科技伦理风险

大型网络平台

个人信息保护负责人

标识符

数据法词典

计算机信息系统安全专用产品

自动化决策

数据出境

个人金融信息

个人信息

工业和信息化领域数据

个人信息泄露

委托处理

生成式人工智能技术

DLawHub
知识库

-= 前言 =-

记得高中时期，看过一部电影叫做《编舟记》，讲述了一位出版社员工因为机缘巧合转岗去了辞典编辑部，并花费十五年的时间编纂了一本新时代辞典。故事很简单，也很淡，没有大起大落的激烈冲突，也没有拯救世界的宏大叙事，甚至也没有同名动画中奇幻的特效，只是认认真真地讲述了一本辞典诞生的故事。故事中，男主和三位同事日复一日地埋头于文字之间。但这部电影却深深地扎根在了我的心中，几乎每年我都会找个时间去重新品味这个故事。

犹记得电影中，老编辑在介绍词典中说过这么一句话："所谓辞典，是横渡词汇海洋的船。人们乘坐辞典这艘船，搜集漂浮在漆黑海面上的点点星光，只为了能用最恰当的措辞准确的把自己的所思所想传达给他人。如果没有辞典，我们只能伫立在这片浩瀚的大海前，裹足不前。"

对于不少初学者和从业者来说，数据法领域也如同一望无尽的大海，从刚踏入这片海域一开始我们就在于各类概念的波涛打交道。如何认识"个人信息"？"关联"说还是"识别"说？"个人信息"与"数据"之间又存在什么样的关系？这些术语不应成为阻碍我们沟通的横沟。

因此，我们 DLaw Hub 在今年 5 月份的时候启动了《数据法词典》的编纂项目。在此之前，已有很多前辈们做出了很多的贡献与成果。例如华东政法大学数据法律研究中心搭建的"数据百科"网站、合规社编写的《105 个数据安全必备词汇》文章、国家市场监督管理总局和标准化管理委员会制订的《信息安全技术 术语》与《信息技术 人工智能 术语》。与此同时，在过去的两年中，我们 DLaw Hub 也先后启动过"数据法大词库"、"一卡识数"等项目。

但我们 DLaw Hub 的小伙伴们仍觉得意犹未尽。我们的律师同学认为在将法条适用于现实案例的过程中，经常需要查阅和分析一些重点概念的含义，因此需要有一个集中的词典提高检索的效率；法务同学会觉得一些概念在不同的语境下会触发不同的法律义务，因此希望对于某些词语有更加全景式的了解；我们的一些青年研究者同学则有感于各种相似概念之间的关系的混乱，希望通过一本词典来帮助大家厘清各类相似概念的内涵与外延，并努力构建出共识；而作为 DLaw Hub 的运营者，我们也期待构建起一个便于大家检索又能与时俱进的工具，在帮助大家敲开数据法大门的同时，也能成为了解我们知识库的新入口。

为此，我们在编纂本次《数据法词典》的过程中，整理了目前散落在各片海域中零散的概念解释，基于编纂组的经验与理解，为这些概念提供更加多维度和贴近实务的注解。并且，我们还通过这些概念串联起了 DLaw Hub 知识库中的各个板块和文章。

在呈现方式上，我们将打破传统纸质文本的限制，通过互联网和人工智能技术，让各位朋友可以离我们的词典更近一步。除了本报告外，我们此次编写的辞典还为大家提供另外三种不同的使用方式：

1. 我们使用飞书的词库功能，将词典融入 DLaw Hub 知识库中。大家在使用飞书知识库时如果遇到了有些词语下方出现了下划线，则能点击阅读我们对该词语编写的解释；

2. 我们将词典做成了查阅页面，大家输入关键词，直接查询相关词语。详情可以点击链接使用：数据法词典（检索版）

3. 我们还借助豆包大模型的技术，在 Coze 上搭建了 AI 版的“数据法词典”，由词典小精灵为大家答疑解惑。点击链接使用：数据法词典（AI 版）

非常感谢这半年来工作组小伙伴们给我提供的帮助。本次的工作只是我们词典项目的开始，未来我们会跟进中国数据法的发展，调整词语的注解，补充新生的概念，并会进一步发布不同细分领域的全量词典。

我们也相信，在不久的将来，中国官方也会发布更加权威的名词解释，帮助大家征服这片精彩的大海。

DLawhub 小伙伴们

2024 年 12 月 12 日

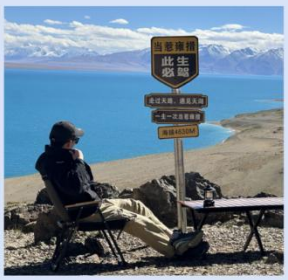
-= 作者 =-

养兔子的好人

往前去见证历史的岁月激荡，
往后去开拓人类空间的边疆。
不愿被重力束缚灵魂的少年。

吃饺子必蘸番茄酱

脚踏实地，仰望星空。

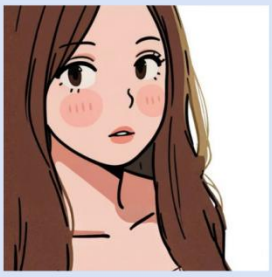


郑书康

控制自己的风向，
减少无谓的磨损。

Sonne

梦里只有诗酒和光影的年华，
往事有底片为证。



emo 瑶

不要因为别人交卷
就乱写答案

章渝昕

尽人事，听天命。

布螺丝

功不唐捐

曾晓洋

要一直迈步，阔步；
要扬帆，要撑桨。

善良萨摩耶

学！

金鱼

把向往的地方，变成走过的路

-= 一卡识数 =-

一卡识数是我们 2024 年新开展的日常项目，希望用一张小小的卡片为大家介绍相关的术语和概念，并且串联起数据法知识的大厦。目前我们已经累计了 9 张卡片。

对于每个词语，我们会深入解读起定义、概念的缘起和流变、相关的重要事件与案例、与相近词语的辨析、配套的法律制度和规定，以及目前尚待解决的问题。

本章节特别感谢李俐青、李诗、李泳江的协助。

DLaw Hub 知识库拓展资料：一卡识数

李俐青

一个努力挖掘真实世界的小法师。

李诗

欲买桂花同载酒，
仍道似，少年游。

李泳江

跑，跑，跑，
在每一个步伐中感受心脏的跳动

匿名化

- **定义**：个人信息经过处理无法识别特定自然人且不能复原的过程
- **源起与流变**：最早关于匿名化的表述可见2016年《网络安全法》第42条第1款。此后在《民法典》第1083条第1款中亦出现类似的表述。在《个人信息保护法》第4条、第73条中首次提出“匿名化”并进行定义
- **近义词**：去标识化、假名化
- **概念对比**：再识别、重标识
- **重要事件**：“AOL事件”“Netflix事件”

- **法律制度**：匿名化概念的诞生是基于保护个人信息的需要
- **相关待解决的问题/领域**：去标识化的程度、数据交易/出境中的个人信息保护
- **锐评**：技术靠不住！！！

匿名化

关键信息基础设施

- **定义**：公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。
- **源起与流变**：《网络安全法》（2017-06-01）第31条第一次对关键信息基础设施进行规定，并颁布了专门的行政法规《关键信息基础设施安全保护条例》（2021-09-01），在第2条中使用了类似的表述进行定义。
- **近义词**：关键基础设施
- **相对概念**：关键信息基础设施运营者、网络产品和服务

- **重要事件**：美光事件，美国燃油运输管道事件
- **法律制度**：网络安全审查、数据安全审查、数据出境
- **相关待解决的问题/领域**：关基的划分、边界
- **锐评**：保护关基，保护你我他

关键信息基础设施

目的限制原则

- **定义**：处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。
- **源起与流变**：在《个人信息保护法》之前，关于个人信息收集、使用的原则主要是合法、正当、必要以及目的明确原则。参考GDPR等域外法，《个保法》中引入了目的限制原则，而关于个人信息的八大原则不仅适用在“收集”和“使用”阶段，而是覆盖“处理”个人信息的全周期。
- **法律制度**：个人信息处理、知情同意
- **近义词**：个人信息最小化原则、必要原则

