ICS 35.040
L80

中华人民共和国国家标准

信息安全技术　个人信息安全规范

Information security techniques - personal information security specification

（报批稿）

2017-05-29

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：北京信息安全测评中心、中国电子技术标准化研究院、颐信科技有限公司、四川大学、北京大学、清华大学、中国信息安全研究院有限公司、公安部第一研究所、上海国际问题研究院、阿里巴巴（北京）软件服务有限公司、深圳腾讯计算机系统有限公司、中电长城网际系统应用有限公司、阿里云计算有限公司、华为技术有限公司。

本标准主要起草人：洪延青、何延哲、高林、钱秀槟、陈兴蜀、左晓栋、刘贤刚、高磊、黄劲、上官晓丽、赵章界、范红、杜跃进、杨思磊、邵华、顾伟、黄晓林、蔡晓丹、张亚男、金涛、叶晓俊、郑斌、闵京华、鲁传颖、周亚超、王海舟、王建民、秦颂、姚相振、葛小宇、沈锡镛。

引　言

近年，随着信息技术的快速发展和互联网应用的普及，越来越多的组织大量收集、使用个人信息，给人们生活带来便利的同时，也出现了对个人信息的非法收集、滥用、泄露等问题，个人信息安全面临严重威胁。

本标准针对个人信息面临的安全问题，规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。

对标准中的具体事项，法律法规另有规定的，应遵照其规定执行。

信息安全技术　个人信息安全规范

1　范围

本标准规范了开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求。

本标准适用于规范各类组织个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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/T 25069—2010　信息安全技术　术语

GB/T AAAAA-AAAA　大数据服务安全能力要求

3　术语和定义

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1

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。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：关于个人信息的范围和类别可参考附录A。

3.2

个人敏感信息　personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等的个人信息。

注1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：关于个人敏感信息的范围和类别可参考附录B。

3.3

个人信息主体 personal data subject

个人信息所标识的自然人。

3.4

个人信息控制者 personal data controller

有权决定个人信息处理目的、方式等的组织或个人。

3.5

收集 collect

获得对个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体的交互自动采集、通过共享转让间接获取等方式。

注：如果产品或服务提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集行为。例如，离线导航软件在终端获取用户位置信息后，如不回传至提供者，则不属于个人信息收集行为。

3.6

明示同意 explicit consent

个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。

3.7

用户画像 user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如其职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

3.8

个人信息安全影响评估 personal information security impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

3.9

删除 delete

在日常业务场景和操作所涉及的系统中去除个人信息，使其不可被检索、访问、传输且不能复原的行为。

3.10

公开披露 public disclosure

向社会或特定群体发布信息的行为。

3.11

转让 transfer of control

将个人信息控制权由一个控制者向另一个控制者转移的过程。

3.12

共享 sharing

个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

3.13

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。

3.14

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

3.15

个人信息最小集 minimum set of personal information

实现产品或服务核心业务功能所必需使用，及满足法律法规要求所必需收集的个人信息集合。

注：例如，发送快递所必需的个人信息为收件人、发件人的地址和联系方式；实现机票预定功能所必需的个人信息为姓名、身份证件号码。

4 个人信息安全基本原则

个人信息控制者开展个人信息处理活动，应遵循以下基本原则：

a）权责一致原则——应对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

b）目的明确原则——应具有合法、正当、必要、特定、明确的个人信息处理目的。

c）选择同意原则——应向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意；个人信息主体有权就除个人信息最小集之外的事项，自由做出选择性的授权同意。

d）最少够用原则——除与个人信息主体另有约定外，应只处理满足用户授权同意的目的所需的最少信息类型和数量。目的达成后，应及时根据约定删除个人信息。

e）公开透明原则——应以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

f）确保安全原则——应具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

g）主体参与原则——应向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户等方法。

5 个人信息的收集

5.1 收集个人信息的合法性要求

a）不得欺骗、诱骗、强制个人信息主体提供其个人信息；

b）不得隐瞒产品或服务所具有的自动采集个人信息的功能；

c）不得从非法渠道获取个人信息。

5.2 收集个人信息的最小化要求

a）收集的个人信息应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现；

b）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；

c）间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

5.3 通过主动提供或自动采集方式收集个人信息时的明示同意

a）通过主动提供或自动采集方式收集个人信息时，应取得个人信息主体的明示同意；收集年满14的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意；

b）应确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示，例如，采取个人信息主体主动声明（电子或纸质形式）、主动勾选、主动点击“同意”等方式；

c）收集前应向个人信息主体告知个人信息控制者的数据安全能力；

d）收集前应向个人信息主体告知所提供产品或服务的核心业务功能及所需收集的个人信息最小集，并明确告知拒绝提供或拒绝同意将带来的影响。应允许个人信息主体选择是否提供或同意自动采集；

e）产品和服务如提供其他附加功能，需要收集超出个人信息最小集之外的个人信息时，收集前应向个人信息主体逐一说明该项个人信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集。当个人信息主体拒绝时，可不提供相应的附加功能，但不应以此为理由停止提供核心业务功能，并应保障相应的服务质量；

f）应保障个人信息主体拒绝将其个人信息用于推送商业广告的权利。

注：上述要求的实现方法可参考附录 C。

5.4 间接获取个人信息时的明示同意

a）应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；

b）应了解个人信息提供方已获得的个人信息处理的授权范围，包括使用目的、个人信息主体是否授权同意转让、共享、公开披露等。如本组织开展业务需进行的个人信

息处理活动超出该授权范围，应在获得个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意。

5.5 征得授权同意的例外

以下情形中，收集个人信息无需征得个人信息主体的授权同意：

a）与国家安全、国防安全有关的；

b）与公共安全、公共卫生、重大公共利益有关的；

c）与犯罪侦查、起诉和审判等有关的；

d）出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；

e）所收集的个人信息是个人信息主体主动向社会公众公开的；

f）从依法向社会公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；

g）法律法规规定的其他情形。

5.6 个人信息保护策略的内容和发布

a）个人信息控制者应制定个人信息保护策略，内容应包括但不限于：

1) 个人信息控制者的基本情况，包括注册名称、注册地址、常用办公地点和相关负责人的联系方式等；

2) 收集、使用个人信息的目的，以及目的所涵盖的各个业务场景，如将个人信息用于维护产品和服务的安全，或发现其中的故障所必需；将个人信息用于发现或阻止欺诈、滥用产品和服务行为；将个人信息用于推送商业广告；将个人信息用于形成直接用户画像及其用途等；

