YOUR logo

报告编号: 165302-207692-794599

欢乐科技有限公司

个人信息保护影响自评估报告

评估单位：欢乐科技有限公司

评估对象：客服系统

评估时间：2022年5月20日

评估对象基本信息表

评估对象基本信息表				
单位名称	欢乐科技有限公司			
被评估对象名称	客服系统			
评估的场景	☑ 产品或服务的年度整体评估 ☐ 新产品或新服务(不限技术平台)设计阶段评估 ☐ 新产品或新服务(不限技术平台)上线初次评估 ☐ 法律法规、政策、标准等出现重大变化时重新评估 ☐ 业务模式、互联网安全环境、外部环境等发生重大变化的重新评估 ☐ 发生重大个人信息安全事件后重新评估 ☑ 发生收购、兼并、重组等情形开展评估 ☑ 处理敏感个人信息 ☑ 利用个人信息进行自动化决策 ☑ 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 ☑ 其他对个人权益有重大影响的个人信息处理活动			
被评估对象业务信息	12			
影响评估 审核批准	编制人		编制日期	2022年5月20日
	审核人		编制日期	2022年5月20日
	批准人		编制日期	2022年5月20日

声明

欢乐科技有限公司（以下简称本公司）遵循《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等法律、法规和其他规范性文件，依据《GB/T 39332-2020 信息安全技术个人信息安全影响评估指南》（以下简称《评估指南》）对其欢乐科技有限公司对象进行个人信息保护影响评估，出具本评估报告，并申明如下：

一、本公司《欢乐科技有限公司 报告》出具日以前已经发生或者存在的事实，严格履行了法定职责，进行了充分的核查验证，保证本评估报告所认定的事实真实、准确、完整，所发表的结论性意见合法、准确，不存在虚假记载、误导性陈述或者重大遗漏，并承担相应法律责任。

二、本公司及具体经办人仅就与本公司个人信息处理活动是否对其个人信息主体合法权益造成损害发表意见。在本评估报告中对有关数据接收方及其所在国家或区域的政治法律环境报告中某些数据和结论的引述，并不意味着本公司对这些数据和结论的真实性及准确性做出任何明示或默示保证。

三、本评估报告中，本公司及具体经办人认定某些事件是否合法有效是以该等事件所发生时应当适用的法律、法规、规章及规范性文件为依据。

四、本评估报告的出具已经得本公司如下保证:
（一）本公司已经提供了出具本评估报告所需要的原始书面材料、副本材料、复印材料、确认函或证明。
（二）本公司提供的文件和材料是真实、准确、完整和有效的，并无隐瞒、虚假和重大遗漏之处，文件材料为副本或复印件的，其与原件一致和相符。

五、对于本评估报告至关重要而又无法得到独立证据支持的事实，本公司依据有关政府部门或其他有关单位等出具的证明文件出具评估报告。

六、本公司同意将本评估报告作为本次个人信息安全影响评估所必备的文件依据，随同其他材料一同备案/上报，并愿意承担相应的法律责任。

七、本评估报告仅供本公司为本次个人信息和重要数据安全出境之目的使用，非经本公司书面同意，不得用作任何其他目的。

八、基于上述，本公司及具体经办人根据有关法律、法规、规章和其他有关规定，出具评估报。本报告中给出的评估结论仅对被评估对象当时的状态有效。当评估工作完成后，由于被评估对象发生变更而涉及到的系统构成组件（或子系统）都应重新进行影响评估，本报告不再适用。

九、在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

单位名称： 欢乐科技有限公司

2022年5月20日

评估工作概述

评估背景及目标

为落实评估义务，保障个人信息主体权益，加强组织个人信息保护合规工作，故进行本次个人信息保护影响自评估工作。

参考依据

本次个人信息安全影响评估主要依据以下法律法规及标准实施。

- 《GB/T 39335-2020信息安全技术个人信息安全影响评估指南》

个人信息保护影响评估参考方法

评估个人信息主体权益影响程度

评估过程中，可先分析个人信息处理活动对某一个个人信息主体造成的影响程度，再根据处理活动的规模、特点、外部环境、个人信息去标识化、群体性特征等要素修正影响等级。比如，个人信息处理活动涉及典型的个人敏感信息，如健康状况等，且达到一定的数量（如 50万人），则影响程度可上升一个级别;如果受影响个人信息主体群体抗财务风险能力差、心理承受能力差等情形，如未成年人、学生、老年人等，则影响程度可上升一个级别;如果个人信息经去标识化后已确认降低敏感程度的，影响程度可降低一个级别。在进行修正时需要具体说明修正的理由，必要时可咨询外部专业组织，保证修正过程的合理性。