- **事件例举**：比利时某市长滥用个人邮件发送竞选信息案，北京快手科技有限公司、快手直播App不正当竞争案
- **相对概念**：合法、正当、诚信、公开透明、质量、安全原则
- **相关待解决的问题/领域**：目的限制原则的有效性
- **锐评**：学好公法才能学好个保法

目的限制原则

知情同意原则

- **定义**：基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出
- **源起与流变**：知情同意最早来源于医疗领域，其后在个人信息领域逐渐围绕个人信息自决权而形成知情同意原则。随着法律法规的完善，知情同意理论也从原则走向规则

- **近义词**：告知同意、告知选择、选择加入（opt-in）、选择退出（opt-out）
- **相对概念**：明示同意、单独同意
- **事件例举**：百度Cookie第一案、杭州人脸识别第一案
- **法律制度**：个人信息处理、匿名化
- **相关待解决的问题/领域**：知情同意形式化、平衡知情同意的严格/僵化与商业发展
- **锐评**：知情同意不是做给监管看的

知情同意原则

重要数据

- **定义**：　一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。
- **源起与流变**：　重要数据首次于《网络安全法》中提出，《数据安全法》中多次强调，但仍未明确范围。随着《数据安全技术 数据分类分级规则》《数据出境安全评估办法》的颁布，重要数据的定义得到明确，数据出境时对企业的负担也减轻。
- **相对概念**：核心数据、一般数据

- **事件例举**：向境外非法提供高铁数据案、全国首个医疗健康数据出境
- **法律制度**：数据分级分类制度、数据出境、关键信息基础设施
- **相关待解决的问题/领域**：重要数据目录
- **锐评**：虽然Authority说不清楚，但是在努力说清楚

重要数据

被遗忘权

- **定义**：信息主体所享有的就其个人信息中不准确、不充分、不相关或超越信息处理目的信息，可以要求运营商等信息处理者把链接删除的权利。
- **源起与流变**：2014年，欧盟法院对冈萨雷斯案的判决系司法层面首次确认了网络时代的被遗忘权。2018年生效的GDPR首次在立法层面对被遗忘权作出明确规定。但我国并未在法律上明确该权利，而是以删除制度或损害赔偿等方式维护被遗忘权所涉及的个人利益。
- **近义词**：删除权

注：本图由AI绘制

- **事件例举**：冈萨雷斯案、任某某诉百度案、比利时谷歌案
- **相关待解决的问题/领域**：我国是否需要将被遗忘权法定化。
- **锐评**：**想要相忘于江湖，可没那么容易。**

被遗忘权

网络安全审查

- **定义**：为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，由国家互联网信息办公室会同其他有关主管部门，针对法律规定的特定对象，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查
- **源起与流变**：最早起源于《国家安全法》中对“影响或者可能影响国家安全的网络信息技术产品和服务”的国家安全审查机制，其后通过《网络安全法》《网络安全审查办法（2020）》《网络安全审查办法（2021）》等法律法规使得网络安全审查机制成型
- **相关概念**：关键信息基础设施、网络平台运营者、赴国外上市

- **事件例举**：滴滴案、知网案、美光公司案
- **法律制度**：国家安全法、网络安全法、网络安全审查办法、网络数据安全管理条例（征）
- **相关待解决的问题/领域**：部分概念不明、企业自身研判与监管部门对影响国家安全的判断口径不一
- **锐评**：网络安全审查的本质是为信息安全、网络安全、国家安全做“加法”

网络安全审查

公共数据

- **定义**：国家机关、法律法规规章授权的具有管理公共事务职能的组织以及供水、供电、供气、公共交通等公共服务运营单位，在依法履行职责或者提供公共服务过程中收集、产生的数据。
- **源起与流变**：公共数据的前身是“政府数据”，地方性法规中《贵阳市政府数据共享开放条例》则最早将政府数据开放共享落地。当前，公共数据正走向从建设服务型政府的无偿使用阶段到推动授权的有偿使用阶段。
- **近义词**：政务数据（政府数据）
- **相对概念**：企业数据、个人数据

- **事件例举**：衢阳政务数据第一拍、深圳数交所气象数据产品
- **法律制度**：公共数据确权授权机制
- **相关待解决的问题/领域**：公共数据运营流动需求、公共数据利用过程中的数据安全
- **锐评**：不能以人民的名义敲竹杠

公共数据

可携带权

- **定义**：自然人对于其同意数据控制者所处理的数据化形式承载的个人信息即个人数据，有权要求该控制者提供结构化的、通用的、机器可读的、能共同操作的以格式形式加以提供的权利，自然人可以将此等个人数据转移给其他的控制者。
- **源起与流变**：2007年，欧洲的“社交网络用户权利法案”提出个人数据自由和控制的相关要求，这被认为是数据可携权的权利雏形。同年，欧洲成立了“可携性数据项目”，以讨论和解决商业交往中的数据如何才能无障碍流动。2016年通过的《通用数据保护条例》正式以法律形式规定了数据可携带权。
- **近义词**：访问权、查阅复制权

注：本图由AI绘制

- **事件例举**：谷歌创建“谷歌外带”工具，意大利调查谷歌限制数据可携带权案，字节跳动所属的抖音、多闪与腾讯所属产品微信之间的数据争议等。
- **相关待解决的问题/领域**：建立关于数据可携带权的具体操作指引与数据格式标准。
- **锐评**：**要保障个人主体权利，还得看技术发展能力。**

可携带权

（点击蓝字即可跳转链接）

-= 全量辞典 =-

（按照拼音首字母排列）

本章节收录了 320 个数据法领域的概念和术语，我们按照汉字拼音顺序向大家依次展示。

每个概念中，我们会向大家介绍它的英文翻译、定义、我们对其的注解、关联词以及 DLaw Hub 知识库中与之相关的资料链接。

其中定义部分，我们会用两种颜色为大家标注不同的出处来源。蓝色框内展示的法律法规和标准中的定义；而绿色框内展示的则是 DLaw Hub 编写组成员自己对这个概念的解释。

此外英文翻译部分，我们主要会依赖法律法规和标准文件中的官方翻译。对于非官方翻译的词语，我们则会用“*”标出。

-= 目录 =-

平台经营者
平台内经营者
平台灵活就业人员

- Q -

汽车数据
汽车数据处理者
请求人
去标识化
去标识化技术
去标识化模型
权限
权限申请

- R -

热更新
人工智能
人工智能生成合成内容
人工智能生成合成内容标识
人脸识别数据
人脸识别数据主体
人脸特征
人脸图像
人类遗传资源材料
人类遗传资源信息
软件开发工具包
软件开发工具包提供者
软件升级

- S -

删除
商用密码
深度合成服务使用者
深度合成服务提供者
深度合成技术
深度合成服务技术支持者
深度合成服务备案
生成式人工智能技术
生成式人工智能服务提供者
生成式人工智能服务使用者
生成式人工智能备案
生成式人工智能登记
生物特征识别
生物特征数据
身份认证信息
识别
收集
受控公开共享
授权同意
数据
数据安全
数据安全风险
数据安全风险评估
数据安全管理认证
数据安全能力
数据安全事件
数据保护能力
数据标注
数据仓库
数据产品
数据处理
数据处理者
数据出境
数据出境安全评估
数据出境标准合同备案
数据分析
数据湖
数据交互
数据交易
数据交易所
数据可视化
数据流通
数据挖掘
数据脱敏
数据泄露、丢失和篡改
数据要素
数据要素市场化配置
数据治理
数据资产
数据资产入表
数据资源
书面同意
数字产业化
数字消费
双清单
受托处理者
算法推荐技术
算法备案

- T -

特定身份信息
提供
同意
推理
推荐算法

- W -

完全公开共享
完整性
网络
网络安全
网络安全保险
网络安全从业人员
网络安全等级保护
网络安全审查
网络安全事件
网络安全事件应急演练
网络安全突发事件
网络产品和服务
网络数据
网络数据安全风险评估
网络音视频服务
网络运营者
违法不良信息
微数据
微调
微调训练数据标注
委托处理
唯一设备识别码
位置轨迹数据
物理隔离
物联网
无线电数据

- X -

系统（敏感）权限
系统损失
显式标识
协议隔离
信息
信息安全事件
信息技术系统服务机构/信息技术服务机构
信息科技外包
信息化突发事件
信息系统
信息系统安全保障
信息系统生命周期
消费者金融信息
小程序
销毁
训练数据
训练语料