3) 各业务场景分别收集的个人信息，以及存放地域、存储期限、收集频率等个人信息处理规则和实际收集的个人信息范围；

4) 对外共享、转让、公开披露个人信息的场景、涉及的个人信息类别、接收个人信息的第三方类型，以及所承担的相应法律责任；

5) 遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施；

6) 个人信息主体的权利和实现机制，如访问方法、更正方法、删除方法、注销账户的方法、撤回同意的方法、获取个人信息副本的方法、约束信息系统自动决策的方法等；

7) 提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；

8) 处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式；

b）个人信息保护策略所告知的信息应真实、准确、完整；

c）个人信息保护策略的内容应清晰易懂，符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言，并在起始部分提供摘要，简述告知内容的重点；

d）个人信息保护策略应公开发布且易于访问，例如，在网站主页、移动应用程序安装页、社交媒体首页等显著位置设置链接；

e）个人信息保护策略应逐一送达个人信息主体，当成本过高或有显著困难时，可以公告的形式发布；

f）在本条a）所载事项发生变化时，应及时更新个人信息保护策略并重新告知个人信息主体。

注：个人信息保护策略的内容可参考附录 D。

6 个人信息的保存

6.1 个人信息保存时间最小化

a）个人信息保存期限应为实现目的所必需的最短时间；

b）超出上述个人信息保存期限后，应对个人信息进行删除或匿名化处理。

6.2 去标识化处理

收集个人信息后，宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。

6.3 个人信息的存储

a）存储个人敏感信息时，应采用加密等安全措施；

b）存储个人生物识别信息时，应采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要。

6.4 个人信息控制者停止运营

当个人信息控制者停止运营其产品或服务时，应：

a）立即停止继续收集个人信息的活动；

b）将停止运营的通知以逐一送达或公告的形式通知个人信息主体；

c）对其所持有的个人信息进行删除或匿名化处理。

7 个人信息的使用

7.1 个人信息访问控制措施

a）对被授权访问个人信息的内部数据操作人员，应按照最小授权的原则，使其只能访问职责所需的最少够用的个人信息，且仅具备完成职责所需的最少的数据操作权限；

b）宜对个人信息的重要操作应设置内部审批流程，如批量修改；

c）应对安全管理人员、数据操作人员、审计人员的角色进行分离设置；

d）如确因工作需要，需授权特定人员超权限处理个人信息的，应由个人信息保护责任人或个人信息保护工作机构进行审批，并记录在案；

注：个人信息保护责任人或个人信息保护工作机构的确定见本标准 10.1。

e）对个人敏感信息的访问、修改等行为，宜在对角色的权限控制的基础上，根据业务流程的需求触发操作授权，例如，因收到客户投诉，投诉处理人员才可访问该用户的相关信息。

7.2 个人信息的展示限制

涉及通过界面展示个人信息的（如计算机屏幕、纸面），应对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。例如在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。

7.3 个人信息的使用限制

a）除业务功能所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人，例如，为准确评价个人信用状况，可使用直接用户画像，而仅用于推送商业广告目的时，则应使用间接用户画像；

b）对所收集的个人信息进行加工处理而产生的信息，能够单独或与其他信息结合识别自然人个人身份，或者反映自然人个人活动情况时，属于个人信息。对其使用应遵循收集个人信息时获得的授权范围；

c）使用个人信息时，不得超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。

注：将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，应对结果中所包含的个人信息进行去标识化处理。

7.4 个人信息访问

应向个人信息主体提供访问下列信息的方法：

a）其所持有的关于该主体的个人信息；

b）上述个人信息的来源、所用于的目的；

c）已经获得上述个人信息的第三方。

7.5 个人信息更正

个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的，个人信息控制者应为其提供请求更正或补充信息的方法。

7.6 个人信息删除

a）符合以下情形的，个人信息主体要求删除的，应及时删除个人信息：

1) 个人信息控制者违反法律法规规定，收集、使用个人信息的；

2) 个人信息控制者违反了与个人信息主体的约定，收集、使用个人信息的；

b）个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除；

c）个人信息控制者违反法律法规规定或与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

7.7 个人信息主体撤回同意

a）应向个人信息主体提供方法撤回收集、使用其个人信息的同意授权；撤回同意后，个人信息控制者后续不得再处理相应的个人信息；

注：撤回同意不影响撤回前基于同意的个人信息处理。

b）应向个人信息主体提供便捷的退订商业广告的方法；

c）对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回同意的方法。

7.8 个人信息主体注销账户

a）通过注册账户提供服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且该方法应简便易操作；

b）个人信息主体注销账户后，应删除其个人信息或做匿名化处理。

7.9 个人信息主体获取个人信息副本

应为个人信息主体提供获取以下类别个人信息副本的方法，或依其要求在技术可行的前提下直接将以下个人信息的副本传输给第三方：

a）个人基本资料、个人身份信息；

b）个人病理及健康信息、个人教育及工作信息、个人财产信息、个人通信信息、联系人信息。

7.10 约束信息系统自动决策

当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时（例如，基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选），个人信息控制者应向个人信息主体提供申诉方法。

7.11 响应个人信息主体的请求

a）在验证个人信息主体身份后，应及时响应个人信息主体基于本标准第7.4至7.10提出的请求，应在三十天内或法律法规规定的期限内做出决定及合理解释，并告知个人信息主体向外部提出纠纷解决的途径；

b）对合理的请求原则上不收取费用，但对一定时期内多次重复的请求，可视情收取一定成本费用；

c）如直接实现个人信息主体的请求需要付出高额的成本或存在其他显著的困难，个人信息控制者应向个人信息主体提供其他替代性方法，以保护个人信息主体的合法权益；

d）以下情况可不响应个人信息主体基于本标准7.4至7.10提出的请求，包括但不限于：

1) 与国家安全、国防安全有关的；
2) 与公共安全、公共卫生、重大公共利益有关的；
3) 与犯罪侦查、起诉和审判等有关的；
4) 个人信息控制者有充分证据表明个人信息主体存在主观恶意或滥用权利的；
5) 响应信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的。

7.12 申诉管理

应建立申诉管理机制，包括跟踪流程，并在合理的时间内，对申诉进行响应。

8 个人信息的委托处理、共享、转让、公开披露

8.1 委托处理

委托处理个人信息时，应遵守以下要求：

a）个人信息控制者应对委托行为进行个人信息安全影响评估，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护水平；

b）应对受委托者提出如下要求：

1) 严格按照个人信息控制者的要求处理个人信息。如受委托者因特殊原因未按照个人信息控制者的要求处理个人信息，应及时反馈；

2) 受委托者确需再次委托时，应事先征得个人信息控制者的授权；

3) 协助其响应个人信息主体基于本标准7.4至7.10提出的请求；

4) 如受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件，应及时反馈；

5) 在委托关系解除时不再保存个人信息；

c）个人信息控制者应对受委托者进行监督，方式包括但不限于：

1) 通过合同等方式规定受委托者的责任和义务；

2) 对受委托者进行审计；

d）准确记录和保存委托处理个人信息的情况。

8.2 个人信息共享、转让

个人信息原则上不得共享、转让，确需共享、转让时，应充分重视风险。共享、转让个人信息，非因收购、兼并、重组原因的，应遵守以下要求：

a）事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b）向个人信息主体告知共享、转让个人信息的目的，数据接收方的类型，并事先征得个人信息主体明示同意；

c）共享、转让个人敏感信息前，除8.2 b）外，还应告知个人信息主体数据接收方的身份和数据安全能力，并事先征得个人信息主体明示同意；

d）准确记录和保存个人信息的共享、转让的情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；

e）承担因共享、转让个人信息对个人合法权益造成损害的相应责任；

f）不得共享、转让个人生物识别信息；

g）帮助个人信息主体了解数据接收方对个人信息的存储、使用等情况，包括个人信息主体的权利，例如，访问、更正、删除、注销账户等。

8.3 收购、兼并、重组时的个人信息转让

当个人信息控制者发生收购、兼并、重组等变更时，变更后的个人信息控制者应继续履行原个人信息控制者的责任和义务。变更个人信息使用目的时，应重新取得个人信息主体的明示同意。

