上海交大教育集团
SHANGHAI JIAO DA EDUCATIONT GROUP

APP 移动应用安全标准

1

移动应用安全标准

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

2

个人信息安全规范

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

个人信息安全规范

3

一、《个人信息安全规范》的效力问题

《规范》的标准为推荐性国家标准。根据《国家标准化法》规定，强制性标准必须执行，国家鼓励采用推荐性标准。

但是，根据《规范》适用范围说明，《规范》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管、管理和评估”。在此之前，国家网信办有关领导也明确指出，规范“定位为我国个人信息保护工作的基础性标准文件.....为制定和实施个人信息保护相关法律法规奠定基础，为国家主管部门、第三方测评机构等开展个人信息安全管理、评估工作提供指导和依据。”

个人信息安全规范

4

一、《个人信息安全规范》的效力问题

在实践中，之前网信办、工信部、公安部等联合开展的隐私条款专项工作也主要是以《规范（征求意见稿）》为依据；国家网信办网络安全协调局约谈“支付宝年度账单事件”当事企业负责人时，也再次强调了《规范》的准据效力。

个人信息安全规范

5

二、个人信息有关的几个法律概念界定

前面提到，《网络安全法》及其配套制度关于个人信息保护的规范相对原则，而本次《规范》重点明确了实践中比较关注的几个概念。

首先，《规范》明确了“敏感个人信息”的范畴。《规范》及其附录确定了敏感个人信息的认定标准、实例以及敏感个人信息的特殊合规要求，这与《网络安全法》规定的数据分类措施相衔接。

其次，《规范》明确了“收集”的法律概念，明确将个人信息收集行为分为主动提交、自动采集、从第三方获取三种方式，并将获取但不回传至服务器的行为排除在“收集”行为之外。

此外，《规范》还明确规定了实践中争议较大的“删除”、“用户画像”、“匿名化”等概念，对于企业合规建设具有重要的参考价值。

个人信息安全规范

6

三、个人信息收集的合规要求

本次《规范》明确了企业收集个人信息的合规要求，主要包括如下几个方面：

第一，《规范》明确了用户知悉的合规要求。《规范》明确规定企业应当告知用户，网络产品或服务的不同业务功能分别收集了哪些个人信息，并应当通过隐私政策的方式明确告知用户收集的个人信息的详细、完整规则。收集行为涉及共同个人信息控制者时，还应当明确告知用户共同控制的第三方及各自责任。

第二，《规范》明确了用户同意的合规要求。《规范》对用户的明示同意作出了示例性规范，包括作出书面声明、主动勾选、主动点击“同意”/“注册”/“发送”等主动性动作。《规范》还规定了收集用户个人敏感信息时的特殊规则。

个人信息安全规范

7

三、个人信息收集的合规要求

本次《规范》明确了企业收集个人信息的合规要求，主要包括如下几个方面：

第三，《规范》明确了收集同意规则的例外情形。《规范》明确，当所收集的个人信息是个人信息主体自行向社会公开的，或者收集着从合法公开披露的信息中收集个人信息的，或者用于学术研究等目的时，可以无需征得信息主体的授权或者同意程序相应克减。

第四，《规范》明确了从第三方获取个人信息的审查要求。《规范》明确，企业从第三方获取个人信息时，应当要求提供者说明来源，并审查来源的合法性以及是否履行了必要的同意程序等。

个人信息安全规范

8

四、个人信息分享的合规要求

《规范》明确规定，委托第三方处理个人信息时，应当开展个人信息安全影响评估，并应当采取措施监督、记录第三方委托处理的行为，并应当对第三方进行审计。

关于个人信息的转让，《规范》规定应当开展个人信息安全影响评估，并应当采取措施监督、记录受让方的行为，同时还规定应承担转让造成损害的法律责任。因并购、重组等发生控制主体变更的，应当单独向用户告知相关情况。

关于个人信息的跨境传输，除了应当满足分享的合规要求外，还应当按照《网络安全法》及其落地政策规定履行安全评估程序。

个人信息安全规范

五、用户控制个人信息的合规要求

根据之前网信办、工信部、公安部等联合开展的隐私条款专项工作反馈的情况，以及全国人大常委会一法一决定的执法检查报告，绝大多数企业关于用户控制个人信息的义务未落实，问题相对突出。

本次《规范》详细规定了用户个人信息控制权的实现方式，明确规定了用户访问、更正、删除个人信息，以及撤回同意授权、注销账户的细则及合规要求。例如，企业应当在30天内相应用户的访问、更正、删除等需求，并告知用户相应的纠纷解决路径。

个人信息安全规范

六、企业个人信息管理制度的合规要求

《网络安全法》实施以后，为企业赋予了很多网络安全义务和责任，其中非常重要的一条即是，应当制定合规的个人信息管理制度。落实到《规范》层面，具体要求包括：

第一，应当明确个人信息保护的责任部门及人员。《规范》明确，规模达到一定条件的企业，应当任命个人信息保护负责人和个人信息保护工作机构并公开其联系方式，并对其职责作出明确规定。

第二，应当建立个人信息岗位人员管理及培训制度。《规范》明确，应当与相关人员签订保密协议，并对相关人员开展背景调查，建立专业化培训和考核机制、处罚机制。

个人信息安全规范

六、企业个人信息管理制度的合规要求

第三，应当建立内部个人信息访问控制措施及制度，并有效的限制个人信息的展示，约束自动化程序使用与救济，等等。与此同时，还应当建立制度限制个人信息的使用、存储、发布等。

第四，应当开展个人信息安全影响评估制度及审计制度。

第五，应当建立个人信息安全事件处置与报告制度。

个人信息安全规范

七、《隐私政策》的主要内容及合规要求

本次《规范》相对详细的规定了《隐私政策》的主要内容及合规要求。

主要内容方面，《隐私政策》应当至少包括个人信息控制者的基本情况；收集、使用个人信息的目的，以及目的所涵盖的各个业务功能；各业务功能分别收集的个人信息，以及收集方式和频率、存放地域、存储 期限等个人信息处理规则和实际收集的个人信息范围；对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收 个人信息的第三方类型，以及所承担的相应法律责任；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；等等。

合规要求方面，《规范》对《隐私政策》的文字要求、放置规范、送达方式、更新要求等都作出了明确的规定。

个人信息安全规范

七、《隐私政策》的主要内容及合规要求

总之，《规范》是监管与执法的重要参考依据，对于企业个人信息合规具有重要的指引意义。企业应当根据《网络安全法》及其配套制度的整体规则，并参照《规范》的细则要求，重新梳理个人信息的收集、使用、存储、分享行为，完善内部管理制度，建立内部岗位及人员责任，降低个人信息违规、违法甚至是刑事法律风险。

当然，我们也应该看到，《规范》的很多细节内容，已经突破了《网络安全法》及其配套制度的法定要求，同时也高于国际同行甚至是欧盟的个人信息保护标准，这不但极大的增加了企业的合规及运营成本，而且对于我国互联网产业尤其是大数据产业的发展也具有一定影响。

个人信息安全规范

七、《隐私政策》的主要内容及合规要求

总之，《规范》是监管与执法的重要参考依据，对于企业个人信息合规具有重要的指引意义。企业应当根据《网络安全法》及其配套制度的整体规则，并参照《规范》的细则要求，重新梳理个人信息的收集、使用、存储、分享行为，完善内部管理制度，建立内部岗位及人员责任，降低个人信息违规、违法甚至是刑事法律风险。

当然，我们也应该看到，《规范》的很多细节内容，已经突破了《网络安全法》及其配套制度的法定要求，同时也高于国际同行甚至是欧盟的个人信息保护标准，这不但极大的增加了企业的合规及运营成本，而且对于我国互联网产业尤其是大数据产业的发展也具有一定影响。

15

移动互联网应用程序（App）系统权限申请使用

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

App系统权限申请使用

16

针对App申请使用系统权限存在的强制、频繁、过度索权，及捆绑授权、 私自调用权限上传个人信息、敏感权限滥用等典型问题，给出了App申请使用系统权限的基本原则和安全要求，建议App 提供者参考规范App系统权限申请和使用行为，防范因系统权限不当利用造成的个人信息安全风险。

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

App系统权限申请使用

权限申请的原则和要求

1　权限申请基本原则

a) 最小必要原则：仅申请App 业务功能所必需的权限，不申请与App 业务功能无关的权限。

b) 用户可知原则：申请的权限均应有明确、合理的使用场景， 并告知用户权限申请目的。

c) 不强制不捆绑原则：不应强制申请系统权限，不要求用户一次性授权同意打开多个系统权限。

d) 动态申请原则：App 所需的权限应在对应业务功能执行时动态申请。在用户未触发相关业务功能时，不提前申请与当前业务功能无关的权限。

App系统权限申请使用

权限申请的原则和要求

2　权限申请通用要求

a) 权限申请应满足“最小必要”原则，与业务功能无关的系统权限不向操作系统声明.