此外，从组织实践角度出发，可以进一步将个人信息主体权益的影响映射到对组织的影响，以促进组织进一步认识到其中的风险。比如，可根据个人权益受损对组织付出的成本进行评价。成本一般包括:违规成本（如监管处罚、诉讼费用、整改费用等）、直接的业务损失（如流失客户减少了业务收入等）、名誉损失（如品牌形象受损、客户信任受损等）、内部企业文化损失（如企业执行力受损、价值观冲突引起员工积极性下降等）等，以上方面还可以进行初步的半定量或定量分析（比如处罚的案例与罚金等），以促进组织充分重视个人信息保护工作，积极改进，降低个人信息处理过程对个人权益的影响。

个人权益影响程度评价可采用定性.半定量和定量的方式。个人权益影响程度判定准则可参考下表。

个人信息保护影响评估参考方法

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、被银行列入黑名单、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、无法使用应提供的服务、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

以定性方式为例，可从“影响个人自主决定权”、“引发差别性待遇”、“个人名誉受损和遭受精神压力”、“个人财产受损”四个维度，依据《信息安全技术 个人信息安全影响评估指南》GB/T 39335-2020的判定准则，对个人信息主体的权益进行影响程度评价。影响程度分为“严重”、“高”、“中”、“低”四个等级，影响程度判定可参考下表。

影响程度判定表

影响类别	影响程度判定原则	影响描述	影响程度
影响个人自主决定权	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：个人人身自由受限、遭受人身伤害。	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：被强迫执行违反个人意愿的操作、被蓄意推送资讯影响个人价值观判断、可能引发个人人身自由受限或遭受人身伤害。	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：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
	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。	低

影响程度判定表

影响类别	影响程度判定原则	影响描述	影响程度
引发差别性待遇	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：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
	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：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应提供的产品或服务）。	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：造成误解、为使用应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
	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：被打扰、产生厌烦和恼怒的情绪等。	低
个人名誉受损和遭受精神压力	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：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
	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：名誉受损以致长期无法获得财务收入、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。	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：造成误解、名誉受损（通过澄清可全部或部分恢复）、产生害怕或紧张的情绪、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
	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：被频繁打扰、产生厌烦和恼怒的情绪等。	低
个人财产受损	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：遭受金融诈骗、资金被盗用、征信信息受损等。	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：社会信用受损，为获取金融产品或服务需付出额外的成本等。	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：因个人信息更正而需执行额外的流程（或提供额外的证明材料）等。	低

个人信息保护影响评估参考方法

评估安全事件发生的可能性

评估过程中，可根据事件自身的性质估计和经验数据评估其可能性,再根据组织所实施的针对性安全控制措施、相关事件处置经验对可能性进行修正。比如,个人信息处理的规模超过1000万人,但有完备的、针对性的个人信息保护揩施和应急机制,或者已具备类似事件处置的经验,并得到了个人信息主体的认同,则安全可能性等级可降低一个级别。在进行修正时需要具体说明修正的理由,必要时可咨询外部专业组织保证修正过程的合理性。

安全事件可能性等级评价可采用定性、半定量和定量的方式。安全事件可能性等级判定准则可参考下表。

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

以定性方式为例，可从“网络环境和技术措施”、“处理流程规范性”、“参与人员与第三方”、“安全态势及处理规模”等方面，依据本标准表2.1的判定原则，对安全事件可能性等级进行评价。可能性等级分为“很高”、“高”、“中”、“低”四个等级，安全事件可能性判定可参考下表。

个人信息保护影响评估参考方法

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，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，或已在合作方已经发生，或收到过权威机构发出的相关风险预警信息，或处理个人信息的规模超过1000万人。	
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。	
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同领域其他组织发现，或在专业机构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的保护个人信息安全。	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。	
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机构所预测。	