- Y -

衍生个人信息
衍生数据
业务
业务功能
业务影响分析
一般数据
移动互联网应用程序
移动互联网应用程序提供者
移动互联网应用程序分发平台
移动互联网应用程序（App）安全认证
移动智能终端
医疗器械网络安全
医疗器械相关数据
医疗卫生机构数据
隐式标识
隐私保护计算
隐私政策
应用程序分发服务
应用（程序）分发平台
应用程序信息服务
应用商店
用户个人信息
用户标签
用户画像
有用性
预置应用软件
元数据
原始数据
云计算
运行数据/汽车运行数据

- Z -

在线升级

自动化决策

自然资源领域数据

自然资源领域数据处理者

真实性

证券期货业网络安全事件

政务数据

支付敏感信息

知情同意原则

直接标识符

智能网联汽车

重要数据

重要信息系统

重要网络设施和信息系统

转让

组织数据

准标识符

座舱数据

-= A =-

安全

Security

对某一系统，据以获得保密性、完整性、可用性、可核查性、真实性以及可靠性的性质。

[来源：ISO/IEC TR 15443-1:2012 《信息技术-安全技术-安全保证框架》]

安全保护能力

Security Protection Ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

[来源：GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》]

安全策略

Security Policy

有关管理、保护和发布敏感信息的法律、规定和实施细则。

[来源：GB 17859-1999 《计算机信息系统安全保护等级划分准则》]

安全计算环境

Security Computing Environment

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

[来源：GB/T 25070-2019 《信息安全技术 网络安全等级保护安全设计技术要求》]

安全区域边界

Security Area Boundary

对定级系统的安全计算环境边界,以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

[来源：GB/T 25070-2019 《信息安全技术 网络安全等级保护安全设计技术要求》]

安全通信网络

Security Communication Network

对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。

[来源：GB/T 25070-2019 《信息安全技术 网络安全等级保护安全设计技术要求》]

安全性数据标注

Security Data Annotation

用于训练生成式人工智能模型提升输出响应信息安全性的数据标注。

[来源：《信息安全技术 生成式人工智能数据标注安全规范（征求意见稿）》，2024]

关联词：数据标注

安全域

Security Domain

具有相同的安全保护需求和相同安全策略的计算机或网络区域。

[来源：GB/T 20279-2015《信息安全技术 网络和终端隔离产品安全技术要求》]

-= B =-

半结构化数据

Semi-structured Data*

不符合关系型数据库或其他数据表的形式关联起来的数据模型结构，但包含相关标记，用来分隔语义元素以及对记录和字段进行分层的一种数据化结构形式。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：结构化数据，非结构化数据

保密性

Confidentiality

（1）使信息不泄漏给未授权的个人、 实体、进程，或不被其利用的特性。[来源：GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》]

（2） 保密性是指信息不被未授权实体（含产品、服务、个人、组织）获得或知悉的特性，即医疗器械产品自身和相关数据仅可由授权用户在授权时间以授权方式进行访问和使用。[来源：《医疗器械网络安全注册审查指导原则（2022 年修订版）》]

保险中介机构信息化工作

Digitization Work of Insurance Intermediaries*

是指保险中介机构将计算机、通信、网络等现代信息技术，应用于业务处理、经营管理和内部控制等方面，以持续提高运营效率、优化内部资源配置和提升风险防范水平为目的所开展的工作。其中保险兼业代理机构信息化工作，仅指该机构与保险兼业代理业务相关的信息化工作。

[来源：《保险中介机构信息化工作监管办法》，2021]

被遗忘权

Right To Be Forgotten*

被遗忘权是信息主体所享有的就其个人信息中不准确、不充分、不相关或超越信息处理目的信息，可以要求运营商等信息处理者把链接删除的权利。

[来源：丁宇翔，《个人信息保护纠纷理论释解与裁判实务（第二版）》]

1. 虽然被遗忘权并非我国《个人信息保护法》所明确的法定权利，但其所涉及的利益可通过删除制度及损害赔偿等方式得以保护。

2. 被遗忘权一词并不同于我国对权利的命名逻辑，无法直接看出该权利的客体是什么，如，我们不能参照肖像权的客体是肖像利益这种角度，来推断出被遗忘权的客体是被遗忘利益。但我们从被遗忘权的英文用词（right to be forgotten）来看，也许就能更好理解该权利的内涵。

DLaw Hub 知识库拓展资料： 一卡识数 · 被遗忘权

必要个人信息

Necessary Personal Information*

指保障 App 基本功能服务正常运行所必需的个人信息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。

[来源：《常见类型移动互联网应用程序必要个人信息范围规定》，2021]

必要性 / 最小必要

Necessity

（1）根据处理的目的，信息的处理是必要的，且不得超过合理的限度。[来源：杨合庆，《个人信息保护法释义》]

（2）最小必要原则——只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息。该原则具体包括：a）收集的个人信息的类型应与实现产品或服务的业务功能有直接关联；直接关联是指没有上述个人信息的参与，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。[来源：GB/T 35273-2020《信息安全技术 个人信息安全规范》]

在中国的《个人信息保护法》中，必要性可以从两个方面去理解：（1）处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式（目的限制原则）；（2）个人信息的收集应当限于实现处理目的的最小范围，不得过度收集个人信息（最小化原则）。[参见《个人信息保护法》第 6 条]

与此同时，在移动应用服务（APP）领域，一系列法规和标准从正面强制性地规定了 App 服务处理信息的必要范围，包括但不限于《网络安全实践指南--移动互联网应用（APP）基本业务功能必要信息规范》、《网络安全实践指南—移动互联网应用业务功能个人信息收集必要性规范》、《APP 收集使用个人信息最小必要评估规范》。《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第 1 部分：总则》具体提出了 APP 领域最小必要原则的评估要求和评估方法。

另一方面，必要性经常还出现在数据出境场景中。无论是数据出境安全评估还是数据出境标准合同备案，在自评估报告中，个人信息处理者都需要评估相关数据出境的必要性。

DLaw Hub 知识库拓展资料： 目的限制和最小化原则

标识度

Identifiability

（1）从数据中能识别出个人信息主体的概率。[来源：GB/T 42460—2023 《信息安全技术 个人信息去标识化效果评估指南》]

（2）从数据中能识别出个人信息主体的程度。[来源：20210996-T-469 《信息安全技术 个人信息去标识化效果分级评估规范》]

标识符

Identifier

微数据中的一个或多个属性 ，可以实现对个人信息主体的唯一识别。注：标识符分

为直接标识符和准标识符。

[来源：GB/T 37964—2019 《信息安全技术 个人信息去标识化指南》]

不良信息

Adverse (Credit) Information*

是指对信息主体信用状况构成负面影响的下列信息：信息主体在借贷、赊购、担保、租赁、保险、使用信用卡等活动中未按照合同履行义务的信息，对信息主体的行政处罚信息，人民法院判决或者裁定信息主体履行义务以及强制执行的信息，以及国务院征信业监督管理部门规定的其他不良信息。

[来源：《征信业管理条例》，2013]

-= C =-

产业互联网

Industrial Internet*

利用数字技术、数据要素推动全产业链数据融通，赋能产业数字化、网络化、智能化发展，推动业务流程、组织架构、生产方式等重组变革，实现产业链上下游协同转型、线上线下融合发展、全产业降本增效与高质量发展，进而形成新的产业协作、资源配置和价值创造体系。

[来源：《数据领域常用名词解释（第一批）》，2024]

产业数字化

Industrial Digitalization*

传统的农业、工业、服务业等产业通过应用数字技术、采集融合数据、挖掘数据资源价值，提升业务运行效率，降低生产经营成本，进而重构思维认知，整体性重塑组织管理模式，系统性变革生产运营流程，不断提升全要素生产率的过程。

[来源：《数据领域常用名词解释（第一批）》，2024]

超大型平台

Extra Large-scale Platform*

在中国的上年度年活跃用户不低于 5000 万、具有表现突出的主营业务、上年底市值（或估值）不低于 1000 亿人民币、具有较强的限制平台内经营者接触消费者（用户）能力的平台。