b) 申请权限时应同步告知权限申请目的，目的应明确且易于理解， 不包含广告及任何欺诈、诱骗、误导用户授权的描述。

c) App（包括嵌入的SDK）申请所需权限，应在声明文件（如AndroidManifest.xml）中严格按照格式规范逐个声明。

d) 如仅需使用权限组中部分权限，不应在权限声明文件中声明同一权限组其他权限，例如当App仅需使用写入日历权限时，不应在AndroidManifest.xml中声明读取日历权限。

App系统权限申请使用

19

权限申请的原则和要求

2　权限申请通用要求

e) 如用户拒绝或撤回授予某服务类型非必要系统权限，App不应强制退出或关闭，且不影响与此权限无关的业务功能使用。

f) 如用户明确拒绝App业务功能所需权限，App不应频繁申请系统权限干扰用户正常使用，除非由用户主动触发功能，且没有该权限参与此业务功能无法实现。“频繁”的形式包括但不限于：

1) 单个场景在用户拒绝权限后，48小时内弹窗提示用户打开系统权限的次数超过1次；

2) 每次重新打开App或使用某一业务功能时，都会向用户索要或提示用户缺少相关系统权限。

App系统权限申请使用

20

权限申请的原则和要求

2　权限申请通用要求

g) 除仅用于安全风控场景外，App不应收集不可变更的唯一设备识别码（如IMEI、MAC地址）。

h)定向推送和用户画像场景下标识用户时，应使用可重置的标识符，且标识符不与可识别用户身份信息或不可变更的唯一设备识别码关联。

i) 如App业务功能所需的权限被用户拒绝且选择禁止后不再提示，当用户再次使用此功能时，宜以不干扰用户的方式（如文字提示）引导用户到系统设置中去开启所需权限。

App系统权限申请使用

权限申请的原则和要求

2　权限申请通用要求

j)　App应尊重用户的权限设置，不应欺骗或强迫用户同意不必要的数据访问，若有可能宜为拒绝授权的用户提供替代解决方案。

k)　内嵌第三方SDK的App，宜要求SDK向App明示申请的系统权限及申请目的。

l)　App宜对内嵌第三方SDK申请使用权限进行审核，确保其申请的权限有业务功能场景对应，且不超过约定的范围。

App系统权限申请使用

权限使用的原则和要求

1　权限使用基本原则

a)　一致性原则：权限的使用应与权限申请时和隐私政策中所描述的目的用途、使用场景和规则相一致。

b)　不扩散原则：App 通过系统权限获得的数据和能力，不应在用户未授权的情况下私自提供给小程序或终端上的其他App 使用。

c)　访问显性化原则：使用系统权限（例如相机、麦克风、位置）获取个人敏感信息时，应采用显性方式提示用户，避免以隐蔽方式收集用户个人信息。

App系统权限申请使用

权限使用的原则和要求

2　权限使用通用要求

a)　权限申请获得授权后，App应仅访问满足业务功能需要的最少个人信息，例如读取日历时，若仅需读取某个日期的日程信息则不应读取其他日期的日程。

b)　权限申请后自动采集个人信息的频率应在实现App业务功能所必需的最低合理频率范围内。

c)　App不应未经用户同意更改其设置的系统权限授权状态，如App更新时自动将用户设置的权限恢复到默认状态。

d)　若系统权限申请目的、使用场景发生变化，应重新告知用户。

App系统权限申请使用

权限使用的原则和要求

2　权限使用通用要求

e)　当App对外提供的接口涉及个人信息，且操作系统定义的权限无法达到目的时，App应通过自定义权限对访问个人信息的对外交互组件设置合理的访问权限。

f) App自定义权限应严格按照操作系统权限要求定义和命名，确保完整、清晰、准确，并为权限配置合理的保护级别。

g)　以下操作应由用户主动触发，并在用户知情情况下执行：

1)　执行拨打电话、发送短信等操作；

2)　打开或关闭Wi-Fi、蓝牙、GPS等；

3)　拍摄、录音、截屏、录屏等；

4)　读写用户短信、联系人等个人信息。

App系统权限申请使用

权限使用的原则和要求

2　权限使用通用要求

h)　不应隐蔽收集个人信息，当录音、拍摄、录屏、定位等敏感功能在后台执行时，应采用显著方式（如图标闪烁、状态栏提示、自定义提示条等）提示用户。

i)　不应在用户不知情或未授权的情况下，通过隐蔽方式读取并上传剪切板中包含的个人信息和公共存储区中的个人信息。

j)　如操作系统支持，App申请相机、位置、麦克风等可收集个人敏感信息的权限宜提供用户选择临时单次授权。

k)　提供小程序接入平台的App，宜要求小程序向接入平台说明申请的系统权限及申请目的。

l)　提供小程序接入平台的App应为小程序提供权限管理的功能， 小程序应允许用户关闭或撤回对小程序可收集个人信息权限的授权。

安卓系统典型权限的申请和使用要求

1　日历权限（CALENDAR）
2　通话记录权限（CALL_LOG）
3　相机权限（CAMERA）
4　通讯录权限（CONTACTS）
5　位置权限（LOCATION）
6　麦克风权限（MICROPHONE）
7　电话权限（PHONE）
8　传感器权限（SENSORS）
9　短信权限（SMS）
10　存储权限（STORAGE）

27

移动互联网应用程序（App）中
第三方软件开发工具包（SDK）安全

App中 SDK 安全

28

第三方软件开发工具包（SDK）被广泛应用于各 类移动互联网应用程序（App）的开发中，由第三方SDK带来的安全问题已经引起多方关注。2020年央视“3.15”晚会曝光了第三方SDK违法违规收集用户个人信息的问题，在社会上引起了强烈反响。

针对当前第三方SDK使用过程中存在的第三方SDK自身安全漏洞、恶意第三方SDK、第三方SDK违法违规收集App用户的个人信息等问题，结合当前移动互联网技术及应用现状，给出了App提供者、第三方SDK提供者针对第三方SDK安全问题的实践指引，旨在减少因第三方SDK造成的App安全与个人信息安全问题。

App中 SDK 安全

第三方 SDK 概述

软件开发工具包（Software Development Kit，简称SDK）是指辅助开发某一类软件的相关文档、范例和工具的集合。第三方SDK是指由第三方服务商或开发者提供的实现软件产品某项功能的工具包，通常不包括企业自己开发的仅供自己使用的通用功能模块。

当前，第三方SDK被广泛应用于各类App的开发中。按所提供的功能划分，常见的第三方SDK有框架类、广告类、推送类、统计类、地图类、社交类、支付类、客服类等。按来源划分，可大致分为第三方服务商提供类和开源社区提供类，开源社区提供的第三方SDK又可分为有明确开发主体和无明确开发主体。

App中 SDK 安全

第三方 SDK 概述

第三方SDK将实现特定功能的代码进行封装，向App提供者提供简单的调用接口，使App提供者不必关心所需功能的具体代码实现便能使用相关功能，极大地简化了App开发和运营的过程，提高了App 开发和运营的效率。但也正因为如此，第三方SDK自身的行为具有较强的隐蔽性，其所造成的安全问题不易被察觉。此外，一款第三方SDK 可能会被多款App集成，因此一旦该SDK出现安全问题，就会影响多款App及其用户。

App中 SDK 安全

第三方 SDK 安全问题

1 第三方 SDK 自身安全漏洞
2 恶意第三方 SDK
3 第三方 SDK 违法违规收集 App 用户的个人信息

App中 SDK 安全

措施和建议

建议App提供者、第三方SDK提供者针对第三方SDK安全问题进行排查，评估相关安全风险，并优化安全防护策略。

1 对 App 提供者
2 对第三方 SDK 提供者

App中 SDK 安全

措施和建议

建议App提供者、第三方SDK提供者针对第三方SDK安全问题进行排查，评估相关安全风险，并优化安全防护策略。

1 对 App 提供者
2 对第三方 SDK 提供者

App中 SDK 安全

关于告知要求

第三方 SDK 提供者在采集使用用户个人信息前，应向用户明示其收集使用个人信息的目的、方式与范围、调用权限的类型与目的， 并征得用户同意。如涉及信息回传或分享等行为，也应当告知用户。

35

个人信息去标识化

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

36

《网络安全法》要求

第十八条 国家鼓励开发网络**数据安全保护**和**利用**技术，促进公共数据资源**开放**，推动技术创新和经济社会发展。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，**经过处理无法识别特定个人且不能复原的除外。**

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 35273—2017

信息安全技术　个人信息安全规范

Information security technology—Personal information security specification

2017-12-29 发布　　2018-05-01 实施

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

“匿名化”出现6次
“去标识化”总计出现12次

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。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