个人信息保护影响评估参考方法

个人信息安全风险综合评估

综合分析个人权益影响程度和安全事件可能性两个要素，得出风险等级，并给出相应的改进建议，最终形成评估报告。风险等级可分为：严重、高、中、低四个等级。以定性分析为例，可参考下表。

组织可以根据自身业务特点和内部风险管理策略,设计科学、合理的风险等级判定表,并设定何种等级风险为不可接受的风险,但注意保证风险等级判定表不得随意变更或修订,必要时可咨询外部专业组织保证风险等级判定表的合理性。

风险等级判定表

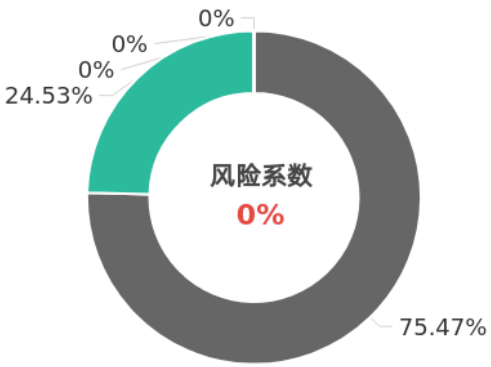
影响级别		可能性级别			
		低	中	高	很高
影响级别	严重	中	高	严重	严重
	高	中	中	高	严重
	中	低	中	中	高
	低	低	低	中	中

个人信息安全风险综合评估

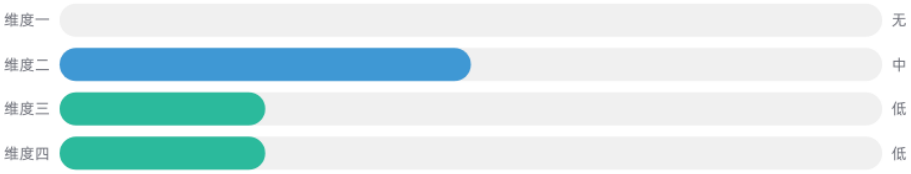
在本次评估中，评估项符合率为75.47%，不符合率为24.53%，其中评估项总数53个，符合项总数40个，不符合项总数13个。问题数总计13个，其中严重风险问题0个，高风险问题0个，中风险问题0个，低风险问题13个。

风险分析

风险等级：无 低 中 高 很高



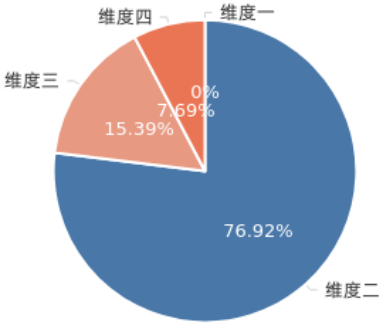
每个维度的风险级别

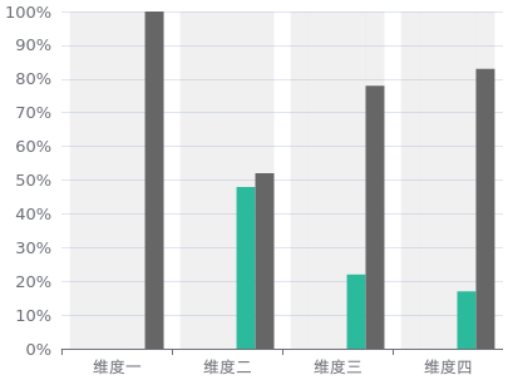


维度一：网络环境和技术措施
维度二：个人信息处理流程
维度三：参与人员与第三方
维度四：业务特点和规模及安全态势

每个维度不符合比例

风险等级：无 低 中 高 很高





总体评价概况

评估结果

序号	可能性描述	可能性等级
1	网络环境和技术措施	暂未发现风险
2	个人信息处理流程	中
3	参与人员与第三方	低
4	业务规模和特点及安全态势	低

注释：速评版问题项较片面，仅做大致的了解，从审慎尽责的自证清白角度出发，建议继续做深度版。

风险分析结果

风险分析

进行风险分析时，首先，我们根据个人信息处理活动的目的、状态、相关个人信息的敏感程度，同时考虑个人信息主体数量、群体特征等要求，评价对个人权益影响的程度等级；其次，我们根据个人信息处理活动涉及的特点、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、及预防性措施等，评价安全事件发生的可能性等级。最后，综合分析个人权益影响程度和安全事件可能性两个要素，得出风险等级。其中，风险分析的具体过程和风险等级的判定可参考附录三。

