息安全	低
该个人信息处理行为非常态业务行为，个人信息处理行为符合规范，几乎没有出现关于该行为的投诉	
有完善的管理机制，对人员的管理和审核比较严格，与第三方合作时提出有效的约束条件并进行监督	
威胁引发的安全事件仅被专业组织所预测	

2.6 个人权益影响程度判定准则

影响描述	影响程度
个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响，如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等	严重
个人信息主体可能遭受重大影响，个人信息主体克服难度高，消除影响代价大，如遭受诈骗、资金被盗用、被银行列人黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等	高
个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的难度，如付出额外成本、无法使用所提供的服务、造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等	中
个人信息主体可能会遭受一定程度的困扰，但尚可以克服，如被占用额外的时间、被打扰、产生厌烦和恼怒情绪等	低

2.7 影响程度判定表

影响类别	影响描述	影响程度
限制个人自主决定权	例如个人人身自由受限	严重
	例如被强迫执行违反个人意愿的操作、被蓄意推送消息影响个人价值观判断、可能引发个人人身自由受限	高
	例如缺乏相关知识或缺少相关渠道更正个人信息、为使用应提供的产品或服务而付出额外的成本等	中
	例如被占用额外的时间	低
引发差别性待遇	例如因信息泄露造成歧视性对待以致被用人单位解除劳动关系	严重
	例如造成对个人合法权利的歧视性待遇、造成对个人公平交易权的损害（无法全部或部分使用所提供的产品或服务）	高
	例如造成误解、为使用所提供的产品或服务而需付出额外的成本（包含资金成本、时间成本等）	中
	例如耗费额外的时间获取公平的服务或取得相应的资格等	低

个人名誉受损和遭受精神压力	例如名誉受损以致长期无法获得财务收人、导致长期的心理或生理疾病以至于失去工作能力、导致死亡等	严重
	例如名誉受损以致被用人单位解除劳动关系、导致心理或生理疾病以致健康遭受不可逆的损害等	高
	例如造成误解、名誉受损（通过澄清可全部或部分恢复）、产生害怕和紧张的情绪、导致心理或生理疾病（通过治疗或纠正措施，短期可痊愈）等	中
	例如被频繁打扰、产生厌烦和恼怒情绪等	低
人身财产受损	例如造成重伤、遭受无法承担的债务等	严重
	例如造成轻伤、遭受金融诈骗、资金被盗用、征信信息受损等	高
	例如造成轻微伤、社会信用受损，为获取金融产品或服务，或挽回损失需付出额外的成本等	中
	例如因个人信息更正而需执行额外的流程（或提供额外的证明性材料）等	低

2.8 风险等级判定表

风险等级		可能性级别			
		低	中	高	很高
影响级别	严重	中	高	严重	严重
	高	中	中	高	严重
	中	低	中	中	高
	低	低	低	中	中

3 个人信息处理活动对个人信息主体合法权益的影响

个人信息处理活动对个人信息主体合法权益的影响，内容见下文：

1. 个人信息收集环节是否遵循目的明确、选择同意、最小必要等原则；
2. 个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等；
3. 个人信息安全措施的有效性；
4. 匿名化或去标识化处理后的数据集重新识别出个人信息主体或与其他数据集汇聚后重新识别出个人信息主体的风险；
5. 共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响；
6. 发生安全事件时，对个人信息主体合法权益可能产生的不利影响。