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。

5.4　征得授权同意的例外

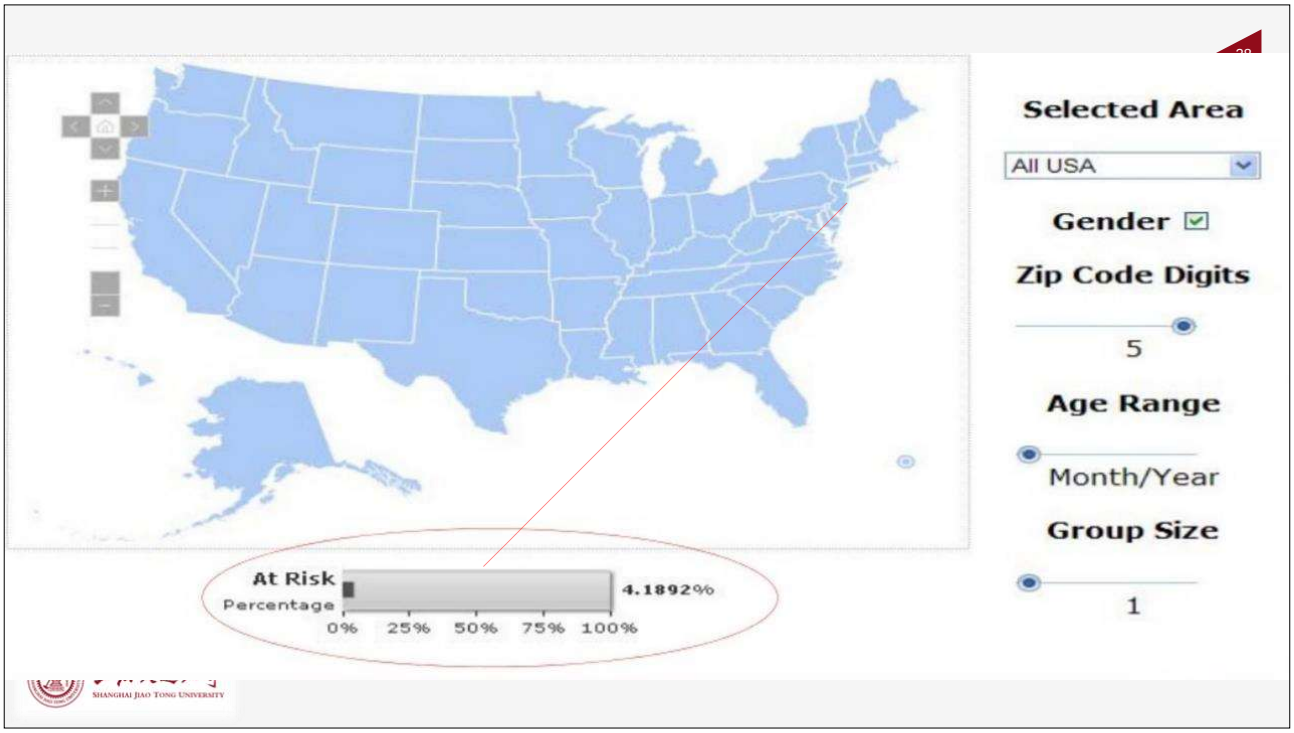
j）个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；

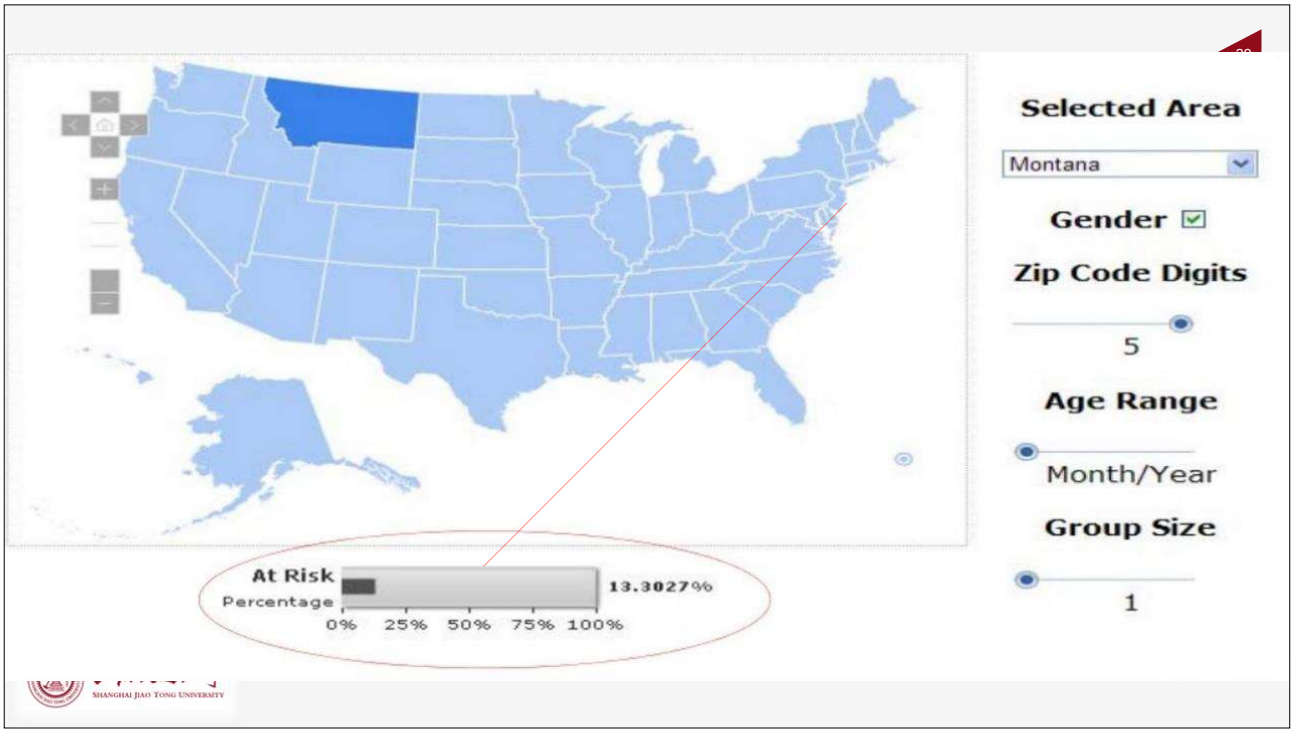
6.2　去标识化处理

收集个人信息后，个人信息控制者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。

8.2　个人信息共享、转让

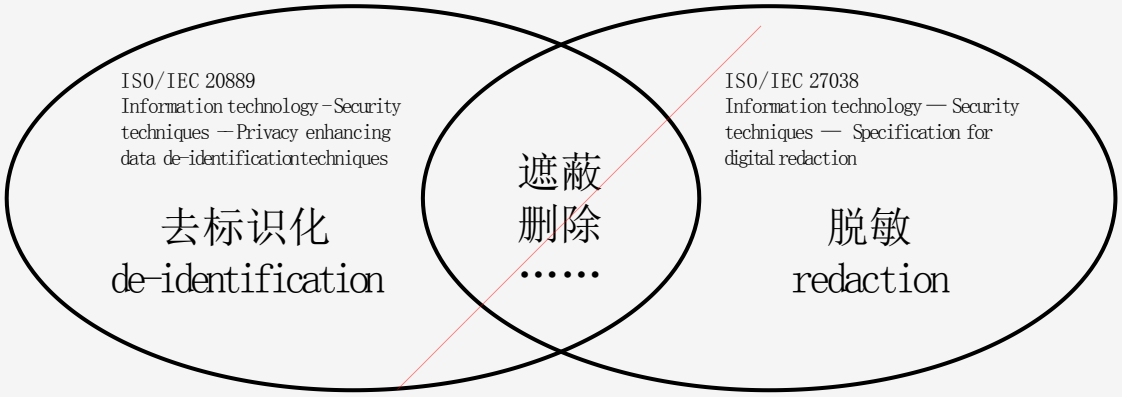
b）向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别个人信息主体的除外；





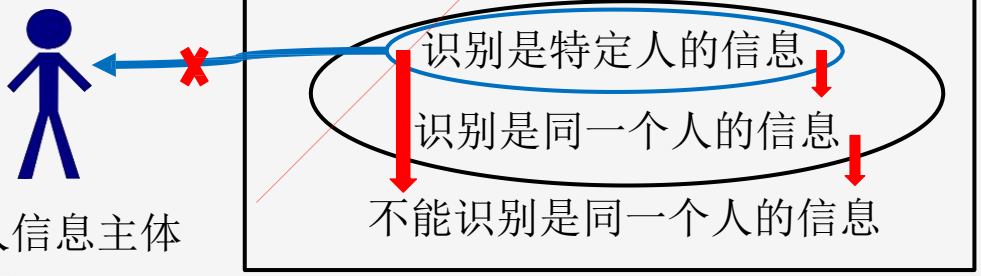
40

去标识化与脱敏的区别



去标识化核心任务

- 降低区分度
- 断开和个人信息主体的关联



常用去标识化技术和模型

统计	加密	抑制
假名	泛化	随机
合成	K 匿名	差分隐私

统计技术（Statistical techniques）

- 数据抽样（Sampling）
  - 因为是部分数据，无法确定主体是否被抽中
- 数据聚合（Aggregation）
  - 统计结果，无个体信息

密码技术（Cryptographic techniques）

- 确定性加密（Deterministic encryption）
- 保序加密（Order-preserving encryption）
- 保留格式加密（Format-preserving encryption）
- 同态加密（Homomorphic encryption）
- 同态秘密共享（Homomorphic secret sharing）