风险分析结果

风险分析过程表

维度	风险点/脆弱点	影响程度	安全事件可能性	风险等级
网络环境和技术措施	无	无	无	无
个人信息处理流程	评估对象未能够依照个人敏感信息的判定标准定义个人敏感信息，存在个人敏感信息保护措施不足，导致个人敏感信息泄露的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
个人信息处理流程	评估对象未征得用户同意，存在监管处罚，或法律诉讼的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
个人信息处理流程	评估对象未存储超范围收集个人信息的情况，但未定义个人信息最小元素集，存在处理个人信息时无明确标准规范，可能存在超范围采集个人信息的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
个人信息处理流程	评估对象存在变更个人信息使用目的的情况，其情况会对个人信息主体造成影响，但未再次告知个人信息主体，存在数据非授权使用，及监管处罚或法律诉讼的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
个人信息处理流程	评估对象未向个人信息主体提供权利，如个人信息查询、更正、删除、注销、个人信息主体撤回授权同意、获取个人信息副本等，存在监管处罚，或法律诉讼的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	中	低	低
个人信息处理流程	个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
个人信息处理流程	评估对象未个人信息主体提供投诉渠道，存在监管处罚或法律诉讼的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
个人信息处理流程	评估对象存在散播不准确数据或不完整误导性数据的情况，存在监管处罚或法律诉讼的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	中	低	低
个人信息处理流程	评估对象存在诱导或强迫个人信息主体提供过多个人信息的行为，存在监管处罚或法律诉讼的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
个人信息处理流程	评估对象不存在个人信息处理流程的规范，存在个人信息处理流程不规范，导致个人信息处理行为不可控的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
参与人员与第三方	本机构未设立个人信息保护工作机构/部门/组织，存在个人信息保护管理程序不完善的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低

维度	风险点/脆弱点	影响程度	安全事件可能性	风险等级
参与人员与第三方	本机构未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，其内容应该包括隐私政策和相关规程，存在个人信息保护责任人能力不足的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	低	低	低
业务规模和特点及安全态势	本机构近期收到过或公开发布的安全相关的警示信息，存在监管处罚或法律诉讼的风险。 个人信息主体可能会遭受一定程度的困扰，但尚可以克服；	中	低	低

风险处置建议

网络安全业务的风险处置意见

- 建议评估对象依照个人敏感信息的判定标准正确定义个人敏感信息。
- 建议评估对象在对个人信息进行处理前，应征得用户同意。
- 建议评估对象应定义个人信息最小元素集并不要超范围收集个人信息，当超范围收集个人信息时，应当再次告知个人信息主体，并获得个人信息主体授权。
- 建议评估对象变更个人信息使用目的时，应当再次告知个人信息主体，并获得个人信息主体授权。
- 建议评估对象应响应个人信息查询、更正、删除、撤回授权统一、注销账户、获取个人信息副本的权利。
- 建议评估对象对于个人信息的保存时间为最小化，当个人信息保存时间超出范围时应采取删除等机制。
- 建议评估对象为个人信息主体提供投诉渠道。
- 建议评估对象不散播不准确的数据或不完整的误导性数据，或采取手段保证数据的准确性。
- 建议评估对象不应采取诱导或强迫个人信息主体提供过多个人信息。
- 建议评估对象建立个人信息处理流程的规范。
- 建议机构设立个人信息保护负责人，并且个人信息保护负责人应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。
- 建议机构应定期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，其内容应该包括隐私政策和相关规程。
- 建议当机构近期收到过或公开发布的安全相关的警示信息时，机构应对当前情况进行评估，并对评估结果及时整改。

附录A

网络环境和技术措施

评估对象与互联网交互现象为以下哪种?

- [ ] 网络环境与互联网有交互现象
- [x] 网络环境比较独立，与互联网无交互现象

嵌入可收集个人信息的第三方代码、插件时，是否采取了全面的安全措施防止信息泄露、窃取等风险?

- [x] 是，或未嵌入可收集个人信息的第三方代码、插件等
- [ ] 否

访问评估对象时是否进行身份鉴别，并基于工作职责最小必要需求设置个人信息操作权限?