3.1 个人信息收集

序号	收集个人信息	收集目的	是否必须收集	收集方式	备注
1.	手机号	用于用户登录、短信通知、课程预定/购买服务	是	用户提供	
2.	姓名	用于课程购买服务使用第三方支付的身份验证	否	用户提供	
3.	邮箱	用于课程购买服务	否	用户提供	
4.	用户名	用于用户登录	否	用户提供	
5.	密码	用于用户登录	否	用户提供	
6.	头像	用于用户个人中心、配送/邮寄服务及个性化推荐	否	用户提供	
7.	地区	用于配送/邮寄服务	否	用户提供	
8.	详细地址	用于配送/邮寄服务	否	用户提供	
9.	昵称	用于配送/邮寄服务	否	用户提供	
10.	微信账号	用于用户个人中心	否	用户提供	
11.	学校信息	用于用户个人中心	否	用户提供	
12.	入学年份/年级	用于完善个人资料	否	用户提供	
13.	课中视频/录像信息	用于提供课程产品预订/购买服务	否	用户提供	
14.	评价和发布内容	用于提供相关可成功推荐	否	用户提供	
15.	客服服务相关的通信记录	主动对产品/服务进行评价或发布评论内容	否	用户提供	
16.	支付和订单信息	便于客服查看、解答疑问或协助处理请求	否	用户提供	
17.	设备型号	用于完成语音测评并得到测评结果	否	用户提供	
18.	操作系统	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	
19.	IMEI	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	
20.	Android ID	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	
21.	OAID	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	
22.	IDFA	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	

23.	IDFV	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	
24.	WIFI 信息	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	
25.	MAC 地址	用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	
26.	IMSI	用于高德导航	否	经用户同意相关权限后采集	
27.	位置信息	用于高德导航	否	经用户同意相关权限后采集	
28.	运营商信息	用于查看对应城市的服务推荐内容	否	经用户同意相关权限后采集	
29.		用于安全风控、问题定位、提升服务稳定性	否	经用户同意相关权限后采集	

3.2 个人信息处理对可能造成的不利影响

序号	个人信息处理活动	限制个人自主决定权	引发差别性待遇	个人名誉受损或遭受精神压力	人身财产受损	备注
1.	共享收件地址给第三方物流	无不利影响	无不利影响	无不利影响	无不利影响	
2.	个性化内容推荐	无不利影响	无不利影响	无不利影响	无不利影响	
3.						
4.						
5.						
6.						
7.						

3.3 个人信息安全措施有效性

序号	收集个人信息	所采取的安全措施	安全措施是否有效	备注
1.	手机号	数据加密存储和传输，前端脱敏展示	此安全措施能保证个人信息不被泄露	
2.	邮箱	数据加密存储和传输，前端脱敏展示	此安全措施能保证个人信息不被泄露	
3.	用户名	数据加密存储和传输	此安全措施能保证个人信息不被泄露	
4.	密码	数据采用多次加盐哈希存储，并使用AES256算法传输	此安全措施能保证个人信息不被泄露	
5.	头像	文件服务器安全防护	此安全措施能保证个人信息不被泄露	
6.	地区	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
7.	详细地址	数据加密存储和传输，前端部分脱敏展示	此安全措施能保证个人信息不被泄露	
8.	昵称	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
9.	微信账号	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
10.	学校信息	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
11.	入学年份/年级	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
12.	课中视频/录像信息	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
13.	评价和发布内容	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
14.	客服服务相关的通信记录	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
15.	支付和订单信息	数据加密存储和传输	此安全措施能保证个人信息不被泄露	
16.	设备型号	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
17.	操作系统	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
18.	IMEI	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
19.	Android ID	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
20.	OAID	数据库服务器安全防	此安全措施能保证个	

		护	人信息不被泄露	
21.	IDFA	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
22.	IDFV	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
23.	WIFI 信息	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
24.	MAC 地址	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
25.	IMSI	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	
26.	运营商信息	数据库服务器安全防护	此安全措施能保证个人信息不被泄露	