8.4 个人信息公开披露

个人信息原则上不得公开披露，确需公开披露时，应充分重视风险，遵守以下要求：

a）事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b）向个人信息主体告知公开披露个人信息的目的、范围，并事先征得个人信息主体明示同意；

c）准确记录和保存个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

d）承担因公开披露个人信息对个人合法权益造成损害的相应责任；

e）不得公开披露个人生物识别信息。

8.5 共享、转让、公开披露个人信息时事先征得授权同意的例外

以下情形中，共享、转让、公开披露个人信息无需事先征得个人信息主体的授权同意：

a）与国家安全、国防安全有关的；

b）与公共安全、公共卫生、重大公共利益有关的；

c）与犯罪侦查、起诉和审判等有关的；

d）出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；

e）个人信息主体主动向社会公众公开个人信息的；

f）从依法向社会公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

8.6 共同个人信息控制者

当个人信息控制者与第三方共同为个人信息控制者时，如电商平台与平台上的签约电商，个人信息控制者应通过合同等形式，与第三方共同确定应满足的个人信息安全要求，以及在个人信息保护方面自身和第三方应分别承担的责任和义务。

8.7 个人信息跨境传输要求

在中华人民共和国境内运营中收集和产生的个人信息应当在境内存储。如确需跨境传输，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

9 个人信息安全事件处置

9.1 安全事件应急处置和报告

a）应制定个人信息安全事件应急预案；

b）应定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其了解岗位职责和应急处置策略和规程；

c）发生个人信息安全事件后，个人信息控制者应根据应急响应预案进行以下处置：

1) 记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

2) 评估事件可能造成的影响，并采取必要措施控制事态，消除隐患；

3) 按《国家网络安全事件应急预案》的有关规定及时上报，报告内容包括但不限于：涉及个人信息主体的类别、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；

4) 按照9.2的要求实施安全事件的告知。

d）根据相关法律法规变化情况，以及事件处置情况，及时更新应急响应预案。

9.2 安全事件告知

a）应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息；

b）告知内容应包括但不限于：

1) 安全事件的内容和影响；
2) 已采取或将要采取的处置措施；
3) 个人信息主体自主防范和降低风险的建议；
4) 针对个人信息主体提供的补救措施；
5) 个人信息保护负责人和个人信息保护工作机构的联系方式。

10 组织的管理要求

10.1 明确责任部门与人员

a）应明确其法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全保护工作提供人力、财力、物力保障等；

b）应任命个人信息保护负责人和个人信息保护工作机构；

c）满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作：

1) 主要业务涉及个人信息处理，且规模大于200人；
2) 处理超过50万人的个人信息，或在12个月内预计处理超过50万人的个人信息。

d）个人信息保护负责人和个人信息保护工作机构应履行以下职责：

1) 对个人信息保护负总责；
2) 制定、签发、实施、定期更新个人信息保护策略和规程；
3) 应建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源等）和授权访问策略；
4) 开展个人信息安全影响评估；
5) 组织开展个人信息安全培训；
6) 进行安全审计。

10.2 开展个人信息安全影响评估

a）建立个人信息安全影响评估制度，定期（至少每年一次）开展个人信息安全影响评估；

b）个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于：

1) 个人信息收集环节是否遵循目的明确、最少够用等原则；
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，包括处理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) 如发生安全事件，对个人信息主体合法权益可能产生的不利影响。

c）在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，应重新进行个人信息安全影响评估；

d）形成个人信息安全影响评估报告，并以此采取保护个人信息主体的措施，使风险降低到可接受的水平；

e）妥善留存个人信息安全影响评估报告，确保可供相关方查阅，并以适宜的形式对外公开。

10.3 数据安全能力

应根据GB/T AAAAA-AAAA的要求，采取必要的管理和技术措施，建立合适的数据安全能力，防止个人信息的泄漏、损毁、丢失。

10.4 人员管理与培训

a）应与从事个人信息处理岗位上的相关人员签署保密协议，必要时开展背景审查；

b）应明确内部涉及个人信息处理不同岗位的安全职责，以及发生安全事件的处罚机制；

c）应要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；

d）应明确可能访问个人信息的外部服务人员应遵守的个人信息安全要求，与其签署保密协议，并进行监督；

e）应定期（至少每年一次）或在个人信息保护策略发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息保护专业化培训和考核，确保相关人员熟练掌握个人信息保护策略和规程。

10.5 安全审计

a）应对个人信息保护策略和规程，以及安全措施的有效性进行审计；

b）应建立自动化审计系统，监测记录个人信息处理活动；

c）根据审计情况形成的审计记录，应能对安全事件的处置、应急响应和事后调查提供支撑；

d）应防止非授权访问、篡改或删除审计记录；

e）审计过程中发现的个人信息违规使用、滥用等情况，应及时处理。

附 录 A
（资料性附录）
个人信息示例

个人信息是指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，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，则由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

表A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮箱等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等信息
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等
虚拟身份标识信息	软件系统账号、社交类软件昵称、IP 地址、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息，及体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账号、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易信息、消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	如通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的用户的操作记录，包括网站浏览记录、软件使用记录、点击记录等
个人常用设备信息	指包括硬件型号、设备 MAC 地址、操作系统类型、软件列表唯一设备识别码（如 IMEI/androidID/IDFA/OPENUDID/GUID、SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

附 录 B
（资料性附录）
个人敏感信息判定

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等的个人信息。通常情况下，隐私信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