45

抑制技术（Suppression techniques）

- 屏蔽（Masking）
- 局部抑制（Local suppression）
- 记录抑制（Record suppression）

440524188*****0014

Age (Years)	Gender	ZIP Code	Diagnosis
	Male	00000	Diabetes
21	Female	00001	Influenza
36	Male		Broken Arm
	Female		Acid Reflux

46

假名化技术（Pseudonymization techniques）

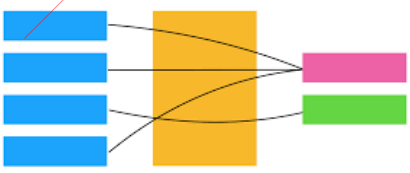
- 独立于标识符的假名创建
- 基于密码技术的标识符派生假名创建

Original Data

Name	SSN	Salary
Smith	123-21-9812	$77,000
Patel	992-43-3421	$83,500

Masked Data

Name	SSN	Salary
Young	531-51-5279	$79,250
Lopez	397-70-0493	$81,250



泛化技术（Generalization techniques）

- 取整（Rounding）
  - 如果取整基数为10，观察值为7，应将7向上取整至10，概率为0.7，若向下取整至0，概率为0.3。
- 顶层与底层编码（Top and bottom coding）
  - 如果一个人的薪水非常高，则可将该用户的薪水值设置为“高于X元”

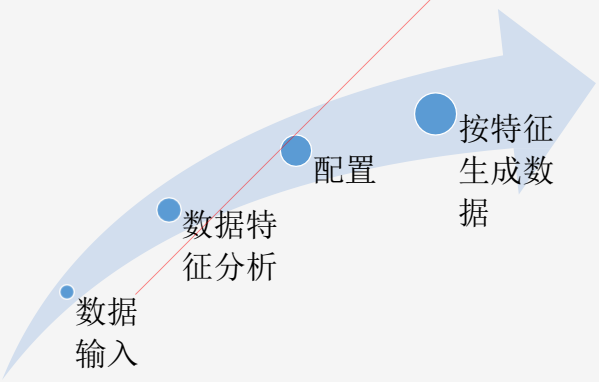
随机化技术（Randomization techniques）

- 噪声添加（Noise addition）
- 置换（Permutation）
- 微聚集（Microaggregation）

Identifier	Gold	System	TP	FN	Sensitivity
Alpha-Numeric-Id	4165	**NLM-S**	4163	2	**1.000 (0.998,1.000)**
		MITdeid	1444	2721	0.347 (0.334,0.359)
		MIST	4091	74	0.982 (0.977,0.986)
Address	292	NLM-S	244	48	0.836 (0.769,0.888)
		MITdeid	129	163	0.442 (0.371,0.510)
		MIST	250	42	**0.856** (0.791,0.905)
Date	29134	NLM-S	28823	311	0.989 (0.984,0.992)
		MITdeid	27595	1539	0.947 (0.942,0.951)
		MIST	28906	228	**0.992 (0.988,0.994)**
PHI	33591	**NLM-S**	33390	201	**0.994 (0.992,0.995)**
		MITdeid	29347	4244	0.874 (0.868,0.879)
		MIST	33310	281	0.992 (0.988,0.994)

数据合成技术（Synthetic data）

- 根据需要，按照原始数据的特征生成数据



K-匿名模型（K-anonymity model）

- K-匿名模型要求发布的数据中，指定标识符（直接标识符或准标识符）属性值相同的每一等价类至少包含K 个记录，使攻击者不能判别出个人信息所属的具体个体，从而保护了个人信息安全。

- L-多样性（L-diversity）
- T-接近性（T-closeness）

年齢	性別	住所	医療費
25	女	横浜市	5,000
28	女	横浜市	1,000
26	男	府中市	800
28	男	府中市	2,000
32	男	川崎市	10,000
32	男	川崎市	6,000
33	男	川崎市	8,000
37	女	青梅市	2,000
38	女	府中市	15,000
43	女	川崎市	30,000
44	女	横浜市	20,000
46	男	港区	3,000
49	男	港区	100,000

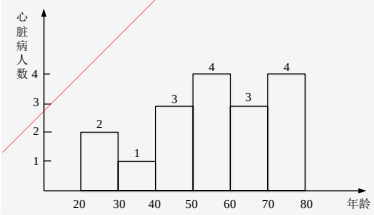
k-匿名化
(k = 2)

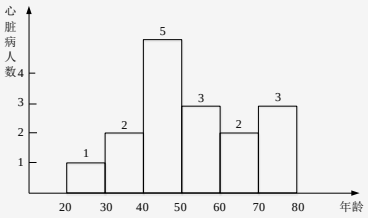
年齢	性別	住所	医療費
25-29	女	神奈川	5,000以下
25-29	女	神奈川	5,000以下
25-29	男	東京	5,000以下
25-29	男	東京	5,000以下
30-34	男	神奈川	5,000-10,000
30-34	男	神奈川	5,000-10,000
30-34	男	神奈川	5,000-10,000
35-39	女	東京	15,000以下
35-39	女	東京	15,000以下
40-44	女	神奈川	20,000-30,000
40-44	女	神奈川	20,000-30,000
45-49	男	東京	100,000以下
45-49	男	東京	100,000以下

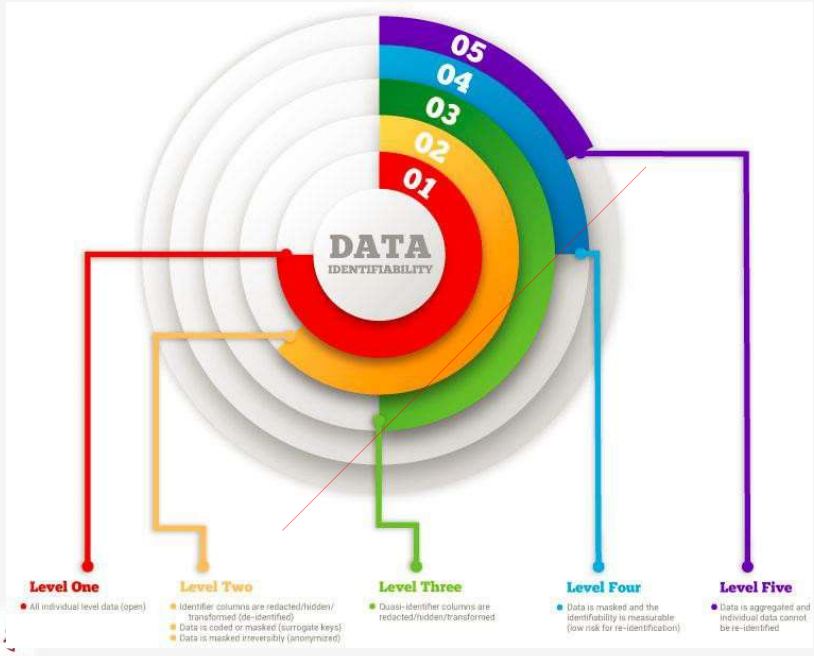
差分隐私模型（Differential privacy model）

- 差分隐私确保数据集中任何特定的个人信息主体的存在与否无法从去标识化数据集或系统响应中推导出。
  - 服务器模式（Server model）
  - 本地模式（Local model）