3.4 个人信息匿名化和去标识化效果评估

序号	收集个人信息	是否匿名化	是否去标识化	数据集是否可重新识别个人信息主体	是否可与其他数据集汇聚后重新识别出个人信息主体	存在风险	备注
1.	手机号	是	否	否	否	低风险	
2.	身份证	是	否	否	否	低风险	
3.	邮箱	是	否	否	否	低风险	
4.	用户名	是	否	否	否	低风险	
5.	密码	是	否	否	否	低风险	
6.	头像	是	否	否	否	低风险	
7.	地区	是	否	否	否	低风险	
8.	详细地址	是	否	否	否	低风险	
9.	昵称	是	否	否	否	低风险	
10.	微信账号	是	否	否	否	低风险	
11.	学校信息	是	否	否	否	低风险	
12.	入学年份/年级	是	否	否	否	低风险	
13.	课中视频/录像信息	是	否	否	否	低风险	
14.	评价和发布内容	是	否	否	否	低风险	
15.	客服服务相关的通信记录	是	否	否	否	低风险	
16.	支付和订单信息	是	否	否	否	低风险	
17.	设备型号	是	否	否	否	低风险	
18.	操作系统	是	否	否	否	低风险	
19.	IMEI	是	否	否	否	低风险	
20.	Android ID	是	否	否	否	低风险	
21.	OAID	是	否	否	否	低风险	

22.	IDFA	是	否	否	否	低风险	
23.	IDFV	是	否	否	否	低风险	
24.	WIFI 信息	是	否	否	否	低风险	
25.	MAC 地址	是	否	否	否	低风险	
26.	IMSI	是	否	否	否	低风险	
27.	运营商信息	是	否	否	否	低风险	

3.5 共享、转让、公开披露个人信息对个人信息的不利影响；

序号	收集个人信息	是否为敏感信息	是否征得客户同意	个人信息是否做加密处理	是否进行过去标识化处理	是否发生过安全事件（补救措施）	第三方响应请求范围	备注
1.	手机号	是	是	是	否	未发生过	课程服务咨询、购买，及图书、教材、讲义的物流寄送	
2.	邮箱	否	是	是	否	未发生过	未共享至第三方	
3.	用户名	否	是	是	否	未发生过	未共享至第三方	
4.	密码	是	是	是	否	未发生过	未共享至第三方	
5.	头像	否	是	否	否	未发生过	课程服务咨询、购买	
6.	地区	否	是	否	否	未发生过	课程服务咨询、购买	
7.	详细地址	是	是	是	否	未发生过	课程服务咨询、购买，及图书、教材、讲义的物流寄送	
8.	昵称	否	是	否	否	未发生过	课程服务咨询、购买	
9.	微信账号	否	是	否	否	未发生过	未共享至第三方	
10.	学校信息	否	是	否	否	未发生过	未共享至第三方	
11.	入学年份/年级	否	是	否	否	未发生过	课程服务咨询、购买	
12.	课中视频/录像信息	否	是	否	否	未发生过	未共享至第三方	
13.	评价和发布内容	否	是	否	否	未发生过	未共享至第三方	
14.	客服服务相关的通信记录	否	是	否	否	未发生过	未共享至第三方	

15.	支付和订单信息	否	是	是	否	未发生过	未共享至第三方	
16.	设备型号	否	是	否	否	未发生过	未共享至第三方	
17.	操作系统	否	是	否	否	未发生过	未共享至第三方	
18.	IMEI	否	是	否	否	未发生过	未共享至第三方	
19.	Android ID	否	是	否	否	未发生过	未共享至第三方	
20.	OAID	否	是	否	否	未发生过	未共享至第三方	
21.	IDFA	否	是	否	否	未发生过	未共享至第三方	
22.	IDFV	否	是	否	否	未发生过	未共享至第三方	
23.	WIFI信息	否	是	否	否	未发生过	未共享至第三方	
24.	MAC地址	否	是	否	否	未发生过	未共享至第三方	
25.	IMSI	否	是	否	否	未发生过	未共享至第三方	
26.	运营商信息	否	是	否	否	未发生过	未共享至第三方	

3.6 发生安全事件可能产生的不利影响；

序号	可能发生的安全事件	存在影响	安全事件发生的可能性	备注
1.	数据泄露	客户数据泄露可能会为用户带来电话骚扰，或者名誉受到损失等	低	
2.				
3.				
4.				
5.				
6.				
7.				