[来源：《互联网平台落实主体责任指南》（征求意见稿），2021]

关联词：大型网络平台、大型互联网企业、互联网平台

DLaw Hub 知识库拓展资料：互联网平台 - 个人信息处理者

车载软件升级系统

On-board Software Update System

安装在车端并具备直接接收、分发和校验来自车外的升级包等用于实现软件升级功能的软件和硬件。

[来源：GB 44496-2024《汽车软件升级通用技术要求》]

关联词：软件升级

车外数据

Vehicle External Data*

通过摄像头、雷达等传感器从汽车外部环境采集的道路、建筑、地形、交通参与者等数据，以及对其进行加工后产生的数据；

注 1：交通参与者是指参与交通活动的人，包括机动车、非机动车、其他交通工具的驾驶员与乘员，以及其他参与交通活动相关的人员。

注 2：车外数据可能包含人脸、车牌等个人信息以及车辆流量、物流等法律法规标准所规定的重要数据。

[来源：TC260 《汽车采集数据处理安全指南》，2021]

对于座舱数据，目前国家标准如 GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》要求车外数据未完成匿名化处理前，不应向车外提供。

沉浸式拟真场景

Immersive Virtual Reality Scene*

是指应用深度合成技术生成或者编辑的、可供参与者体验或者互动的、具有高度真实感的虚拟场景。

[来源：《互联网信息服务深度合成管理规定》，2022]

重标识

Re-identification

把去标识化的数据集重新关联到原始个人信息主体或一组个人信息主体的过程。

[来源：GB/T 37964—2019 《信息安全技术 个人信息去标识化指南》]

重标识风险

Re-identification Risk

从数据中能识别出个人信息主体的概率。

[来源：GB/T 42460—2023 《信息安全技术 个人信息去标识化效果评估指南》]

存储

Storage

数据在存储器中的保存。

[来源：GB/T 5271.12-2000 《信息技术 词汇 第 12 部分：外围设备》]

-= D =-

大数据平台

Big Data Platform*

是指以处理海量数据存储、计算、分析等为目的的基础设施，包括数据统计分析类的平台和大数据处理类平台（如数据湖、数据仓库等）。

[来源：《银行保险机构数据安全管理办法》（征求意见稿），2024]

大型互联网企业

Large Internet Enterprise

提供重要互联网平台服务、用户数量巨大、业务类型复杂的互联网企业，同时具备较大用户规模、较广业务种类、较多业务范围、较高经济体量和较强影响能力的大型互联网平台。

[来源：《信息安全技术 大型互联网企业内设个人信息保护监督机构要求(征求意见稿）》，2023]

关联词：大型网络平台、超大型平台、互联网平台

DLaw Hub 知识库拓展资料：互联网平台 - 个人信息处理者

大型网络平台

Large Internet Platform*

是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。

[来源：《网络数据安全管理条例》，2024]

关联词：大型互联网企业、超大型平台、互联网平台

DLaw Hub 知识库拓展资料：互联网平台 - 个人信息处理者

单独同意

Separate Consent

> 个人针对其个人信息进行特定处理而专门作出具体、明确授权的行为，不包括一次性针对多种目的或方式的个人信息处理活动作出的同意。注： 单独同意的告知内容与取得同意的方式需与其他处理活动予以区分。
>
> [来源：GB/T42574—2023《信息安全技术 个人信息处理中告知和同意的实施指南》]

DLaw Hub 知识库拓展资料： 第二十九条 特别同意规则

等级保护 / 网络安全等级保护

Classified Protection / Multi-Level Protection Scheme (MLPS)

> （信息系统）等级保护是指对国家重要信息、法人和其他组织及公民的专有信息以及信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。
>
> [来源：《信息安全等级保护管理办法(试行)》，2006]

中国的等级保护制度经历了两个阶段，一是 1994-2016 的 1.0 时代，一般称为“信息安全等级保护”。在该时期已经逐步探索出了五个等级的分级保护要求。而随着 2017 年《网络安全法》的颁布，对于安全的理解也从信息安全拓展到了网络安全。《网络安全法》第 21 条规定“国家实行网络安全等级保护制度”，等级保护制度进入了 2.0 时代。

网络安全等级保护分为五个等级，从低到高分别为：一级、二级、三级、四级和五级。不同等级的保护对象、保护要求和保护措施各不相同。通俗理解，一级等保适用于一般信息系统，五级等保适用于国家重要信息系统，级别越高，等保的合规要求越高，也需要企业采取更严格的安全保障措施。

DLaw Hub 知识库拓展资料： 等级保护

等级保护对象

Target of Classified Protection

（1）网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括基础信息网络云计算平台/系统、大数据应用/平台/资源、物联网、工业控制系统和采用移动互联技术的系统等。[来源：GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》]

（2）网络安全等级保护工作直接作用的对象。注：主要包括信息系统 、通信网络设施和数据资源等。[来源：GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》]

第三方应用

Third-party Components

（1）由产品服务提供者之外的其他组织或个人，提供的软件开发工具包、代码 、插件、程序等应用。注 1：包括商业应用和开源应用。注 2：既包括嵌入产品服务的 SDK、代码、插件等（称为”第三方组件”），也包括接入产品服务的移动互联网应用程序（简称“移动应用”小程序、应用系统等（称为“第三方产品或服务“）。[来源：GB/T 41817—2022 《信息安全技术 个人信息安全工程指南》]

（2）由移动互联网应用程序运营者之外的其他法人实体提供，通过移动互联网应用程序面向用户提供服务的应用程序。注 1：第三方应用提供的形式，通常包括 SDK、小程序、Web 页面等。如果 SDK 没有直接向用户提供服务，则不属于本文件所称的第三方应用。注 2：虽与 App 运营者属于不同法人实体，但与 App 运营者属于同一企业集团，且遵守同一套管理制度、统一进行安全和运维管理的，不属于 App 运营者的第三方。关联公司通常属于 App 运营者的第三方。[来源：GB/T 41391-2022《信息安全技术 移动互联网应用程序 App 收集个人信息基本要求》]

第三方软件开发工具包

Third-party Software Development Kit*

由移动互联网应用程序运营者之外的其他法人实体提供的软件开发工具包。

[来源：GBT 41391-2022《信息安全技术 移动互联网应用程序<App>收集个人信息基本要求》]

电信数据

Telecom Data*

是指在电信业务经营活动中产生和收集的数据。

[来源：《工业和信息化领域数据安全管理办法（试行）》，2022]

定向推送

Directional Push

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体推荐或展示信息内容、提供商品或服务的搜索结果以及推送商业广告等活动。

注：业务实践中，定向推送也被称为个性化展示或个性化推荐。

[来源：《APP 用户权益保护测评规范定向推送》，2021]

其与其他相近概念的比较可参见个性化推荐

关联词：个性化展示；个性化推送；算法推荐；自动化决策；用户画像

DLaw Hub 知识库拓展资料：个性化推荐

多方安全计算

Secure Multi-party Computation (SMPC / MPC)*

是指在无可信第三方的条件下，通过特殊设计的密码学算法和协议，允许多个参与方在不泄露各自隐私数据的前提下，协同完成计算任务。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：隐私保护计算

-= E =-

儿童

Child

> 不满十四周岁的未成年人。
>
> [来源：《儿童个人信息网络保护规定》，2019]

儿童是数据合规领域一个特殊的概念，《个人信息保护法》将儿童个人信息作为敏感个人信息，并提出了更严格的保护要求。而在比较法视角下，各国对于“儿童”的年龄范围作出了不同的定义。

DLaw Hub 知识库拓展资料：未成年/儿童个人信息保护

-= F =-

访问控制

Access Control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

[来源：GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》]

非结构化数据

Unstructured Data*

不具有预定义模型或未以预定义方式组织的数据。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：结构化数据，半结构化数据

风险隐患

Potential Risk*

可能导致危害数据的保密性、完整性、可用性和数据处理合理性等事件的威胁、脆弱性、问题、隐患等，也称“风险源”。注：风险隐患，既包括安全威胁利用脆弱性可能导致数据安全事件的风险隐患，也包括数据处理活动不合理操作可能造成违法违规处理事件的风险隐患。