- [x] 是
- [ ] 否

评估对象的个人信息处理系统作为重点区域部署，是否设有边界防护措施，如部署防火墙、IPS、IDS等?

- [x] 是
- [ ] 否

评估对象是否采用技术手段对网络运行状态进行检测和记录，其技术手段能够标记、分析个人信息在内部或与第三方交互时的状态，及时发现异常流程和违规使用情况?

- [x] 是
- [ ] 否

评估对象采取的技术措施是否能防范入侵行为?

- [x] 是
- [ ] 未能采取有效技术措施防范入侵行为

评估对象能防范以下何种入侵行为?（多选）注：若未防范以上常见入侵行为，第6题请修订为“否”。

- [x] 防范病毒
- [ ] 木马后门攻击
- [ ] 端口扫描
- [ ] 拒绝服务攻击

评估对象是否采用校验技术或密码技术保证数据在传输过程中的完整性?

- [x] 是
- [ ] 否

对个人敏感信息进行保护，是否采取加密、去标识化、匿名化等技术手段?

- [x] 是
- [ ] 否

评估对象是否做到制定网络安全事件应急预案，其内容包括应急处置、报告机制?

- [x] 制定网络安全事件应急预案，其内容包括应急处置、报告机制

☐ 否

评估对象是否定期组织对网络安全事件进行应急预案演练？

☑ 是

☐ 否

评估对象是否制定有网络安全事件应急预案报告模板？

☑ 是

☐ 否

评估对象是否有定期漏洞扫描或渗透测试？

☑ 是，两项均有

☐ 仅其中一项（漏洞扫描或渗透测试）

☐ 无

评估对象是否有针对定期漏洞扫描或渗透测试结果或报告及时的整改（补丁更新和安全加固）？

☑ 是

☐ 否

评估对象是否采取技术及管理措施对数据存储介质进行安全保护，以及恢复、备份的演练？

☑ 是

☐ 否

评估对象是否有定期进行数据备份？

☑ 是

☐ 否

评估对象是否有定期对数据备份进行恢复演练？

☑ 是

☐ 否

个人信息处理流程

评估对象是否能够依照个人敏感信息的判定标准定义个人敏感信息？

☐ 是，或已按照个人敏感信息的判定标准进行评估，但未发现存在个人敏感信息

☑ 否；或未按照个人敏感信息的判定标准定义个人敏感信息

评估对象处理个人信息是否出于以下任一种情况：（一）取得个人的同意；（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；（三）为履行法定职责或者法定义务所必需；（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；（七）法律、行政法规规定的其他情形。

☑ 是

☐ 否

评估对象从第三方获得的数据时，是否得到正式的处理授权？

☑ 是；或未从第三方获取个人信息

☐ 否

17

评估对象是否会告知个人信息主体会对个人信息进行处理，其告知内容清晰易懂，无歧义，并且以友好可达的方式告知个人信息主体？

- [x] 告知个人信息主体，告知内容清晰易懂，无歧义，并且以友好可达的方式
- [ ] 告知个人信息主体，但告知内容不清晰易懂，存在歧义，或未以友好可达的方式告知个人信息主体
- [ ] 未告知个人信息主体

评估对象所有的处理活动是否都征得了用户同意？

- [ ] 是
- [x] 否

评估对象是否定义了个人信息最小元素集，并未超范围收集个人信息？

- [ ] 存在超范围收集个人信息的情况
- [x] 未存储超范围收集个人信息的情况，但未定义个人信息最小元素集
- [ ] 未存储超范围收集个人信息的情况，且定义了个人信息最小元素集

评估对象存在变更个人信息使用目的的情况，并且其情况会对个人信息主体造成影响，是否再次告知个人信息主体？

- [ ] 是
- [x] 否；或存在变更个人信息使用目的的情况，但其情况未对个人信息主体造成影响

评估对象是否提供个体参与的机制，包括查询、更正、删除、撤回同意、注销账号等？

- [ ] 有（请在扩展问题中补充选择）
- [x] 无,未能响应个人信息主权利

评估对象是否有委托第三方处理个人信息、或共享个人信息、或与第三方共同处理个人信息、或转让个人信息的情况，并且涉及的第三方存在变更个人信息使用目的的情况？

- [x] 存在上诉情况的第三方，并涉及第三方变更个人信息使用目的的情况
- [ ] 未存在上诉情况的第三方，或存在上诉情况的第三方但未涉及第三方变更个人信息使用目的的情况