公开披露：某些个人信息仅因在个人信息主体授权的范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

表B.1给出了个人敏感信息的示例。

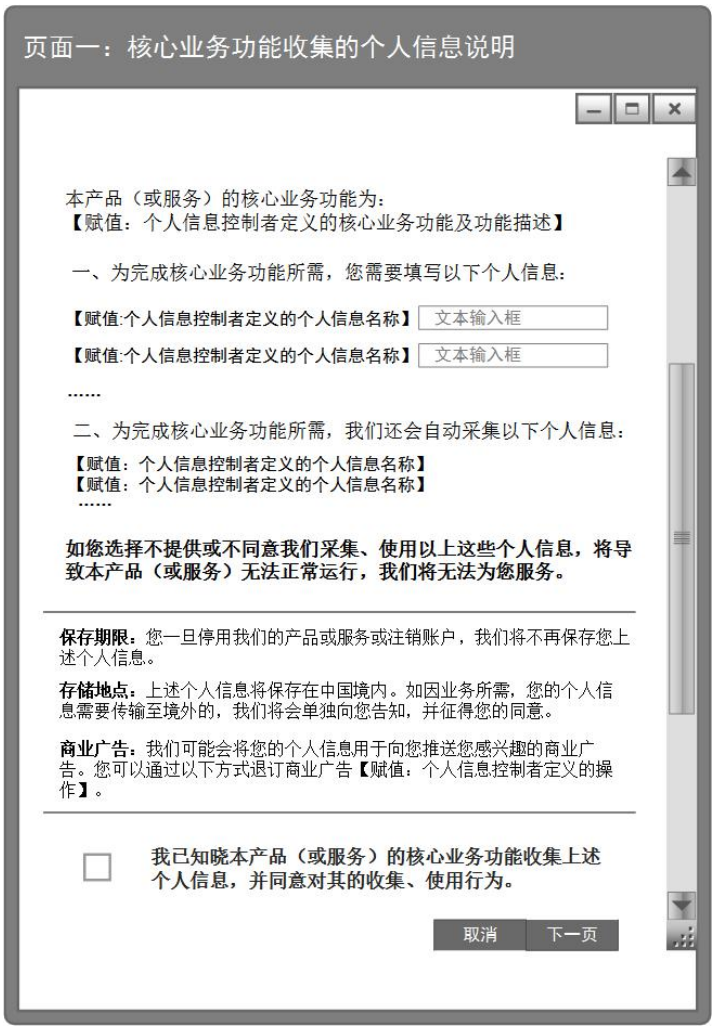
表B.1 个人敏感信息举例

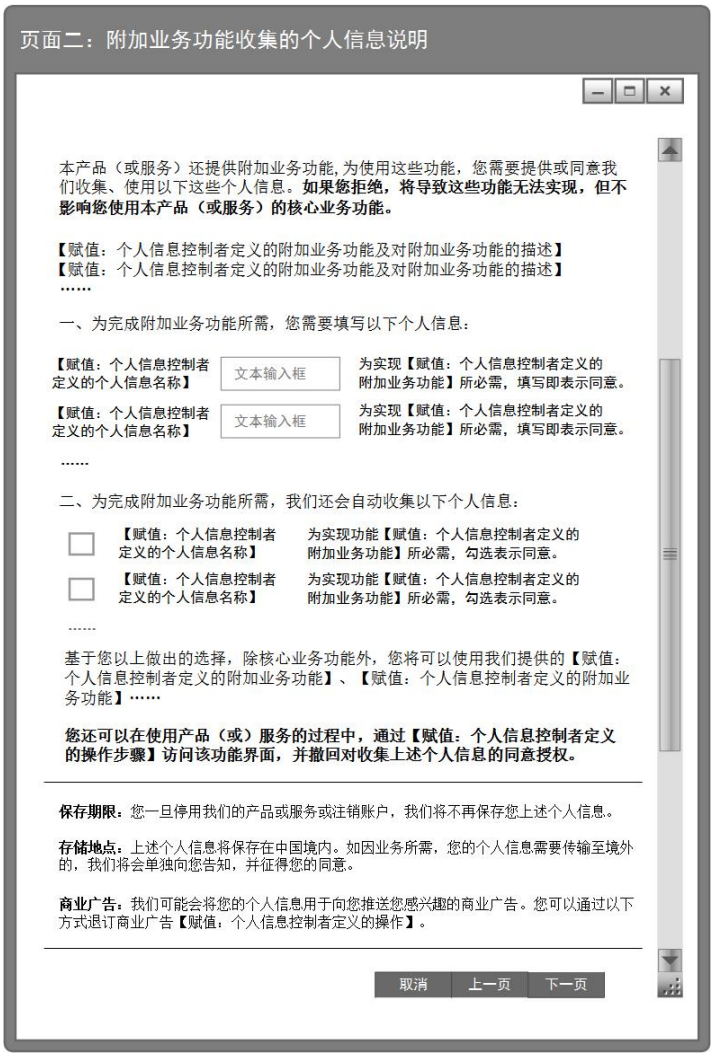
个人财产信息	银行账号、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易信息、消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息，及体重、身高、肺活量等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
虚拟身份标识信息	软件系统账号、社交类软件昵称、IP 地址、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、行踪轨迹、住宿信息、精准定位信息等