[来源：《网络安全标准实践指南—网络数据安全风险评估实施指引》，2023]

风险源

Risk Source

可能导致危害数据的保密性、完整性、可用性和数据处理合理性等事件的威胁、脆弱性、问题、隐患等，也称“风险隐患”。注：风险隐患，既包括安全威胁利

用脆弱性可能导致数据安全事件的风险隐患， 也包括数据处理活动不合理操作可能造成违法违规处理事件的风险隐患。

[来源：GB/T 20984-2022《信息安全技术 信息安全风险评估方法》]

风险转移

Risk Mitigation

与另一方对风险带来的损失或收益的共享。注：在信息安全风险的语境下 ，对于风险转移仅考虑负面结果（损失）。

[来源：GB/T 33132-2016《信息安全技术 信息安全风险处理实施指南》]

-= G =-

告知

Notice

使个人知晓其个人信息处理活动及其有关规则的行为。

[来源：GB/T 42574—2023《信息安全技术 个人信息处理中告知和同意的实施指南》]

个人健康医疗数据

Personal Health Data

单独或者与其他信息结合后能够识别特定自然人或者反映特定自然人生理或心理健康的相关电子数据。

注：个人健康医疗数据涉及个人过去、现在或将来的身体或精神健康状况,接受的医疗保健服务和支付的医疗保健服务费用等。

[来源：GB/T 39725-2020《信息安全技术健康医疗数据安全指南》]

个人健康医疗数据范围可见《信息安全技术健康医疗数据安全指南》的附录 A。

关联词：健康医疗数据

个人金融信息

Personal Financial Information*

是指银行业金融机构在开展业务时，或通过接入中国人民银行征信系统、支付系统以及其他系统获取、加工和保存的以下个人信息：

（一）个人身份信息，包括个人姓名、性别、国籍、民族、身份证件种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等；

（二）个人财产信息，包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等；

（三）个人账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等；

（四）个人信用信息，包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息；

（五）个人金融交易信息，包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户在通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等；

（六）衍生信息，包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息；

（七）在与个人建立业务关系过程中获取、保存的其他个人信息。

[来源：《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》，2011]

个人敏感信息

Personal Sensitive Information

即“敏感个人信息”，具体可参见“敏感个人信息”的解释。

个人信息

Personal Information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。[来源：《个人信息保护法》，2021]

注：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，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，属于个人信息。

[来源：GB/T 35273—2020《信息安全技术 个人信息安全规范》]

目前中国对于个人信息采取了“识别+关联”的判断方式，即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，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。

具体示例可见《信息安全技术 个人信息安全规范》的附录 A 和《数据安全技术 数据分类分级规则》的附录 B，包括但不限于姓名、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。

DLaw Hub 知识库拓展资料： 第四条 个人信息的概念

关联词： 匿名化；去标识化；直接标识符

个人信息安全工程

Personal Information Security Engineering

> 也称隐私工程，是指将个人信息安全原则和要求融入到产品服务规划 、建设的每个阶段，使个人信息安全要求在产品服务中有效落实的工程化过程。
>
> [来源：GB/T 41817—2022《信息安全技术 个人信息安全工程指南》]

个人信息保护负责人

Data Protection Officer (DPO) *

> 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。
>
> [来源：《个人信息保护法》，2021]

根据《信息安全技术 个人信息安全规范》，个人信息保护负责人和个人信息保护工作机构的职责应包括但不限于：（1）全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任；（2）组织制定个人信息保护工作计划并督促落实；（3）制定、签发、实施、定期更新个人信息保护政策和相关规程；（4）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、接收方等）和授权访问策略；

（5）开展个人信息安全影响评估，提出个人信息保护的对策建议，督促整改安全隐患；（6）组织开展个人信息安全培训；（7）在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为；（8）公布投诉、举报方式等信息并及时受理投诉举报；（9）进行安全审计；（10）与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。

除了个人信息保护负责人外，《网络安全法》和《数据安全法》以及配套的其他法规还提出了各类“网络安全负责人”或“数据安全负责人”的要求。关于中国相关负责人的介绍，可参见网安、数安及个保岗位负责人梳理。

此外，近两年来，一些地方政府还推出了“首席数据官”（CDO）制度，并要求相关企业备案“首席数据官”的信息。具体可参见首席数据官制度。

DLaw Hub 知识库拓展资料：第五十二条 个人信息保护负责人制度

个人信息保护监督机构

Personal Information Protection Supervision Agency

大型互联网企业建立的主要由外部成员组成，对自身个人信息保护合法合规情况、履行个人信息保护社会责任情况等进行独立监督，并对提升个人信息保护水平提出建议和意见的机构。

[来源：《信息安全技术 大型互联网企业内设个人信息保护监督机构要求》(征求意见稿），2023]

个人信息保护监督机构外部成员

External Member of Personal Information Protection Supervision Agency

具备个人信息保护专业知识和技能，不在大型互联网企业担任除个人信息保护监督机构外部成员外的其他职务，与受聘大型互联网企业及其主要股东不存在可能妨碍其进行独立客观判断的关系，对大型互联网企业个人信息保护情况进行监督，发表独立客观建议、意见的外部专家。

[来源：《信息安全技术 大型互联网企业内设个人信息保护监督机构要求》(征求意见

稿），2023]

个人信息保护认证

Personal Information Protection Certification*

对个人信息处理者开展个人信息收集、存储、使用、加工、传输、提供、公开、删除以及跨境等处理活动进行认证。个人信息处理者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求。对于开展跨境处理活动的个人信息处理者，还应当符合 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。

个人信息保护认证的认证模式为：技术验证 + 现场审核 + 获证后监督。通过认证后，认证证书有效期为 3 年。

[来源：《个人信息保护认证实施规则》，2022]

实践中，个人信息保护认证也是数据出境的重要合法途径。具体可参见“跨境安全认证”。

DLaw Hub 知识库拓展资料： 个人信息保护认证解读

个人信息安全影响评估

Personal Information Security Impact Assessment

也称“个人信息保护影响评估 ”，具体可参见“个人信息保护影响评估”的解释。

关联词： 个人信息保护影响评估

个人信息保护影响评估（PIA）

Personal Information Protection 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。

[来源：GB/T 35273—2020《信息安全技术 个人信息安全规范》]

也称“个人信息安全影响评估” 。

起初，全国信息安全标准化技术委员会于 2020 年发布的《信息安全技术 个人信息安全规范》和《信息安全技术 个人信息安全影响评估指南》都采用了“个人信息安全影响评估”这个概念，而到了 2021 年的《个人信息保护法》中则使用了“个人信息保护影响评估”。

DLaw Hub 知识库拓展资料： PIA：个人信息保护影响评估

关联词： 个人信息保护影响评估（PIA）星级认证

个人信息保护影响评估（PIA）星级认证

Personal Information Protection Impact Assessment (PIA) Star Certification*

2022 年 3 月，为改善个人信息保护影响评估在细分操作指引、协调落地执行、评估结果效力等方面的问题，切实推进个人信息保护影响评估制度发挥实效，“数据安全共同体计划（DSC）”“中国网络安全产业联盟（CCIA）数据安全工作委员会”等组织共同发起“个人信息保护影响评估专题工作”。“个人信息保护影响评估专题工作”陆续开展了编制个人信息保护影响评估常用工具表、开展个人信息保护影响试点评估等工作。

评估采取的个人信息保护影响评估方法参照了以下文件：（1）《个人信息保护法》中相关要求；（2） GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》；（3）《个人信息保护影响评估常用工具表（含 A、B、C 子表）》（专题工作组发布）。

通过评估的企业会获得相应的星级标识。

DLaw Hub 知识库拓展资料： 数据保护相关认证

关联词： 个人信息保护影响评估

个人信息保护政策

Personal Information Protection Policy / Privacy Policy

又名“隐私政策”，是指说明移动互联网应用程序处理个人信息规则的文本。

[来源：GB/T 42582-2023 《信息安全技术 移动互联网应用程序（APP）个人信息安

全测评规范》]

GB/T 35273-2020《信息安全技术 个人信息安全规范》第 5.5 条规定了个人信息保护政策的基本要求，而且附录 D 也提供了政策的模板。

DLaw Hub 知识库拓展资料： 隐私政策

个人信息处理 / 处理

Personal Information Processing

对个人信息的收集 、存储 、使用、加工 、传输 、提供、公开 、删除等行为。

[来源：《个人信息保护法》，2021]