4 评估实施

4.1 个人信息映射表

个人信息处理活动	个人信息主体	个人信息的类型	收集/使用个人信息的原因	个人信息控制者	个人信息处理者	是否涉及跨境转移	是否涉及第三方共享
共享收件地址给第三方物流	考研帮用户	姓名、性别、详细地址、手机号、地区、昵称	商品兑换或课程购买后图书、教材、讲义的物流寄送服务	学而思、第三方物流公司	无	无	对外共享姓名、性别、详细地址、手机号、地区、昵称

4.2 个人信息生命周期安全管理

序号	个人信息的类型	收集来源	收集方式	存储方式（加密措施）	传输方式（加密措施）	存储期限	删除或匿名化方式
1.	手机号	用户中心SDK	用户提供	AES256	AES256	客户注销后删除数据	删除
2.	身份证	用户中心SDK	用户提供	AES128	AES256	客户注销后删除数据	删除
3.	姓名	用户中心SDK	用户提供	AES128	AES256	客户注销后删除数据	删除
4.	银行卡	用户中心SDK	用户提供	AES128	AES256	客户注销后删除数据	删除
5.	邮箱	用户中心SDK	用户提供	AES128	AES256	客户注销后删除数据	删除
6.	用户名	用户中心SDK	用户提供	AES128	AES256	客户注销后删除数据	删除
7.	密码	用户	用户	加盐多次哈希	AES256	客户注销后	删除

序号	个人信息的类型	收集来源	收集方式	存储方式（加密措施）	传输方式（加密措施）	存储期限	删除或匿名化方式
		中心SDK	提供			删除数据	
8.	性别	用户中心SDK	用户提供	无	无	客户注销后删除数据	删除
9.	头像	用户中心SDK	用户提供	无	无	客户注销后删除数据	删除
10.	生日	用户中心SDK	用户提供	AES128	AES256	客户注销后删除数据	删除
11.	地区	用户中心SDK	用户提供	无	无	客户注销后删除数据	删除
12.	详细地址	用户中心SDK	用户提供	AES128	AES256	客户注销后删除数据	删除
13.	邮编	用户中心SDK	用户提供	无	无	客户注销后删除数据	删除
14.	昵称	用户中心SDK	用户提供	无	无	客户注销后删除数据	删除
15.	英文名	用户中心SDK	用户提供	无	无	客户注销后删除数据	删除
16.	微信账号	用户提供的微信登录	用户提供	无	无	客户注销后删除数据	删除
17.	学校信息	用户提供的个人资料	用户提供	无	无	客户注销后删除数据	删除
18.	入学年份/年级	用户中心SDK	用户提供	无	无	客户注销后删除数据	删除
19.	校内成绩与作	用户提供	用户提供	无	无	客户注销后删除数据	删除

序号	个人信息的类型	收集来源	收集方式	存储方式（加密措施）	传输方式（加密措施）	存储期限	删除或匿名化方式
	业	的验证信息					
20.	课中视频/录像信息	用户课程学习操作	用户提供	无	无	客户注销后删除数据	删除
21.	浏览和搜索记录	用户的应用内访问和搜索操作	用户提供	无	无	客户注销后删除数据	删除
22.	评价和发布内容	用户在应用内作出的评价和发布的内容	用户提供	无	无	客户注销后删除数据	删除
23.	客服服务相关的通信记录	用户与客服联系时的记录	用户提供	无	无	客户注销后删除数据	删除
24.	支付和订单信息	用户的支付和课程购买操作	用户提供	AES128	AES256	客户注销后删除数据	删除
25.	语音测评的音频	用户使用语音测评功能	用户提供	无	无	客户注销后删除数据	删除
26.	设备型	用户	经用	无	无	客户注销后	删除