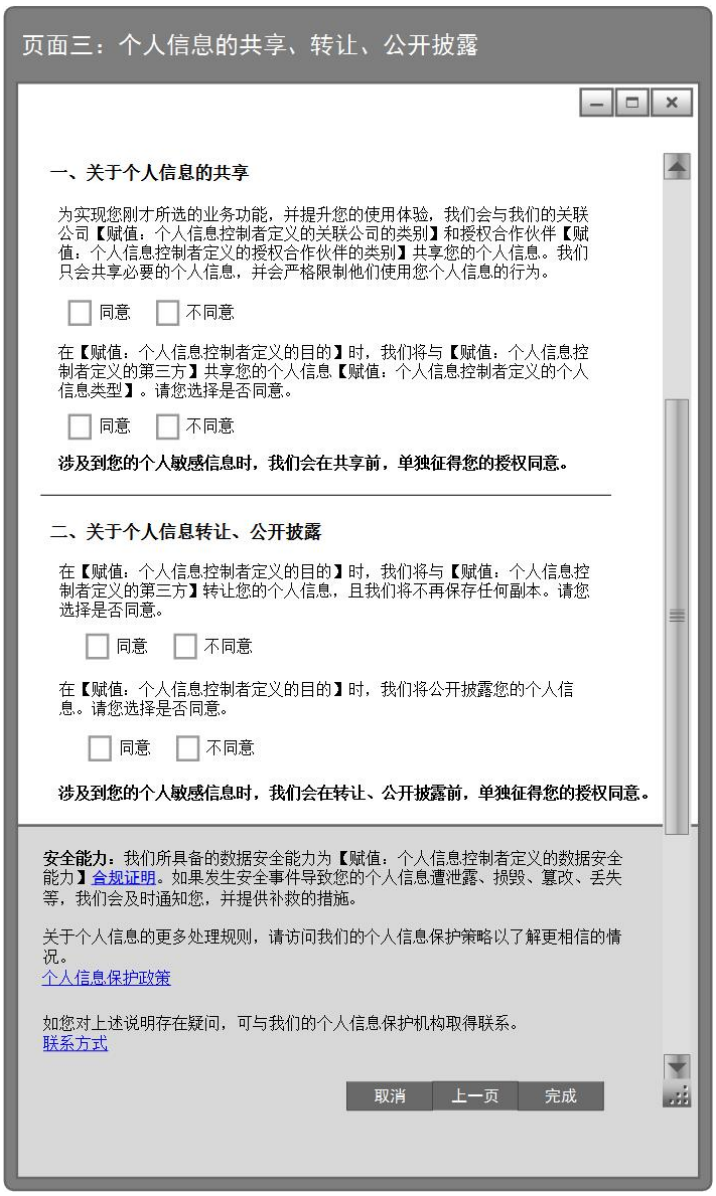
附　录　C
（资料性附录）
保障个人信息主体选择同意权的方法

按照本标准5.2的要求，本附录给出了保障个人信息主体选择同意权的实现方法。个人信息控制者可参考以下模板设计功能界面，保障个人信息主体能充分行使其选择同意的权利。

该功能界面应在个人信息控制者开始收集个人信息前，如产品安装过程中，或个人信息主体首次使用产品或服务时，或个人信息主体注册账号时，由个人信息控制者主动向个人信息主体提供。如以填写纸质材料收集个人信息的，个人信息控制者可以参考以下模板内容设计表格，以保障个人信息主体能行使选择同意的权利。

功能界面模板	说明
	1、为向个人信息主体清晰展示收集个人信息的目的、种类等，并分情形征得个人信息主体同意，建议个人信息控制者采用分阶段、分窗口、分屏幕等方式向个人信息主体展示左侧模板中的功能界面。 2、核心业务功能收集的个人信息即最小集，个人信息控制者需明确定义其产品（或服务）的核心业务功能，识别其必需收集的个人信息。 3、左侧模板中的赋值需要个人信息控制者根据实际情形给出，且内容应清楚明白易懂，不得使用概括性、模糊性语句描述所收集的个人信息。 4、个人信息控制者可结合实际的产品（或服务）形态，考虑适宜、便捷等因素实现左侧模板中的功能。 5、个人信息控制者在实现左侧功能界面时，“空白处”和“勾选处”不得采用预填写的方式。

功能界面模板	说明
	5、附加业务功能是核心业务功能之外的其他功能，常见的附加业务功能如：提高产品（或服务）的使用体验的附加功能（如语音识别、图片识别、地理定位等）、提升产品（或服务）的安全机制的附加功能等（如收集密保邮箱、指纹等）。 6、附加业务功能一般具有可选择、可退订、不影响核心业务等特点，个人信息控制者在识别附加业务功能时需要充分分析其是否具备这些特点，不得将附加业务功能等同于核心业务功能，强制过度收集个人信息。 7、在此页面中，综合个人信息主体主动填写的个人信息项和同意自动收集的个人信息项，个人信息控制者应即时展示个人信息主体可使用的附加功能。 8、个人信息控制者应告知个人信息主体再次访问该功能界面的方法，保障个人信息主体撤回同意的权利。

功能界面模板	说明
	9、与第三方共享、转让和公开披露的情形可能因业务场景复杂的原因变得多样化。个人信息控制者可酌情在此页面增加共享、转让、公开披露的业务场景，或在用户使用过程中以弹窗等形式单独告知，并征得同意。 10、个人信息的保存地域主要指个人信息被存储、备份的国家或地区，而非具体的数据中心地址。 11、数据安全能力指个人信息控制者保护个人信息保密性、完整性和可用性的能力，个人信息控制者可以通过开展相关的国家标准合规工作证明其数据安全能力，并将相关证明以链接形式向个人信息主体展示。 12、个人信息控制者应向个人信息主体提供针对处理规则的答疑渠道，如果个人信息主体不认可其处理规则，可以选择不继续使用该产品（或服务）。 13、应向个人信息主体告知与个人信息控制者联系的方式； 14、应明示个人信息保护策略的链接，以便个人信息主体查阅。

附 录 D
（资料性附录）
个人信息保护策略模板

个人信息保护策略是个人信息控制者遵循公开透明原则的重要体现，保证个人信息主体知情权的重要手段，还是约束自身行为和配合监督管理的重要机制。个人信息保护策略应清晰、准确、完整地描述个人信息控制者的个人信息处理行为。

个人信息保护策略模版	编写要求
本政策仅适用于XXXX的XXXX产品或服务，包括……。 最近更新日期：XXXX年XX月。 如果您有任何疑问、意见或建议，请通过以下联系方式与我们联系： 电子邮件： 电　　话： 传　　真：	该部分为适用范围。包含个人信息保护策略所适用的产品或服务范围、所适用的用户类型、生效及更新时间等。
本政策将帮助您了解以下内容： 1、我们如何收集和使用您的个人信息 2、我们如何使用 Cookie 和同类技术 3、我们如何共享、转让、公开披露您的个人信息 4、我们如何保护您的个人信息 5、您的权利 6、我们如何处理儿童的个人信息 7、您的个人信息如何在全球范围转移 8、本策略如何更新 9、如何联系我们 XXXX深知个人信息对您的重要性，并会尽全力保护您对自身的个人信息的安全可控。我们致力于维持您对我们的信任，恪守以下原则，保护您的个人信息：权责一致原则、目的明确原则、选择同意原则、最少够用原则、确保安全原则、主体参与原则、公开透明原则等。同时，XXXX承诺，我们将按业界最高水平的安全标准，采取相应的安全保护措施来保护您的个人信息。 请在使用我们的产品（或服务）前，仔细阅读并了解本《个人信息保护策略》。	该部分为个人信息保护策略的重点说明，是个人信息保护策略的一个要点摘录。目的是使个人信息主体快速了解个人信息保护策略的主要组成部分、个人信息控制者所做声明的核心要旨。