程啸老师在《个人信息保护法理解与适用》一书中记载“虽然在《个人信息保护法》的审议过程中，一些委员、代表和专家提出应当增加对个人信息处理活动的列举，如增加“记录”“删除”“检索”等。最终本条第 2 款只是增加了“删除”这一类处理活动，没有增加其他的类型。这主要是考虑到个人信息处理活动的类型很多，对于不是特别典型和重要的处理活动，可以用“等”字涵盖，无须一一列举。我国《个人信息保护法》并未限定个人信息处理的具体方式，也就是说，并不需要考虑到个人信息处理的媒介和方式，无论是以自动方式(通过计算机以电子介质)处理个人信息，还是以其他方式(通过人工以纸介质)处理个人信息，都属于个人信息的处理。”

DLaw Hub 知识库拓展资料： 第四条 个人信息的概念

个人信息处理活动记录

Records of Processing Activities (ROPA)

个人信息控制者宜建立、维护和更新所收集、使用的个人信息处理活动记录。

[来源：GB/T 35273—2020《信息安全标准 个人信息安全规范》]

《网络数据安全管理条例》第十二条规定，向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存 3 年。

但是目前国内并没有对于该记录要求提出更加具体且可有操作性的规定，因此相关个人

信息处理者可以参考域外法律的经验。欧盟 GDPR 中也有对于数据处理活动的记录的要求，被称为“ROPA”（records of processing activities）。GDPR 第 30 条规定分别规定了数据控制者（Controller）和处理者（Processor）的记录要求。ROPA 需要包含的信息如下：（1）控制者 / 联合控制者 / 处理者的名称和联系方式和数据保护官员；（2）处理目的；（3）数据主体类别和个人数据类别；（4）个人数据已经或将被披露的接收者类别，包括第三国或国际组织的接收者；（5）数据跨境传输所需的记录；（6）在可能的情况下，各个数据类别的删除时间限制；（7）在可能的情况下，采取的技术和组织安全措施的概括描述。

个人信息处理者

Personal Information Handler/ Processor

在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

[来源：《个人信息保护法》，2021]

注：本概念与 GB/T 35273—2020 中的“个人信息控制者”所指一致。

中国法下的个人信息处理者等于 GDPR 中的数据控制者（data conrtoller），而 GDPR 的数据处理者（data processor）则在中国法下对应的是“受托处理者”。这很容易在做比较法研究时让人搞混。因此，部分文件在翻译时为了避免混淆，会采用“handler”来翻译“处理者”。

中国法为什么要采用“处理者”这一称呼，目前众说纷纭，其中一种说法是为了配合《民法典》中使用“处理”概念来囊括对信息的收集、使用、共享、删除等行为。

此外，一些标准中还出现了“个人信息管理者”、“个人信息获得者”和“个人信息控制者”的概念。但这次概念目前实践中已经不再被使用了。

关联词：受托处理者；个人信息控制者

个人信息合规审计

Personal Information Protection Compliance Audit

指针对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查

和评价的监督活动。

[来源：《个人信息保护合规审计管理办法（征求意见稿）》，2023]

根据《个人信息保护合规审计管理办法（征求意见稿）》，个人信息保护合规审计主要分为两类：（1）定期开展个人信息保护合规审计，以及（2）监管部门要求合规审计。

1. 定期开展个人信息保护合规审计（个人信息保护法第 54 条）
    - **触发：**处理超过 100 万人个人信息的个人信息处理者，应当每年至少开展一次个人信息保护合规审计；其他个人信息处理者应当每二年至少开展一次个人信息保护合规审计。
    - **谁来做：**本组织内部机构或者委托专业机构
2. 监管部门要求合规审计（个人信息保护法第 64 条）
    - **触发：**监管部门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
    - **谁来做：**委托专业机构
    - **程序：**选定机构 - 实施审计 - 审计报告各方签字盖章 - 审计报告报送监管部门 - 按照专业机构给出的整改建议进行整改 - 专业机构复核 - 整改情况报送监管部门

2024 年，中国发布了《数据安全技术 个人信息保护合规审计要求》（征求意见稿），提出了个人信息保护合规审计原则，规定了个人信息保护合规审计的具体实施要求，并提供了相应的审计模板文件。

DLaw Hub 知识库拓展资料：《个人信息保护合规审计管理办法（征求意见稿）》

个人信息管理者

Administrator of Personal Information

决定个人信息处理的目的和方式，实际控制个人信息并利用信息系统处理个人信息的组织和机构。

[来源：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保护

指南》]

个人信息获得者

Receiver of Personal Information

从信息系统获取个人信息，并对获得的个人信息进行处理的个人、组织和机构。

[来源：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保护指南》]

个人信息控制者

Personal Information Controller*

GB/T 35273—2020 中的概念，与《个人信息保护法》中的“个人信息处理者”所指一致。

这个概念目前基本不被使用。

关联词：个人信息处理者

个人信息去标识化效果分级

Grading of the De-Identification Effect of Personal Information*

基于数据是否能直接识别个人信息主体，或能以多大概率识别个人信息主体 ，个人信息标识度分级划分为 4 级，用于区分个人信息去标识化效果。

[来源：GB/T 42460—2023 《信息安全技术 个人信息去标识化效果评估指南》]

分级	划分依据
1 级	包含直接标识符,在特定环境下能直接识别个人信息主体
2 级	消除了直接标识符,但包含准标识符,且重标识风险高于或等于可接

	受风险阈值
3 级	消除了直接标识符,但包含准标识符,且重标识风险低于可接受风险阈值
4 级	不包含任何标识符

个人信息生命周期

Lifecycle of Personal Information

> 包括个人信息持有者收集、保存、应用、委托处理、共享、转让和公开披露、删除个人信息在内的全部生命历程。
>
> [来源：《互联网个人信息安全保护指南》，2019]

个人信息泄露

Personal Information Breach*

> 我们通常所说的“个人信息泄露”包括“未经授权的访问以及个人信息泄露、篡改、丢失”。
>
> [来源：《个人信息保护法》，2021]

从比较法上，这个定义与 GDPR 中的概念相似。GDPR 第 4 条定义了“个人数据泄露”（‘personal data breach’），是指“安全漏洞导致个人数据被意外或非法销毁、丢失、更改、未经授权披露或获取，这些个人数据可能是传输、存储或以其他方式处理的。”（a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed）

另外，鉴于通俗的表达中并不会严格区分“个人信息”和“数据”，因此人们常说的“数据泄露”也与本概念同义。

关联词：数据安全事件；网络安全事件；网络安全突发事件；信息安全事件

DLaw Hub 知识库拓展资料：数据泄露 / 网络安全事件

个人信息主体

Personal Information Subject

个人信息所识别或者关联的自然人。

[来源：GB/T 35273—2020 《信息安全技术 个人信息安全规范》]

个人信息转移

Personal Information Transfer

个人信息主体请求处理其个人信息的个人信息处理者，将其所处理的个人信息转移至个人信息主体指定的其他个人信息处理者的过程。

[来源：《数据安全技术 基于个人请求的个人信息转移要求》（征求意见稿），2024]

个人生物识别信息

Personal Biometric Information*

个人生物识别信息包括生物识别原始信息（如样本、图像等）和比对信息（如特征值、模板等），如人脸、指纹、步态、声纹、基因、虹膜、笔迹、掌纹、耳廓、眼纹等。

[来源：《网络安全标准实践指南——网络数据分类分级指引》，2021]

个性化展示

Personalized Display

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

注：基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。

[来源：GB/T 35273—2020《信息安全标准 个人信息安全规范》]

其与其他相近概念的比较可参见个性化推荐

关联词：个性化推荐；个性化展示；定向推送；算法推荐；自动化决策；用户画像

DLaw Hub 知识库拓展资料：个性化推荐

个性化推送

Personalized Push

基于对特定用户或用户群体进行个性化用户画像实现的信息推送，信息推送的展现形式包括但不限于推荐、列表页面、弹窗等。

[来源：T/TAF 138—2022《App 推荐算法用户权益保护技术要求及测评规范》]