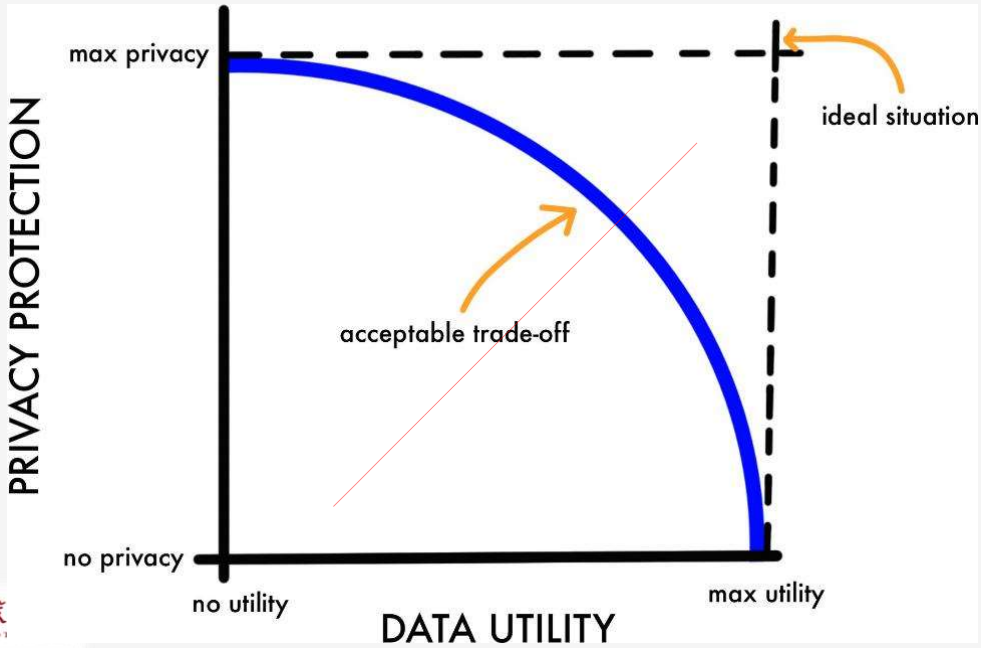
姓名	年龄	心脏病
Alice	31	Yes
Cici	72	No
Dave	46	Yes
Emily	78	Yes
…	…	…







53



54

选择去标识化模型技术

- 是否需要对重标识风险进行量化；聚合数据是否够用；数据是否可删除；
- 是否需要保持唯一性；是否需要满足可逆性；是否需要保持原有数据值顺序；
- 是否需要保持原有数据格式，如数据类型、长度等保持不变；
- 是否需要保持统计特征，如平均值、总和值、最大值、最小值等；
- 是否需要保持关系型数据库中的实体完整性、参照完整性或用户自定义完整性；
- 是否可以更改数据类型，比如在针对字符串类型的“性别”（男/女）进行去标识化时，是否可以变成数字类型表示（1/0）；
- 是否需要满足至少若干个属性值相同，以加强数据的不可区分性；
- 是否可以对属性值实施随机噪声添加，对属性值做微小变化；
- 去标识化的成本约束。
- ……

参数设置

- 美国加拿大重标识阈值一般：0.33
- 默认值：0.2

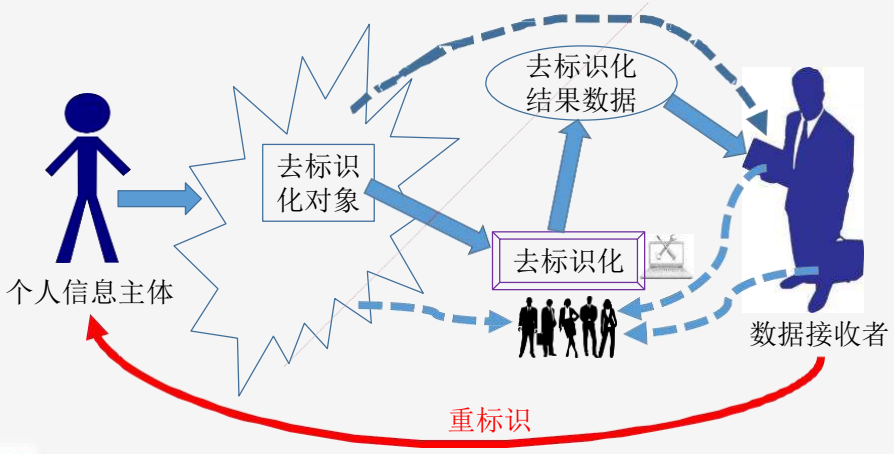
- HIPAA：20K rule
- Census Bureau：100k rule
- Statistics Canada：70k rule
- British census：120k rule

De-identification Maturity Model

Maturity Level		Key Characteristics of De-identification Methodology Used	Implementation Dimension				Automation Dimension	
			I1 Initial	I2 Repeatable	I3 Defined	I4 Measured	A1 Homegrown Automation	A2 Standard Automation
Key De-identification Practice Dimension	P1- Ad hoc	• De-identification is ad-hoc if performed at all • No processes are defined, and there is no consistency across data uses and disclosures		X	X	X		X
	P2 –Masking	• Masking techniques, *including pseudonymization*, are applied to direct identifiers only						
	P3 – Heuristics	• Masking techniques are applied *to* direct identifiers ; Heuristics are applied *to* indirect identifiers						
	P4 – Risk-based	• Masking techniques are applied *to* direct identifiers ; Risk-based methods are used *for* indirect identifiers						
	P5 - Governance	• Masking techniques are applied *to* direct identifiers ; Risk-based methods are used *for* indirect identifiers						

57

去标识化场景



58

结果导向——防范重标识风险

- 重标识方法
  - 分离：将属于同一个个人信息主体的所有记录提取出来。
  - 关联：将不同数据集中关于相同个人信息主体的信息联系起来。
  - 推断：通过其它属性的值以一定概率判断出一个属性的值。
- 重标识攻击
  - 重标识一条记录属于一个特定个人信息主体
  - 重标识一条特定记录的个人信息主体
  - 尽可能多的将记录和其对应的个人信息主体关联
  - 判定一个特定的个人信息主体在数据集中是否存在
  - 推断和一组其它属性关联的敏感属性

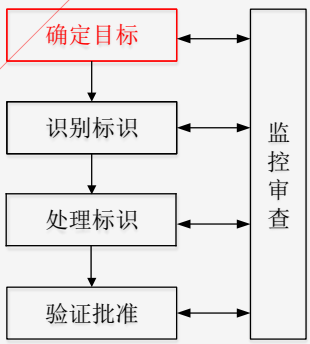
去标识化过程—确定目标

确定去标识化对象

建立安全目标

- 重标识风险阈值
- 有用性阈值

制定工作计划

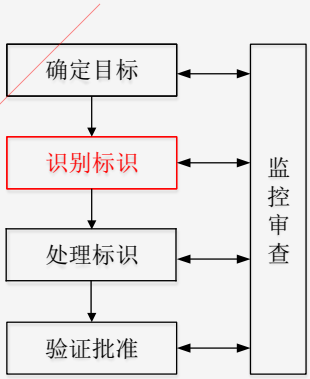


去标识化过程—识别标识

查表识别法

规则判定法

人工分析法



61

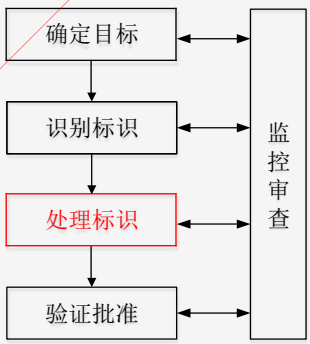
去标识化过程—处理标识

预处理

选择模型技术

- 是否需要对重标识风险进行量化：聚合数据是否够用；数据是否可删除；
- 是否需要保持唯一性：是否需要满足可逆性；是否需要保持原有数据值顺序；
- 是否需要保持原有数据格式，如数据类型、长度等保持不变；是否需要保持统计特征，如平均值、总和值、最大值、最小值等；是否需要保持关系型数据库中的实体完整性、参照完整性或用户自定义完整性；是否可以更改数据类型，比如在针对字符串类型的“性别”（男/女）进行去标识化时，是否可以变成数字类型表示（1/0）；
- 是否需要满足至少若干个属性值相同，以加强数据的不可区分性；是否可以对属性值实施随机噪声