个人信息保护策略模版	编写要求
一、我们如何收集和使用您的个人信息 个人信息是指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。 XXXX仅会出于本政策所述的以下目的，收集和使用您的个人信息： **（一）为您提供网上购物服务**【注：示例】 1、业务场景一：注册成为用户 为完成创建账号，您需提供以下信息：您的姓名、电子邮箱地址、创建的用户名和密码、……。 在注册过程中，如果您提供以下额外信息，将有助于我们给您提供更好的服务和体验：手机号、工作职位、公司、教育背景、……。但如果您不提供这些信息，将不会影响使用本服务的基本功能。 您提供的上述信息，将在您使用本服务期间持续授权我们使用。在您注销账号时，我们将停止使用并删除上述信息。 上述信息将存储于中华人民共和国境内。如需跨境传输，我们将会单独征得您的授权同意。 2、业务场景二：商品展示、个性化推荐、发送促销营销信息。 （略） 3、业务场景三：与卖家沟通交流 （略） 4、业务场景四：支付结算 （略） **（二）交付产品或服务**【注：示例】 （略） **（三）开展内部审计、数据分析和研究，改善我们的产品和服务**【注：示例】 （略） **（四）改善我们的防损和反欺诈计划**【注：示例】 （略） **（五）……** …… 当我们要将信息用于本策略未载明的其它用途时，会事先征求您的同意。 当我们要将基于特定目的收集而来的信息用于其他目的时，会事先征求您的同意。	1、详细列举收集和使用个人信息的目的，不得使用概括性语言。 2、根据目的下属的不同业务场景，详细列出收集的个人信息类型。 3、明确描述哪些类型的个人信息属于特定业务场景所必需的。 4、收集身份证、护照、驾照等法定证件信息和个人生物识别信息时，应专门提醒个人信息主体此次收集活动涉及的信息，并说明处理目的、处理规则。 5、不得使用概括性语言综述所收集个人信息，如“我们收集您的身份等相关信息”此类描述，而应明确写明“我们收集您的姓名、电话号码、地址信息”。 6、说明个人信息在使用过程中涉及的地理区域，如个人信息存储和备份的地域，个人信息传输过程中涉及的地域范围；如果个人信息存在出境处理情况，需单独列出或重点标识。 7、使用个人信息时，是否形成直接用户画像及其用途需要明确说明。 8、根据个人信息的使用情况，注明不同类别个人信息预计的保留时间（如：自收集日期开始5年内）以及需要删除或销毁的截止日期（如：2019年12月31日或用户注销账户时）。 9、确需改变信息收集和使用的目的，应当说明会征得用户的同意。

个人信息保护策略模版	编写要求
二、我们如何使用 Cookie 和同类技术 **（一）Cookie** 为确保网站正常运转，我们会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符。借助于 Cookie，网站能够存储您的偏好或购物篮内的商品等数据。 我们不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。有关详情，请参见 AboutCookies.org。您可以清除计算机上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问我们的网站时亲自更改用户设置。如需详细了解如何更改浏览器设置，请访问以下链接：<Internet Explorer>、<Google Chrome>、<Mozilla Firefox>、<Safari> 和 <Opera>。 **（二）网站信标和像素标签** 除 Cookie 外，我们还会在网站上使用网站信标和像素标签等其他同类技术。例如，我们向您发送的电子邮件可能含有链接至我们网站内容的点击 URL。如果您点击该链接，我们则会跟踪此次点击，帮助我们了解您的产品和服务偏好并改善客户服务。网站信标通常是一种嵌入到网站或电子邮件中的透明图像。借助于电子邮件中的像素标签，我们能够获知电子邮件是否被打开。如果您不希望自己的活动以这种方式被追踪，则可以随时从我们的寄信名单中退订。 **（三）Do Not Track（请勿追踪）** 很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何应对此类请求。但如果您的浏览器启用了 Do Not Track，那么我们的所有网站都会尊重您的选择。 **（四）……** ……	1、如果个人信息控制者或其授权第三方使用自动数据收集工具收集个人信息，则需要对使用的技术机制做详细描述。 2、常见的自动数据收集工具有：Cookie、脚本、Web 信标、Flash Cookie、内嵌 Web 链接、本地存储器等。 3、说明使用自动工具收集个人信息的目的，并向用户提供限制自动工具进行数据收集的方法和详细的指导。

个人信息保护策略模版	编写要求
三、我们如何共享、转让、公开披露您的个人信息 **（一）共享** 我们不会与XXXX以外的任何公司、组织和个人分享您的个人信息，但以下情况除外： 1、在获取明确同意的情况下共享：获得您的明确同意后，我们会与其他方共享您的个人信息。 2、我们可能会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。 3、与我们的附属公司共享：您的个人信息可能会与XXXX的附属公司共享。我们只会共享必要的个人信息，且受本个人信息保护策略中所声明目的的约束。附属公司如要改变个人信息的处理目的，将再次征求您的授权同意。 我们的附属公司包括：……。 4、与授权合作伙伴共享：仅为实现本策略中声明的目的，我们的某些服务将由授权合作伙伴提供。我们可能会与合作伙伴共享您的某些个人信息，以提供更好的客户服务和用户体验。例如，在您上网购买我们的产品时，我们必须与物流服务提供商共享您的个人信息才能安排送货，或者安排合作伙伴提供服务。我们仅会出于合法、正当、必要、特定、明确的目的共享您的个人信息，并且只会共享提供服务所必要的个人信息。我们的合作伙伴无权将共享的个人信息用于任何其他用途。 目前，我们的授权合作伙伴包括以下X大类型： 1）广告、分析服务类的授权合作伙伴。除非得到您的许可，否则我们不会将您的个人身份信息（指可以识别您身份的信息，例如姓名或电子邮箱，通过这些信息可以联系到您或识别您的身份）与提供广告、分析服务的合作伙伴分享。我们会向这些合作伙伴提供有关其广告覆盖面和有效性的信息，而不会提供您的个人身份信息，或者我们将这些信息进行汇总，以便它不会识别您个人。例如，只有在广告主同意遵守我们的广告发布准则后，我们才可能会告诉广告主他们广告的效果如何，或者有多少人看了他们广告或在看到广告后安装了应用，或者向这些合作伙伴提供不能识别个人身份的人口统计信息（例如“位于北京的25岁男性，喜欢软件开发”），帮助他们了解其受众或顾客。 2）供应商、服务提供商和其他合作伙伴。我们将信息发送给在全球范围内支持我们业务的供应商、服务提供商和其他合作伙伴，这些支持包括提供技术基础设施服务、分析我们服务的使用方式、衡量广告和服务的有效性、提供客户服务、支付便利或进行学术研究和调查。 3）…… 对我们与之共享个人信息的公司、组织和个人，我们会与其签署严格的保密协定，要求他们按照我们的说明、本个人信息保护策略以及其他任何相关的保密和安全措施来处理个人信息。 **（二）转让** 我们不会将您的个人信息转让给任何公司、组织和个人，但以下情况除外： 1、在获取明确同意的情况下转让：获得您的明确同意后，我们会向其他方转让您的个人信息； 2、在涉及合并、收购或破产清算时，如涉及到个人信息转让，我们会在要求新的持有您个人信息的公司、组织继续受此个人信息保护策略的约束，否则我们将要求该公司、组织重新向您征求授权同意。 **（三）公开披露** 我们仅会在以下情况下，公开披露您的个人信息： 1、获得您明确同意后； 2、基于法律的披露：在法律、法律程序、诉讼或政府主管部门强制性要求的情况下，我们可能会公开披露您的个人信息。	1、个人信息控制者说明是否需要共享、转让个人信息，并详细描述需要共享转让的个人信息类型、共享转让的原因、个人信息的接收方、对接收方的约束和管理准则、接收方使用个人信息的目的、个人信息共享转让过程中的安全措施、共享转让个人信息是否对用户带来高危风险。 2、个人信息控制者说明是否需要公开披露个人信息，并详细描述需要公开披露的个人信息类型、原因、是否对用户带来高危风险。 3、说明何种情况下个人信息控制者会不经过用户同意，共享转让和公开披露数据，如响应执法机关和政府机构的要求、进行个人信息安全审计、保护用户免受遭受欺诈和严重人身伤害等。 4、平台服务相关责任说明。如果个人信息控制者提供的服务属于平台类服务（如：电商、社交、信息发布等），需要明确提醒用户其在上传、交流、发布共享此类信息时所面临的风险，并说明共享此类信息采取的安全措施。