其与其他相近概念的比较可参见个性化推荐

关联词：个性化推荐；个性化展示；定向推送；算法推荐；自动化决策；用户画像

DLaw Hub 知识库拓展资料：个性化推荐

个性化推荐

个性化推荐是一种利用数据分析和算法技术，为用户提供量身定制内容的方式。其核心思想是根据用户的历史行为、偏好和兴趣，自动生成个性化的推荐列表，从而提升用户体验和满意度。例如，当用户在观看视频、浏览电商平台或阅读新闻时，平台所展示的内容往往精准地契合用户的近期兴趣，这正是个性化推荐技术在背后发挥作用的结果。

这种推荐方式就像朋友知道你喜欢什么，主动给你推荐一样，不仅能提高用户的购物体验，还能帮助用户发现很多新的东西，省去很多寻找的时间。但是，与此同时，在用户享受这种“量身定制”的信息服务的同时，也存在一些隐患。例如“大数据杀熟”对于消费者权利的侵害，有譬如对于个人信息的处理引发对于隐私/个人信息权益的担忧。

为应对这些问题，中国法律在多个规章与标准中对“个性化推荐”及其应用设定了相

应的规范和限制，但也产生了许多长相相近的概念，宛如在玩一个汉字排列组合的游戏。

这些概念列举如下：自动化决策，算法推荐，个性化展示，个性化推送，定向推送。这些概念间的比较可参见个性化推荐。

关联词：个性化推送；个性化展示；定向推送；算法推荐；自动化决策；用户画像

DLaw Hub 知识库拓展资料：个性化推荐

公共数据

Public Data

（1）国家机关和依法经授权、受委托履行公共管理和服务职能的组织（以下统称公共管理和服务机构），在依法履行公共管理职责或提供公共服务过程中收集、产生的数据。注 1： 公共管理和服务机构，包括各级政务机关、事业单位，其他依法经授权或受委托管理公共事务的组织，以及供水、供电、供气、公共交通、教育、卫生健康、社会福利、环境保护等提供公共服务的组织。注 2： 本实践指南给出的公共数据是广义概念，实际使用时也存在狭义的公共数据，即仅将提供公共服务的组织在公共服务过程中收集产生的数据作为公共数据，将政务机关履职过程中收集产生的数据作为政务数据。注 3： 公共数据通常不包括组织专有的知识产权数据和商业秘密。[来源：《网络安全标准实践指南——网络数据分类分级指引》，2021]

（2）各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或提供公共服务过程中收集、产生的数据。[来源：GB/T 43697-2024《数据安全技术 数据分类分级规则》]

（3）公共数据，是指本市国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织(以下统称公共管理和服务机构)，在履行公共管理和服务职责过程中收集和产生的数据。[来源：《上海市数据条例》，2021]

（4）国家机关、法律法规规章授权的具有管理公共事务职能的组织以及供水、供电、供气、公共交通等公共服务运营单位，在依法履行职责或者提供公共服务过程中收集、产生的数据。[来源：《浙江省公共数据条例》，2022]

（5）各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。[来源：《数据领域常用名词解释（第一批）》，2024]

与个人数据围绕保护的法律体系不同，公共数据是围绕共享、利用的需求而产生合规要求。尽管在国内公共数据的共享、利用仅是基于近几年的发展，但各地政府充分发挥主观能动性下所制定的法律法规，诞生的实践应用，已经昭示着公共数据作为数据要素市场化的先行者。可以说，个人数据保护的诉求是自下而上的，而公共数据利用的诉求是自上而下的。因此，以政府为主体在进行公共数据利用的过程中，不仅需要为个人数据保驾护航，更需要考虑同时在“政府逻辑”和“经济逻辑”的情况下，如何限制权力的行使，更好地促进公共数据的有效利用。

DLaw Hub 知识库拓展资料： 一卡识数 · 公共数据

公开

Disclousre*

个人信息的公开是指个人信息处理者将信息向不特定的人公开，让个人信息处于不特定人都可以获取的状态。若一个人只是在小范围内（如十几人的聊天群）发布一些个人信息，则不意味着公开。

[来源：程啸，《个人信息保护法理解与适用》，2021]

公开披露

Public Disclosure

向社会或不特定人群发布信息的行为。

[来源：GB/T 35273—2020 《信息安全技术 个人信息安全规范》]

公民个人信息

Citizen 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，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

[来源：《最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，2017]

公平性

Fairness

尊重既定事实、社会规范和信仰,且不受偏袒或不公正歧视影响的对待、行为或结果。

注 1: 对公平性的考虑是与环境高度相关的,并且因文化、代际、地理和政治观点而异。

注 2: 公平不等于没有偏见。偏见并不总是导致不公平,不公平可能是由偏见以外的因素引起的。

[来源：GB/ T 41867- 2022《信息技术 人工智能 术语》]

功能性数据标注

Functional Data Annotation

用于训练生成式人工智能模型具备完成特定任务能力的数据标注。

[来源：《信息安全技术 生成式人工智能数据标注安全规范》（征求意见稿），2024]

关联词： 数据标注

共同处理

Joint Processing*

两个以上的数据处理者共同决定数据的处理目的和处理方式的数据处理活动。注：两个以上含两个。

[来源：《网络安全标准实践指南—网络数据安全风险评估实施指引》，2023]

例如，在 APP 与 SDK 之间处理信息的关系中，如果 App 与 SDK 共同决定个人信息的

处理目的、方式（也就是说同一个处理目的，必须两个角色共同参与），那么可能构成“共同处理者”，且都应该对用户以“处理者”的名义来明示告知。以广告 SDK 为例，如果广告 SDK 无法独立完成投放广告的过程，需要 App 运营者参与对个人信息的处理并与广告 SDK 共同决定处理的目的和方式，且双方约定了各自的权利和义务，并对用户在广告服务的相关界面同时披露两个责任主体，则有可能构成“共同处理者”。[来源：CCIA 数据安全工作委员会，《如何理解和规范 App 接入的第三方服务处理个人信息的情形？》]

《中华人民共和国个人信息保护法》第二十条规定了共同处理的规则：“两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。”

知识库链接：第二十条 共同处理个人信息的权义约定和责任承担

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。

[来源：GB/T 35273—2020《信息安全技术 个人信息安全规范》]

关联词：提供

工业和信息化领域数据

Data in the Field of Industry and Information Technology*

包括工业数据、电信数据和无线电数据等。

[来源：《工业和信息化领域数据安全管理办法（试行）》，2022]

关联词：工业数据；电信数据；无线电数据

工业数据

Industrial Data*

工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

[来源：《工业和信息化领域数据安全管理办法（试行）》，2022]

工业和信息化领域数据处理者

Data Processor in the Field of Industry and Information Technology*

数据处理活动中自主决定处理目的、处理方式的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者和无线电频率、台（站）使用单位等工业和信息化领域各类主体。工业和信息化领域数据处理者按照所属行业领域可分为工业数据处理者、电信数据处理者、无线电数据处理者等。

[来源：《工业和信息化领域数据安全管理办法（试行）》，2022]

关键信息基础设施

Critical Information Infrastructure

关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：《关键信息基础设施安全保护条例》，2021]

关键信息基础设施的认定会有有关部门内部通知。

关键信息基础设施运营者需要承担更加严格的数据安全和网络安全保护责任，例如网络安全审查、数据出境时的安全评估义务等、供应链审查等。

DLaw Hub 知识库拓展资料： 关键信息基础设施

-= H =-

行业领域数据

Industry Sector Data

在某个行业领域内依法履行工作职责或开展业务活动中收集和产生的数据。

[来源：GB/T 43697-2024《数据安全技术 数据分类分级规则》]

合理性

Rationality / Reasonableness*

数据处理遵守法律、行政法规要求，尊重社会公德和伦理道德，符合网络安全和数据安全常识道理。

[来源：GB/T 20984-2022《信息安全技术 信息安全风险评估方法》]

核心数据

Core Data

（1）是指关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据。[来源：《网络安全标准实践指南——网络数据分类分级指引》，2021]

（2）特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。[来源：《信息安全技术 网络数据分类分级要求（征求意见稿）》，2022]