评估对象是否存在未经用户同意向第三方共享、转让个人信息的情况？

- [ ] 是
- [x] 否

评估对象对于个人信息的保存时间是否为最小化，并且个人信息保存时间超出范围时采取删除等机制？

- [ ] 存储时间为最小化，并且个人信息保存时间超出范围时采取删除等机制
- [ ] 存储时间为最小化，但个人信息保存时间超出范围时未采取删除等机制
- [x] 永久存储

评估对象是否涉及用户画像的使用，并且用户画像能定位到特定个人？

- [x] 是
- [ ] 否

评估对象是否向用户提供个性化展示，其用户可控制、可退出或关闭个性化展示？

- [ ] 是,或未向用户提供个性化展示
- [x] 否

评估对象是否采用匿名化技术手段，并且匿名化机制有效，去标识化后的个人信息不能够被关联分析等，不会导致可重新识别个人信息主体身份。

- [x] 采用匿名化技术手段，并且匿名化机制有效
- [ ] 未采用匿名化技术手段，或采用的匿名化技术手段能够被关联分析

评估对象是否制定个人信息安全应急处理机制，并提供及时有效的安全事件通知机制？

- [x] 是
- [ ] 否

评估对象是否为个人信息主体提供投诉渠道？
- [ ] 是
- [x] 否

评估对象是否散播不准确的数据或不完整的误导性数据？
- [x] 是
- [ ] 否

评估对象是否诱导或强迫个人信息主体提供过多个人信息？
- [x] 是
- [ ] 否

评估对象是否过多地追踪或监视个人行为？
- [ ] 是
- [x] 否

评估对象是否无根据地限制个人控制其个人信息的行为等？
- [ ] 是
- [x] 否

评估对象是否存在个人信息处理流程的规范？
- [ ] 是
- [x] 否

参与人员与第三方

本机构是否设立个人信息保护负责人或工作机构/部门/组织？
- [ ] 是，有
- [x] 否，没有

本机构是否制定个人信息保护总体方针和安全策略，并提出具体的安全管理要求，其内容包含本机构的个人信息保护工作的目标、范围、原则和安全框架等相关说明？
- [x] 是
- [ ] 否,或未制定个人信息总体方针和安全策略

本机构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？
- [x] 是
- [ ] 否

本机构是否与个人信息处理人员签订保密协议，并对入职关键岗位的人员（如接触大量个人敏感信息）进行背景审查？
- [x] 是
- [ ] 否

本机构是否明确内部涉及个人信息处理不同岗位的安全职责，并建立发生个人安全事件的处罚、问责机制？
- [x] 是

- [ ] 否

本机构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，其内容应该包括隐私政策和相关规程？

- [ ] 是
- [x] 否

本机构是否与可能访问个人信息的外部服务人员签订保密协议或明确需遵守的个人信息安全要求？

- [x] 是
- [ ] 否

本机构是否与第三方签署有约束力的合同等文件，并包含如下内容： 1）约定个人信息传输至第三方后的处理目的； 2）约定个人信息传输至第三方后的处理方式； 3）约定第三方留存个人信息的期限； 4）约定第三方超出期限后的处理方式；

- [x] 是
- [ ] 否

本机构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？

- [x] 是
- [ ] 否

业务规模和特点及安全态势

业务对个人信息处理的依赖性。

- [ ] 高
- [x] 低

本机构处理个人信息的规模。

- [ ] 小于100万
- [x] 大于100万小于1000万
- [ ] 超过1000万

本机构若曾经发生过个人信息泄漏、篡改、损坏、丢失等事件，是否进行有效地整改？

- [x] 是,或未发生过个人信息泄露,篡改,损坏,丢失等事件
- [ ] 否

本机构是否关注个人信息保护相关执法监管动态？

- [x] 是
- [ ] 否

本机构若近期内遭受网络攻击或发生安全事件的情况，是否进行有效地整改？

- [x] 是,或近期内未遭受网络攻击或发生安全事件
- [ ] 否

本机构是否近期收到过或公开发布的安全相关的警示信息？

- [x] 是
- [ ] 否