个人信息保护策略模版	编写要求
四、我们如何保护您的个人信息 （一）我们已使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权访问、公开披露、使用、修改、损坏或丢失。我们会采取一切合理可行的措施，保护您的个人信息。例如，在您的浏览器与“服务”之间交换数据（如信用卡信息）时受 SSL 加密保护；我们同时对XXXX网站提供 https 安全浏览方式；我们会使用加密技术确保数据的保密性；我们会使用受信赖的保护机制防止数据遭到恶意攻击；我们会部署访问控制机制，确保只有授权人员才可访问个人信息；以及我们会举办安全和隐私保护培训课程，加强员工对于保护个人信息重要性的认识。 （二）我们已经取得了以下认证：……。 （三）我们的数据安全能力：……。 （四）我们会采取一切合理可行的措施，确保未收集无关的个人信息。我们只会在达成本政策所述目的所需的期限内保留您的个人信息，除非需要延长保留期或受到法律的允许。 （五）互联网并非绝对安全的环境，而且电子邮件、即时通讯、及与其他XXXX用户的交流方式并未加密，我们强烈建议您不要通过此类方式发送保密信息。请使用复杂密码，协助我们保证您的帐号安全。 （六）我们将定期更新并公开安全风险、个人信息安全影响评估等报告的有关内容。您可通过以下方式获得……。 （七）互联网环境并非百分之百安全，我们将尽力确保或担保您发送给我们的任何信息的安全性。如果我们的物理、技术、或管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损，我们将承担相应的法律责任。 在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将及时将事件相关情况以邮件、信函、电话、推送通知等方式告知您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。	1、详细说明个人信息控制者对个人信息进行安全保护的措施。包括但不限于个人信息完整性保护措施，个人信息传输、存储和备份过程的加密措施，个人信息访问、使用的授权和审计机制，个人信息的保留和删除机制等。 2、根据 GB/T AAAAA《信息安全技术 大数据服务安全能力要求》确定自己的数据安全能力。 3、目前遵循的个人信息安全协议和取得的认证。包含个人信息控制者目前主动遵循的国际或国内的个人信息安全法律、法规、标准、协议等，以及个人信息控制者目前已取得的个人信息安全相关的权威独立机构认证。 4、可重点提醒公众如何在使用产品或服务时保护好个人信息。 5、应描述提供个人信息后可能存在的安全风险。 6、应表明：在发生个人信息安全事件后，个人信息控制者将承担法律责任。 7、应表明：发生个人信息安全事件后，将及时告知个人信息主体。

个人信息保护策略模版	编写要求
五、您的权利 按照中国相关的法律、法规、标准，以及其他国家、地区的通行做法，我们保障您对自己的个人信息行使以下权利： **（一）访问您的个人信息** 您有权访问您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问： 账户信息——如果您希望访问或编辑您的账户中的个人资料信息和支付信息、更改您的密码、添加安全信息或关闭您的账户等，您可以通过访问XXXX执行此类操作。 搜索信息——您可以在XXXX中访问或清除您的搜索历史记录、查看和修改兴趣以及管理其他数据。 …… 如果您无法通过上述链接访问这些个人信息，您可以随时使用我们的 Web 表单联系，或发送电子邮件至XXXX。我们将在30天内回复您的访问请求。 对于您在使用我们的产品或服务过程中产生的其他个人信息，只要我们不需要过多投入，我们会向您提供。如果您想行使数据访问权，请发送电子邮件至XXXX。 **（二）更正您的个人信息** 当您发现我们处理的关于您的个人信息有错误时，您有权要求我们做出更正。您可以通过“（一）访问您的个人信息”中罗列的方式提出更正申请。 如果您无法通过上述链接更正这些个人信息，您可以随时使用我们的 Web 表单联系，或发送电子邮件至XXXX。我们将在30天内回复您的更正请求。 **（三）删除您的个人信息** 在以下情形中，您可以向我们提出删除个人信息的请求： 1、如果我们处理个人信息的行为违反法律法规； 2、如果我们收集、使用您的个人信息，却未征得您的同意； 3、如果我们处理个人信息的行为违反了与您的约定； 4、如果您不再使用我们的产品和服务，或您注销了账号； 5、如果我们不再为您提供产品和服务。 若我们决定响应您的删除请求，我们还将同时通知从我们获得您的个人信息的实体，要求其及时删除，除非法律法规另有规定，或这些实体获得您的独立授权。 当您从我们的服务中删除信息后，我们可能不会立即备份系统中删除相应的信息，但会在备份更新时删除这些信息。 **（四）改变您授权同意的范围** 每个业务场景需要一些基本的个人信息才能得以完成（见本策略“第一部分”）。对于最小集之外的个人信息的收集和使用，您可以随时给予或收回您的授权同意。 您可以通过以下方式自行操作： …… 当您收回同意后，我们将不再处理相应的个人信息。但您收回同意的决定，不会影响此前基于您的授权而开展的个人信息处理。 如果您不想接受我们给您发送的商业推广，您随时可通过以下方式取消： …… **（五）个人信息主体注销账户** 您随时可注销此前注册的账户，您可以通过以下方式自行操作： …… 在注销账户之后，我们将停止为您提供产品和服务，并依据您的要求，删除您的个人信息，法律法规另有规定的除外。 **（六）个人信息主体获取个人信息副本** 您有权获得您的个人信息副本，您可以通过以下方式自行操作：	1、说明用户对其个人信息拥有何种权利，内容包括但不限于：信息收集、使用和公开披露时允许用户选择的个人信息范围，用户所具备的访问、更正、删除、获取等控制权限，用户隐私偏好设置，用户可以选择的通信和广告偏好，用户不再使用服务后撤回同意和注销账号的渠道、用户进行维权的有效渠道等。 2、对于需要自行配置或操作（如对所使用的软件、浏览器、移动终端等进行配置和操作）以达到个人信息控制的目的，个人信息控制者应对配置和操作的过程进行详细说明，说明方式易于用户理解，必要时提供技术支持的渠道（客服电话、在线客服等）。 3、如果用户访问和控制其个人信息的过程产生费用，需明确说明收费的原因和依据。 4、如果用户提出访问和控制其个人信息的需求后需要较长时间才能响应，需明确说明响应的时间节点，以及无法短时间内响应的原因。 5、如果用户进行访问和控制其个人信息的过程需要再次验证身份，需明确说明验证身份的原因，并采取适当的控制措施，避免验证身份过程中造成的个人信息泄露。 6、如果个人信息控制者拒绝用户对个人信息进行更正、删除、获取的要求，需明确说明拒绝的原因和依据。如用户提出对调查记录、交易记录等进行删除时，个人信息控制者可以拒绝请求并向用户出示合法的依据。