序号	个人信息的类型	收集来源	收集方式	存储方式（加密措施）	传输方式（加密措施）	存储期限	删除或匿名化方式
	号	中心SDK	户同意相关权限后采集			删除数据	
27.	操作系统	用户中心SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
28.	IMEI	用户中心SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
29.	Android ID	用户中心SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
30.	OAID	用户中心SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
31.	IDFA	用户中心SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
32.	IDFV	用户中心SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除

序号	个人信息的类型	收集来源	收集方式	存储方式（加密措施）	传输方式（加密措施）	存储期限	删除或匿名化方式
33.	WIFI 信息	用户中心 SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
34.	MAC 地址	用户中心 SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
35.	IMSI	用户中心 SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
36.	位置信息	用户中心 SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除
37.	运营商信息	用户中心 SDK	经用户同意相关权限后采集	无	无	客户注销后删除数据	删除

4.3 安全事件可能性分析

个人信息处理活动	涉及的个人敏感信息	风险源维度	个人信息处理活动存在的问题	个人权益影响	安全事件发生可能性
共享收件地址给第三方物流	敏感	网络环境和技术措施	无	无	无
		个人信息处理流程	无	无	无
		参与人员与第三方	无	无	无
		业务特点和规模及安全态势	无	无	无
个性化课程推荐	敏感	网络环境和技术措施	无	无	无
		个人信息处理流程	没有提供定向推送关闭选项	影响个人自主决定权	低
		参与人员与第三方	无	无	无
		业务特点和规模及安全态势	无	无	无

4.4 安全风险评估及整改措施表

个人信息处理活动	风险源维度	个人信息处理活动存在的问题	安全事件发生可能性等级	个人权益产生影响	影响程度	风险等级	相关责任方与风险处置建议	整改效果验证及归档情况
共享收件地址给第三方物流	网络环境和技术措施	无	无	限制个人自主决定权	无	无	无	无
		无	无	引发差别性待遇	无	无	无	无
		无	无	个人名誉受损或遭受精神压力	无	无	无	无

	无	无	人身财产受损	无	无	无	无
个人信息处理流程	无	无	限制个人自主决定权	无	无	无	无
	无	无	引发差别性待遇	无	无	无	无
	无	无	个人名誉受损或遭受精神压力	无	无	无	无
	无	无	人身财产受损	无	无	无	无
参与人员与第三方	无	无	限制个人自主决定权	无	无	无	无
	无	无	引发差别性待遇	无	无	无	无
	无	无	个人名誉受损或遭受精神压力	无	无	无	无
	无	无	人身财产受损	无	无	无	无
业务特点和规模及安全	无	无	限制个人自主决定权	无	无	无	无
	无	无	引发差别性待遇	无	无	无	无

		无	无	个人名誉受损或遭受精神压力	无	无	无	无
		无	无	人身财产受损	无	无	无	无
个性化课程推荐	网络环境和技术措施	无	无	限制个人自主决定权	无	无	无	无
		无	无	引发差别性待遇	无	无	无	无
		无	无	个人名誉受损或遭受精神压力	无	无	无	无
		无	无	人身财产受损	无	无	无	无
	个人信息处理流程	无	无	限制个人自主决定权	无	无	无	无
		无	无	引发差别性待遇	无	无	无	无
		无	无	个人名誉受损或遭受精神压力	无	无	无	无
		无	无	人身财产受损	无	无	无	无
	参与人员与第三方	无	无	限制个人自主决定权	无	无	无	无

		无	无	引发差别性待遇	无	无	无	无
		无	无	个人名誉受损或遭受精神压力	无	无	无	无
		无	无	人身财产受损	无	无	无	无
	业务特点和规模及安全	无	无	限制个人自主决定权	无	无	无	无
		无	无	引发差别性待遇	无	无	无	无
		无	无	个人名誉受损或遭受精神压力	无	无	无	无
		无	无	人身财产受损	无	无	无	无