实施去标识化



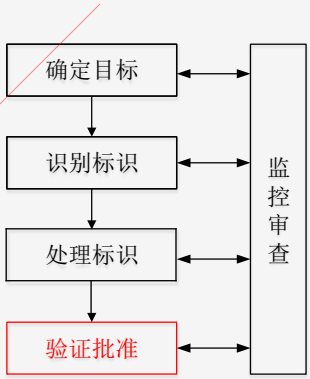
62

去标识化过程—验证批准

验证个人信息安全

验证数据有用性

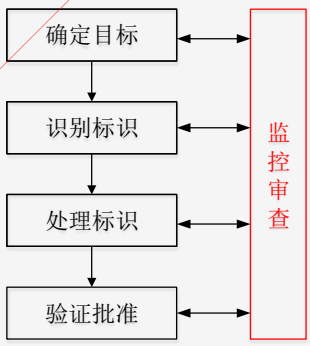
评审批准去标识化工作



63

去标识化过程—监控审查

- 监控审查去标识化步骤
- 持续监控去标识化效果
-



64

去标识化面临的挑战

- 聚合技术的挑战
- 高维数据的挑战
- 关联数据的挑战
- 组合的挑战
- 增量去标识化的挑战

ICS 35.040
L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术
个人信息去标识化指南

Information security technology —

Guide for De-Identifying Personal Information

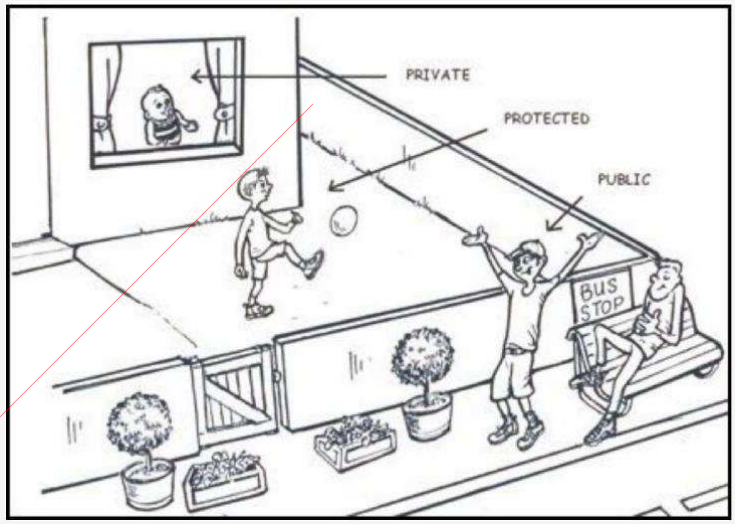
点击此处添加与国际标准一致性程度的标识

（报批稿）

（本稿完成日期：2018 年 5 月 14 日）

XXXX－XX－XX 发布　　XXXX－XX－

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



互联网个人信息安全保护

互联网个人信息安全保护

1、背景

近年来，侵犯公民个人信息的现象日益增多，侵犯公民个人信息的违法犯罪行为也日益猖獗，更为严重的是，此类违法犯罪已经形成了完整的利益链，甚至是灰色产业链，给人们日常生活带来很大的干扰，直至造成财产损失，甚至危及人身安全。随着网络技术的发展，互联网行业持有个人信息的现象日益普遍，侵犯公民个人信息的违法犯罪也与计算机信息系统密切相关。

互联网个人信息安全保护

2、适用范围

范围明确了适用对象为“个人信息持有者”，即对个人信息进行控制和处理的组织或个人，“互联网企业”进一步明确为“通过互联网提供服务的企业”，并且包含了其他“使用专网或非联网环境控制和处理个人信息的组织或个人”，也就是说除了传统意义的互联网企业，也包含金融、电信、交通、教育、医疗等行业，甚至存有大量公民个人信息的房产中介等企业，都在此范畴内。

互联网个人信息安全保护

3、指南与一些法律法规的相关性

《网络安全法》特别加强和明确了个人信息保护方面的要求，指南的业务流程主要要求按照《网络安全法》编制的，一些细化要求参考了推荐性国家标准GB/T 35273—2017《信息安全技术 个人信息安全规范》；

另外，《网络安全法》指出国家实行网络安全等级保护制度，指南的管理要求、技术要求和应急处置，都与《网络安全等级保护基本要求》(《信息系统安全等级保护基本要求》)相一致，履行保护义务，“保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”为目标，这也是《网络安全法》的明确要求。另一方面，是否存在“窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息”等行为，也是检查重点之一。

互联网个人信息安全保护

4、指南与等级保护定级的关系

对于网络安全等级保护级别的要求并非明确为三级。按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”，按照网络安全等级保护基本要求的哪一级进行保护，则是需要经过等级保护定级备案的过程。

这就意味着，根据影响国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的程度，涉及个人信息的数量和类别达到一定规模，仍需按照三级甚至更高级别进行防护。

互联网个人信息安全保护

71

5、指南中的个人信息是否分级

指南中“个人信息”完全引用了《网络安全法》的定义，与国家标准《个人信息安全规范》在个人信息之外还界定一个个人敏感信息不同，指南并不涉及个人敏感信息这个概念。这说明，指南提出的要求，是个人信息保护的最低要求。

互联网个人信息安全保护

72

6、关于匿名化的操作

匿名化是指“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。”这个术语与欧盟GDPR的匿名化说法有所不同。这里直接引用《网络安全法》“经过处理无法识别特定个人且不能复原”的描述。

互联网个人信息安全保护

7、对于用户画像的要求

用户画像是互联网企业最常用的营销手段之一，涉及个人信息该如何合法合规使用是企业非常关心的问题。指南指出，“完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利;如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据”。

App违法违规收集使用个人信息评估

App违法违规收集使用个人信息评估

75

隐私政策的独立性

评估点	评估标准
1. 是否有隐私政策	在App界面中能够找到隐私政策，包括通过弹窗、文本链接、常见问题（FAQs）等形式。
2. 隐私政策是否单独成文	隐私政策以单独成文的形式发布，而不是作为用户协议、用户说明等文件中的一部分存在。
3. 隐私政策是否易于访问	进入 App 主功能界面后，通过 4 次以内的点击，能够访问到隐私政策，且隐私政策链接位置突出、无遮挡。
4. 隐私政策是否易于阅读	隐私政策文本文字显示方式（字号、颜色、行间距等）不会造成阅读困难。

App违法违规收集使用个人信息评估

76

清晰说明各项业务功能及所收集个人信息类型

评估点	评估标准
5.是否明示收集个人信息的业务功能	隐私政策中应当将收集个人信息的业务功能逐项列举，不应使用“等、例如”字样。 注：业务功能是指 App 面向个人用户所提供的一类完整的服务，如地图导航、网络约车、即时通讯、社区社交、网络支付、新闻资讯、网上购物、短视频、快递配送、餐饮外卖、交通票务等；。
6. 业务功能与所收集个人信息类型是否一一对应	隐私政策中对每个业务功能都应说明其所收集的个人信息类型，不应出现多个业务功能对应一类个人信息的情况。
7. 是否明示各项业务功能所收集的个人信息类型	每个业务功能在说明其所收集的个人信息类型时，应在隐私政策中逐项列举，不应使用“等、例如”等方式概括说明。
8. 是否显著标识个人敏感信息类型	隐私政策应对个人敏感信息类型进行显著标识（如字体加粗、标星号、下划线、斜体、颜色等）。 注：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、14 岁以下（含）未成年人的个人信息等。

App违法违规收集使用个人信息评估

清晰说明个人信息处理规则及用户权益保障

14.对外共享、转让、公开披露个人信息规则	如果存在个人信息对外共享、转让、公开披露等情况，隐私政策中应明确以下内容： 1、对外共享、转让、公开披露个人信息的目的； 2、涉及的个人信息类型； 3、接收方类型或身份。
15.用户权利保障机制	隐私政策中应对以下用户操作方法提供明确说明： 1、个人信息查询； 2、个人信息更正； 3、个人信息删除； 4、用户账户注销； 5、撤回已同意的授权。
16. 用户申诉渠道和反馈机制	隐私政策中至少提供以下一种投诉渠道： 1、电子邮件； 2、电话； 3、传真； 4、在线客服； 5、在线表格。
17.隐私政策时效	应明确标识隐私政策发布、生效或更新日期。
18.隐私政策更新	如果发生业务功能变更、个人信息出境情况变更、使用目的变更、个人信息保护相关负责人联络方式变更等情形时，隐私政策应进行相应修订，并通过电子邮件、信函、电话、推送 通知等方式及时告知用户。

App违法违规收集使用个人信息评估

不应在隐私政策等文件中设置不合理条款

评估点	评估标准
19. 隐私政策等文件是否存在免责等不合理条款	App 运营者不应在用户协议、服务协议、隐私政策等文件中出现免除自身责任、加重用户责任、排除用户主要权利条款。 注：免除自身责任是指App 运营者免除其依照法律规定应当负有的强制性法定义务； 加重用户责任是指App 运营者要求用户在法律规定的义务范围之外承担责任或损失； 排除用户主要权利是指App 运营者排除用户依照法律规定或者依照合同的性质通常应当享有的主要权利。

App违法违规收集使用个人信息评估

收集个人信息应明示收集目的、方式、范围

评估点	评估标准
20.是否向用户明示收集、使用个人信息的目的、方式、范围	1、在用户安装、注册或首次开启App时，应主动提醒用户阅读隐私政策。 2、当 App 打开系统权限时（不包括用户自行在系统设置中打开权限的情况），App应当说明该权限将收集个人信息的目的。 3、收集个人敏感信息时，App应通过弹窗提示等显著方式向用户明示收集、使用个人信息的目的、方式、范围。
21.若使用Cookie及其同类技术收集个人信息，是否向用户明示	当使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie 内嵌 Web 链接、sdk 等）收集个人信息时，应向用户明示所收集个人信息的目的、类型。
22.若存在嵌入第三方代码插件收集个人信息的功能，是否向用户明示	如果通过嵌入第三方代码、插件等方式将个人信息传输至第三方服务器，应通过弹窗提示等方式明确告知用户。