个人信息保护策略模版	编写要求
…… 在技术可行的前提下，例如数据接口匹配，我们还可按您的要求，直接将您的个人信息副本传输给您指定的第三方。 **（七）约束信息系统自动决策** 在某些业务场景中，我们可能仅依据信息系统、算法等在内的非人工自动决策机制做出决定。如果这些决定显著影响您的合法权益，您有权要求我们做出解释，我们也将提供适当的救济方式。法律法规另有规定的除外。 **（八）响应您的上述请求** 为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。我们可能会先要求您验证自己的身份，然后再处理您的请求。 我们将在三十天内做出答复。如您不满意，还可以通过以下途径投诉： …… 对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情收取一定成本费用。对于那些无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际（例如，涉及备份磁带上存放的信息）的请求，我们可能会予以拒绝。 在以下情形中，按照法律法规要求，我们将无法响应您的请求： 1、与国家安全、国防安全有关的； 2、与公共安全、公共卫生、重大公共利益有关的； 3、与犯罪侦查、起诉和审判等有关的； 4、有充分证据表明您存在主观恶意或滥用权利的； 5、响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的。	

个人信息保护策略模版	编写要求
六、我们如何处理儿童的个人信息 我们的产品、网站和服务主要面向成人。如果没有父母或监护人的同意，儿童不得创建自己的用户账户。 对于经父母同意而收集儿童个人信息的情况，我们只会在受到法律允许、父母或监护人明确同意或者保护儿童所必要的情况下使用或公开披露此信息。 尽管当地法律和习俗对儿童的定义不同，但我们将不满 14 周岁的任何人均视为儿童。 如果我们发现自己在未事先获得可证实的父母同意的情况下收集了儿童的个人信息，则会设法尽快删除相关数据。	
七、您的个人信息如何在全球范围转移 原则上，我们在中华人民共和国境内收集和产生的个人信息，将存储在中华人民共和国境内。 由于我们通过遍布全球的资源和服务器提供产品和服务，这意味着，在获得您的授权同意后，您的个人信息可能会被转移到您使用产品或服务所在国家/地区的境外管辖区，或者受到来自这些管辖区的访问。 此类管辖区可能设有不同的数据保护法，甚至未设立相关法律。在此类情况下，我们会确保您的个人信息得到在中华人民共和国境内足够同等的保护。例如，我们会请求您对跨境转移个人信息的同意，或者在跨境数据转移之前实施数据匿名等安全举措。	个人信息的跨境传输。如果因业务需求、政府和司法监管要求存在跨境信息传输情况，需详细说明需要进行跨境传输的数据类型，以及跨境传输遵守的标准、协议和法律机制（合同等）。
八、本策略如何更新 我们的个人信息保护策略可能变更。 未经您明确同意，我们不会削减您按照本个人信息保护策略所应享有的权利。我们会在本页面上发布对本策略所做的任何变更。 对于重大变更，我们还会提供更为显著的通知（包括对于某些服务，我们会通过电子邮件发送通知，说明个人信息保护策略的具体变更内容）。 本政策所指的重大变更包括但不限于： 1、我们的服务模式发生重大变化。如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等； 2、我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等； 3、个人信息公开披露的主要对象发生变化； 4、您参与个人信息处理方面的权利及其行使方式发生重大变化； 5、我们负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化时； 6、个人信息安全影响评估报告表明存在高风险时。 我们还会将本策略的旧版本存档，供您查阅。	个人信息控制者在个人信息保护策略发生重大变化时，需及时更新个人信息保护策略，并说明使用何种方式及时通知用户。通常情况下采取的通知方式如：用户登录信息系统时征求用户同意、更新信息系统版本并在用户使用时弹出窗口征求用户同意、用户使用信息系统时直接向用户推送通知、向用户发送邮件、短信征求用户同意等。

个人信息保护策略模版	编写要求
九、如何联系我们 如果您对本个人信息保护策略有任何疑问、意见或建议，通过以下方式与我们联系：…… 我们设立了个人信息保护专职部门（或个人信息保护专员），您可以通过以下方式与其联系：…… 一般情况下，我们将在三十天内回复。 如果您对我们的回复不满意，特别是我们的个人信息处理行为损害了您的合法权益，您还可以通过以下外部途径寻求解决方案：……	1、个人信息控制者需要明确给出处理个人信息安全相关反馈、投诉的渠道，如个人信息安全责任部门的联系方式、地址、电子邮箱、用户反馈问题的表单等，并明确用户可以收到回应的时间。 2、个人信息控制者需给出外部争议解决机构及其联络方式，以应对与用户出现无法协商解决的争议和纠纷。外部争议解决机构通常为：个人信息控制者所在管辖区的法院、认证个人信息控制者个人信息保护策略的独立机构、行业自律协会或政府相关管理机构等。

参 考 文 献

[1] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

[2] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息安全指南

[3] 《全国人大常委会关于维护互联网安全的决定》，2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过

[4] 《全国人大常委会关于加强网络信息保护的决定》，2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过

[5] 《电信和互联网用户个人信息保护规定》，2013 年 7 月 16 日中华人民共和国工业和信息化部令第 24 号公布，自 2013 年 9 月 1 日起施行

[6] 《中华人民共和国刑刑法修正案（五）》，2005 年 2 月 28 日第十届全国人民代表大会常务委员会第十四次会议通过

[7] 《中华人民共和国刑刑法修正案（七）》，2009 年 2 月 28 日第十一届全国人民代表大会常务委员会第七次会议通过

[8] 《中华人民共和国刑刑法修正案（九）》，2015 年 8 月 29 日第十二届全国人民代表大会常务委员会第十六次会议通过

[9] ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework

[10] EU. General Data Protection Regulation, 2015-05-24

[11] CWA 16113:2012 Personal Data Protection Good Practices

[12] ISO/IEC 29101:2013 Information technology — Security techniques — Privacy architecture framework

[13] NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations, 2013-04

[14] NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), 2010-04

[15] ISO/IEC FDIS 29134 Information technology — Security techniques — Privacy impact assessment, 2017-02-20

[16] ISO/IEC FDIS 29151 Information technology — Security techniques — Code of practice for personally identifiable information protection, 2016-12-16

[17] NISTIR 8062 An Introduction to Privacy Engineering and Risk Management for Federal Systems, 2017-01

[18] ISO/IEC 2nd WD 29184 Information technology — Security techniques — Guidelines for online privacy notices and consent, 2016-12-04

[19] EU-U.S. Privacy Shield, 2016-02-02

[20] The OECD Privacy Framework, OECD 2013

[21] APEC Privacy Framework, APEC 2005-12

[22] Consumer Bill of Rights, White House 2012-02