App违法违规收集使用个人信息评估

收集使用个人信息应经用户自主选择同意，不应存在强制捆绑授权行为

评估点	评估标准
23．收集个人信息前是否征得用户自主选择同意	App收集个人信息前应提供由用户主动选择同意或不同意的选项，不同意应仅影响与所拒绝提供个人信息相关的业务功能。
24.是否存在将多项业务功能和权限打包，要求用户一揽子接受的情形	1、不应通过捆绑App多项业务功能的方式，要求用户一次性接受并授权同意多项业务功能收集个人信息的请求。 2、根据用户主动填写、点击、勾选等自主行为，作为产品或服务的业务功能开启或开始收集个人信息的条件。

App违法违规收集使用个人信息评估

收集个人信息应满足必要性要求

评估点	评估标准
25. 实际收集的个人信息类型是否超出隐私政策所述范围	各业务功能实际收集的个人信息类型应与隐私政策所描述内容一致，不应超出隐私政策所述范围。
26. 收集与业务功能有关的非必要信息，是否经用户自主选择同意	当 App 运营者收集的个人信息超出必要信息范围时，应向用户明示所收集个人信息目的并经用户自主选择同意。 注 1：必要信息指与基本业务功能直接相关，缺少该信息则基本业务功能无法实现的信息。 注 2：自主选择同意是指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。肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。
27. 是否收集与业务功能无关的个人信息	App 不应收集与业务功能无任何关系的个人信息。
28. 是否在用户明确拒绝后继续索要权限、打扰用户	对于用户明确拒绝使用、关闭或退出的特定业务功能，App不应再次询问用户是否打开该业务功能或相关系统权限。
29.App更新是否更改系统权限设置	App 更新升级后，不应更改原有的系统权限设置。

App违法违规收集使用个人信息评估

支持用户注销账号、更正或删除个人信息

评估点	评估标准
30. 是否支持用户注销账号	App 应提供注销账号的途径（如在线功能界面、客服电话等），并在用户注销账号后，及时删除其个人信息或进行匿名化处理。
31.是否支持用户查询、更正或删除个人信息	App 应提供查询、更正、删除个人信息的途径。

App违法违规收集使用个人信息评估

及时反馈用户申诉

评估点	评估标准
32.是否及时反馈用户申诉	App 运营者应妥善受理并及时反馈用户申诉，原则上在15天内回复处理意见或结果。

App违法违规收集使用个人信息行为认定方法

App违法违规收集使用个人信息

近年来，移动互联网应用程序（App）发展迅速，在促进经济社会的发展、服务民生等方面发挥了不可替代的作用。同时，App强制授权、过度索权、超范围收集个人信息的现象大量存在。纵观全文，可以发现该《认定方法》共有六大认定方面、三十一项具体认定方法，主要适用于界定App运营者违法违规收集使用个人信息的行为，为监督管理部门认定App违法违规收集使用个人信息行为提供参考，为App运营者自查自纠和网民社会监督提供指引。

App违法违规收集使用个人信息

在隐私政策方面，主要涉及文件中的第一、第二及第四条认定标准。对App中有无隐私政策、首次运行时的提醒方式、个人信息的权限、访问及阅读时的难易程度进行了认定。总体概括来说，运营者实行告知行为的时间点应为用户安装、首次使用App以及新的信息收集使用方式或更新的隐私政策正式实施之前，主要以弹窗或链接的方式对用户进行告知，隐私政策等收集使用规则应易访问易阅读，应收集与其提供的服务有关的个人信息，并明示收集使用个人信息的目的、方式和范围。此外，还强调了个人敏感信息的保护力度，提出在每次需要用户提供个人敏感信息时皆应同步实时说明原因。

App违法违规收集使用个人信息

87

取得用户同意是目前我国App运营者降低违法违规风险的重要方式。文件的第三大认定标准中涵盖9条未取得用户同意而收集使用个人信息的违法违规行为，第五大认定标准涵盖3条未经同意向他人提供个人信息的违法违规行为。概括来说，运营商应在收集前提前告知用户、用户必须明确同意才可收集相关信息及向他人提供其个人信息。同时，值得关注的是《认定方法》提出，运营商应提供非定向推送信息的选项，设置可撤回同意收集个人信息的途径。

App违法违规收集使用个人信息

88

文件中的认定了标准：“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”。对此，运营者应提供有效的更正、删除个人信息及注销用户账号功能，并且及时响应用户相应操作、App后台及时完成、建立并公布个人信息安全投诉、举报渠道，15个工作日内受理并处理。

App违法违规收集使用个人信息

89

此《认定方法》的出台，进一步明确了App违法违规收集使用个人信息行为的认定，广大App运营者应根据法律法规要求，主动自查自纠，规范个人信息收集使用行为。同时，对 APP的使用者来说，应切实对APP进行监督，提升个人信息保护水平，维护好自身的权益。

App违法违规收集使用个人信息

90

1月8日，工业和信息化部信息通信管理局通报第二批侵害用户权益行为的App名单，15款产品在列。

第一批未按要求完成整改的企业，已依法组织下架。

存在问题的应用软件名单（第二批）

序号	软件名称	企业名称	版本	版本来源	所涉问题
1	拉勾招聘	北京拉勾网络技术有限公司	7.31.0	应用宝	私自收集个人信息
2	天涯社区	天涯社区网络科技股份有限公司	6.9.7	官网	不给权限不让用 过度索取权限
3	风行视频	北京风行在线技术有限公司	3.6.1.1	应用宝	不给权限不让用
4	一点资讯	北京一点网聚科技有限公司	5.2.1.0	应用宝	私自收集个人信息 私自共享给第三方 过度索取权限
5	飞贷	深圳中兴飞贷金融科技有限公司	6.3.9	应用宝	不给权限不让用
6	云南招考	云南尚强科技文化有限公司	2.1.4	应用宝	私自收集个人信息 不给权限不让用
7	茶山闹钟	苏州世纪飞越网络信息有限公司	2.5	应用宝	私自共享给第三方 账号注销难
8	爱青岛	青岛市广播电视台	5.2	应用宝	私自收集个人信息 私自共享给第三方 账号注销难
9	江油都市网	江油阳光都市网络科技有限公司	4.7.6	应用宝	私自收集个人信息 不给权限不让用
10	快提款	厦门极铂互动网络科技有限公司	1.0.8	应用宝	私自共享给第三方
11	男衣库	深圳高飞传媒有限公司	3.0.28	应用宝	私自收集个人信息 私自共享给第三方 过度索取权限
12	知米背单词	杭州蓝猫教育科技有限公司	4.9.7	应用宝	私自收集个人信息 私自共享给第三方 不给权限不让用 账号注销难
13	luckin coffee	瑞幸咖啡信息技术（厦门）有限公司	3.2.2	应用宝	私自收集个人信息
14	绿城生活	绿城物业服务集团有限公司	4.9.1	应用宝	私自收集个人信息 私自共享给第三方
15	金榜网校课服版	上海金榜教育培训有限公司	2.2.3	应用宝	私自共享给第三方 强制用户使用定向推送功能

App违法违规收集使用个人信息

91

第一部分

主要是针对隐私政策的，严格要求APP中必须要有隐私政策，且隐私政策中要包含收集使用个人信息规则的条目，在首次运行时必须通过弹窗等明显方式提示用户阅读隐私政策。同时，隐私政策要容易访问，容易阅读，文字大小适中，颜色刚好，像之前看到的苏宁、微信的都是比较好的典范。

一、以下行为可被认定为“未公开收集使用规则”

1.在App中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

2.在App首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

3.隐私政策等收集使用规则难以访问，如进入App主界面后，需多于4次点击等操作才能访问到；

4.隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

App违法违规收集使用个人信息

92

第二部分

主要是针对个人信息的目的、方式和范围的。要求必须一一列出这几点，且在发生变化时，要采用更新隐私政策提醒用户阅读等适当的形式通知用户，比如更新之后需要弹出隐私政策让用户确认同意才可继续使用。如果涉及到敏感信息收集需要同步告知用户目的，必须明确、简单直观。不仅如此，收集使用规则的内容也必须简单直观，容易理解，不得使用大量专业术语让用户难以理解。

二、以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1.未逐一列出App(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等；

2.收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；

3.在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

4.有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

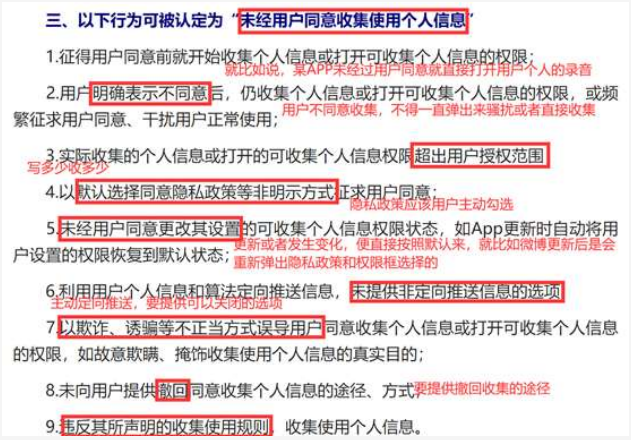
上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

App违法违规收集使用个人信息

93

第三部分

是用户同意收集使用个人信息。这里面有几点比较重要，一点是用户必须明确同意才能够收集，也不得干扰用户和直接收集，第二点是不能超出收集范围，更新或者发生变化时需要用户重新选择更改或者设置权限状态，第三点是隐私政策应该用户主动勾选而不得直接默认同意，不得诱骗误导用户非法收集，或者违反规则收集，同时要提供撤回收集的途径。

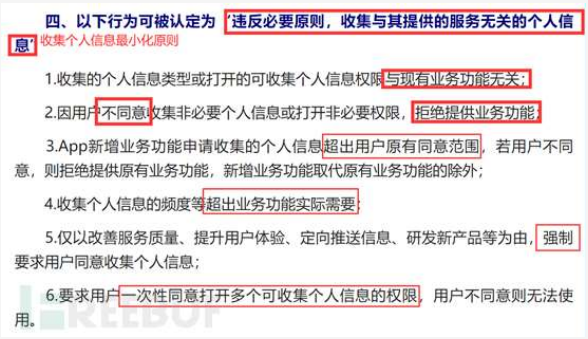


App违法违规收集使用个人信息

94

第四部分

针对收集个人信息最小化原则，最主要的一点是用户不同意收集非必要个人信息或者打开非必要权限或者一次性打开多个收集权限时，拒绝提供业务功能的，就好比如说，不同意某个APP的位置权限，然后就闪退掉了，这就是违法行为了。而且不得强制要求用户收集个人信息，仅仅因为服务质量用户体验等原因。



App违法违规收集使用个人信息

第五部分

是关于第三方提供个人信息的，表明要向第三方提供用户个人信息需要经过用户同意，而且要做匿名化处理，不然像很多用户个人信息泄露就是因为这样，一个地方传到另一个地方，同时也不可以直接数据传输到后台供第三方收集。其次，接入第三方应用时，也要明确告知用户，征求同意才可提供个人信息。

五、以下行为可被认定为“未经同意向他人提供个人信息”

1.既未经用户同意，也未做匿名化处理，App客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；

2.既未经用户同意，也未做匿名化处理，数据传输至App后台服务器后，向第三方提供其收集的个人信息；

3.App接入第三方应用，未经用户同意，向第三方应用提供个人信息。

App违法违规收集使用个人信息

第六部分

是针对用户注销删除个人信息和投诉举报两个部分，要求企业必须提供有效的更正、删除个人信息和注销账号的功能，不得设置不必要或不合理条件，提供了同时还要及时响应，需要人工处理的话要规定时限且不得超过。后台要随时保持跟进操作行为。

企业同时要建立和公布个人信息安全投诉和举报渠道，要承诺时限且在规定时限内完成。

六、以下行为可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”

1.未提供有效的更正、删除个人信息及注销用户账号功能；

2.为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

3.虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理；

4.更正、删除个人信息或注销用户账号等用户操作已执行完毕，但App后台并未完成的；

5.未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）受理并处理的。

97

个人金融信息保护技术规范

个人金融信息保护技术规范

98

个人金融信息保护技术规范

99

《规范》将个人金融信息按敏感程度、泄露后造成的危害程度，从高到低分为C3、C2、C1三个类别；同时，规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

个人金融信息保护技术规范

100

规范作用

有助于规范金融业机构个人金融信息保护工作，提升金融数据风险防控能力，促进我国金融市场的健康发展；

有助于提高金融机构个人账户信息、银行卡信息安全管理水平，加大互联网交易风险防控力度，防范各类金融交易风险，切实维护金融稳定，保护金融消费者合法权益。

个人金融信息保护技术规范

101

适用机构

《规范》适用的主体包括两大类：金融机构和获取个人金融信息的非金融机构。

金融机构

- 商业银行、城市信用合作社、农村信用合作社、邮政储汇机构、政策性银行
- 证券公司、期货经纪公司、基金管理公司
- 保险公司、保险资产管理公司
- 信托投资公司、金融资产管理公司、财务公司、金融租赁公司、汽车金融公司、货币经纪公司
- 中国人民银行确定并公布的其他金融机构

非金融机构

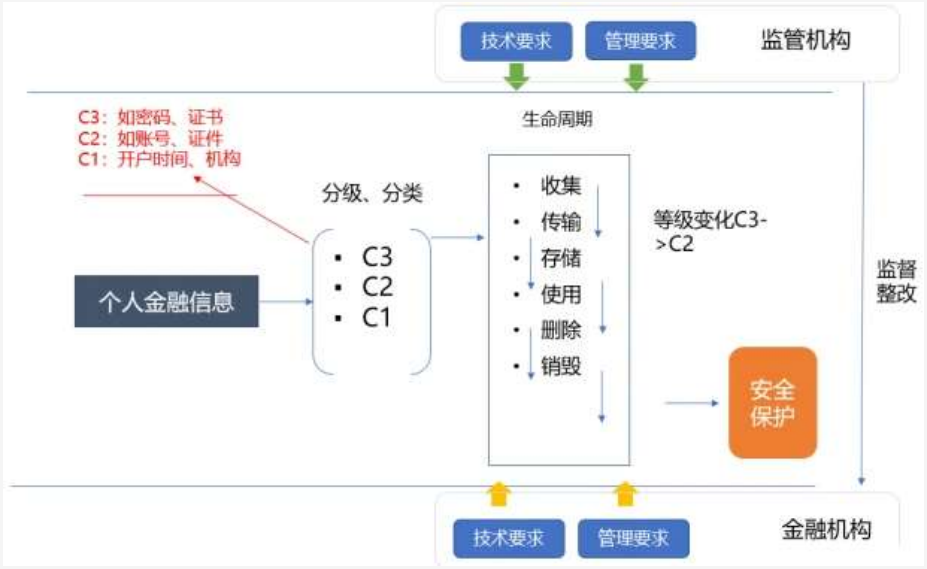
- 第三方支付机构
- 提供代管资金
- 证券或其他资产
- 代管银行账户
- 证券账户等金融服务的机构
- 及其他外包服务机构

上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

个人金融信息保护技术规范

102

整体内容架构



上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

个人金融信息保护技术规范

103

个人金融信息分类分级

个人金融信息保护技术规范

104

生命周期技术要求

01 信息收集
02 信息传输
03 信息存储
04 信息使用
05 删除与销毁

个人金融信息保护技术规范

安全运行技术要求

网络安全要求：承载与处理个人金融信息的信息系统应满足国家等级保护及金融行业等级保护的基本要求，并且存储个人金融信息的数据库应处于金融业机构可控网络内，设置有效的访问控制措施。

WEB应用和客户端软件安全要求：C2/C3类别信息的Web应用应具有防篡改和防web攻击的措施，并具备对处理个人金融信息的系统组件进行实时监测的能力；要求处理个人金融信息相关的 Web 应用系统与组件上线前应进行安全评估。

个人金融信息保护技术规范

安全管理要求重点内容

《规范》的安全管理要求共5大类10个子类，从安全准则、安全策略、访问控制、安全监控和风险评估、安全事件处置五方面进行了安全管理要求。重点包括对个人金融信息收集、存储、使用的安全管理要求，对个人金融信息安全管理的制度、组织、人员、访问控制、安全事件的安全管理要求。

个人金融信息保护技术规范

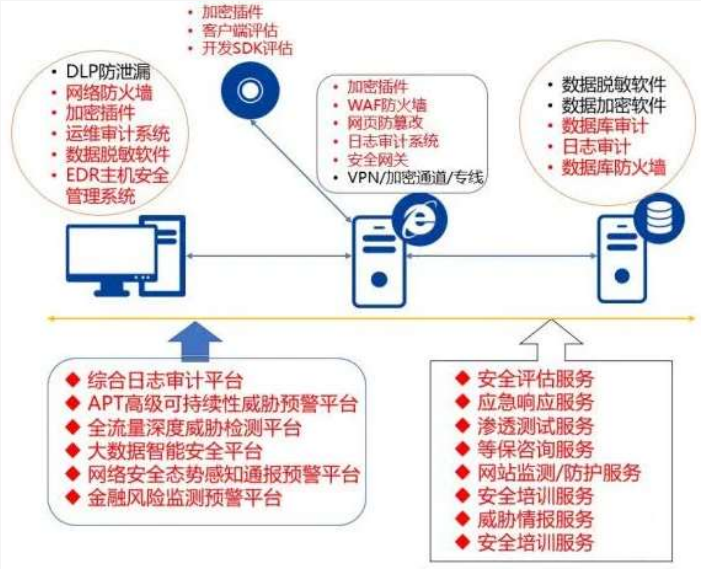
107

个人金融信息保护技术规范

108

个人金融信息生命周期技术防护体系

个人金融信息保护技术规范



个人金融信息技术防护架构

个人金融信息保护技术规范

个人金融信息保护工作开展流程