（3）对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。[来源：GB/T 43697-2024《数据安全技术 数据分类分级规则》]

关联词：数据分类分级；重要数据

湖仓一体

Data Lake-Warehouse Integration*

是指一种新型的开放式的存储架构，打通了数据仓库和数据湖，将数据仓库的高性能及管理能力与数据湖的灵活性融合起来，底层支持多种数据类型并存，能实现数据间的相互共享，上层可以通过统一封装的接口进行访问，可同时支持实时查询和分析，为企业进行数据治理带来了更多的便利性。

[来源：《数据领域常用名词解释（第一批）》，2024]

互联网络

Internet*

是指直接进行国际联网的计算机信息网络。

[来源：《计算机信息网络国际联网管理暂行规定》，1996]

互联网信息服务提供者

Internet Information Service Providers

互联网信息服务提供者为用户提供互联网信息发布和应用平台，包括但不限于互联网新闻信息服务、搜索引擎、即时通讯、交互式信息服务、网络直播、网络支付、广告推广、网络存储、网络购物、网络预约、应用软件下载等互联网服务。

[来源：《互联网信息服务管理办法（修订草案）》，2021]

互联网弹窗信息推送服务

Internet Pop-Up Information Push Service*

是指通过操作系统、应用软件、网站等，以弹出消息窗口形式向互联网用户提供的信息推送服务。

[来源：《互联网弹窗信息推送服务管理规定》，2022]

-=J=-

基本业务功能

Basic Business Function

移动互联网应用程序实现用户主要使用目的的业务功能。

[来源：GBT 41391-2022《信息安全技术 移动互联网应用程序<App>收集个人信息基本要求》]

2019 年，《网络安全实践指南--移动互联网应用（APP）基本业务功能必要信息规范》中将必要信息进一步拆解为基本业务功能相关必要信息和通用功能相关必要信息。其中，基本业务功能相关必要信息，是与基本业务功能直接关联，一旦缺少会导致基本业务功能无法实现或无法正常运行的个人信息；而通用功能相关必要信息，是相关法律法规要求、保障移动互联网应用安全风险管控所必需的个人信息。

关联词：最小必要

基本功能软件

Basic Function Application

直接支撑操作系统运行或实现移动智能终端基本功能所必需的预置应用软件。

[来源：GB/T 43445-2023《信息安全技术 移动智能终端预置应用软件基本安全要求》]

基础模型

Foundation Model

在大量数据上训练的，用于普适性目标、可优化适配多种下游任务的深度神经网络模型。

[来源：TC260《生成式人工智能服务安全基本要求》，2024]

机器可读

Machine-readable

可以由计算机软件应用程序自动读取和处理的数据存储格式。

[来源：《数据安全技术 基于个人请求的个人信息转移要求》，2024]

即时通信服务

Instant Messaging Service

通过计算机、智能终端等客户端软件、浏览器等,向用户提供发送和接收信息(文本、图片、文件、音视频、链接等)的在线实时交互服务。

注 1:本文件所称的即时通信服务,主要针对相关商业服务,组织内部自建或自用服务不包含在内。

注 2：本文件所称的即时通信服务,典型应用场景包括单聊(两个用户之间,用户和管理员之间直接交互)、群聊(在群组内收发即时消息)、聊天室(一种多人在线实时交谈的网络空间),基于即时通信的社交,社区,在线客服,组织通信等。

[来源：GB/T 42012-2022《信息安全技术 即时通信服务数据安全要求》]

计算机病毒

Computer Virus*

编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

[来源：《计算机信息系统安全保护条例》，1994]

计算机信息网络国际联网

International Information Networks Interconnection*

是指中华人民共和国境内的计算机信息网络为实现信息的国际交流，同外国的计算机

信息网络相联接。

[来源：《计算机信息网络国际联网管理暂行规定》，1996]

计算机信息系统 / 计算机系统

Computer (Informtaion) System

（1）由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。[来源：《计算机信息系统安全保护条例》，1994]

（2）是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。[来源：《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》，2011]

基因识别数据

Genetic Recognition Data

个体或群体遗传信息的数据，该数据可以直接或间接使用技术手段，从人类遗传物质中提取的表征识别到人类个体或群体。

注 1：基因识别数据指的是基因数据，主要包括基因乡核酸序列数据、功能基因组数据以及提取过程中生成的原始数据和中间数据；

注 2：基因组核酸序列数据是指在基因组层面,利用类测序技术（如：Sanger 测序技术、高通量测序技术、质谱技术链式反应技术等）或基因分型技术(如:基因芯片技术、聚合酶链式反应技术等）获得的描述核酸排列顺序的数据以及各类遗传变异的数据【如:单核苷酸多态性（SNP）、插入缺失（INDEL）突变、短串联重复序列（STR）、拷贝数变异(Copy Number Variation，CNV)及基因组结构变异(Structural Variation，SV)等】；功能基因组数据是指遗传物质中除基因组核酸序列数据外的表观遗传数据以及基因空间位置数据等。

[来源：GB/T 41806-2022《信息安全技术 基因识别数据安全要求》]

基因识别数据范围可参见《信息安全技术 基因识别数据安全要求》的附录 A。

加密

Encipherment; Encryption

对数据进行密码变换以产生密文的过程。

[来源：GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》]

健康医疗数据

Health Data

个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关电子数据。

示例：经过对群体健康医疗数据处理后得到的群体总体分析结果、趋势预测、疾病防治统计数据等。

[来源：GB/T 39725-2020《信息安全技术健康医疗数据安全指南》]

关联词：个人健康医疗数据

健康医疗大数据

Healthcare Big Data*

在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。

[来源：《国家健康医疗大数据标准、安全和服务管理办法（试行）》，2018]

交通运输政务数据

Transportation Administrative Data*

是指政务部门在履行职责过程中直接或通过第三方依法采集、产生、获取的，以电子形式记录、保存的各类非涉密数据、文件、资料和图表等。

[来源：《交通运输政务数据共享管理办法》，2021]

接入网络

Access Network*

是指通过接入互联网络进行国际联网的计算机信息网络。

[来源：《计算机信息网络国际联网管理暂行规定》，1996]

结构化

Structured

具备一定的规则、格式或模式，使得软件能够提取数据的特定元素的数据组织方式。例如在电子表格中，数据以行和列的方式表示。结构化数据通常是由已定义好的架构、模板、字段等组成，其中每个数据元素都有特定的含义和类型，并严格遵循特定的格式、约定和标准，以便于被计算机等程序自动处理和解释。

[来源：《数据安全技术 基于个人请求的个人信息转移要求》（征求意见稿），2024]

结构化数据

Structured Data*

一种数据表示形式，按此种形式，由数据元素汇集而成的每个记录的结构都是一致的并且可以使用关系模型予以有效描述。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：半结构化数据，非结构化数据

境外接收方

Overseas Recepient

在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。

[来源：《个人信息出境标准合同》，2022]

中国版标准合同在境外接收方义务中，规定了“受个人信息处理者委托处理个人信息”

的义务，说明受托人也可以是境外接收方。根据目前的实践，境外接收方可能是处理者或者受托处理者。

境外机构指定代表

Designated Representative of Overseas Institutions*

本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

[来源：《个人信息保护法》，2021]

注：根据《网络数据安全管理条例》，境外机构指定代表的报送对象为所在地设区的市级网信部门。

金融数据

Financial Data

金融业机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据。

[来源：JR/T 0197-2020《金融数据安全 数据安全分级指南》]

金融账户信息

Financial Account Information*

金融账户信息是指金融账户及金融账户相关信息，包括但不限于支付账号、银行卡磁道数据（或芯片等效信息）、证券账户、基金账户、保险账户、其他财富账户、公积金账户、公积金联名账号、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等。

[来源：《网络安全标准实践指南——网络数据分类分级指引》，2021]

聚合数据

Aggregate Data

表征一组个人信息主体的数据。例如各种统计值的集合。

[来源：GB/T 37964—2019 《信息安全技术 个人信息去标识化指南》]

具有舆论属性或社会动员能力的互联网信息服务

Internet-based Information Services Capable of Shaping Public Opinion or Mobilizing the Public*

具有舆论属性或社会动员能力的互联网信息服务，包括下列情形：

（一）开办论坛、博客、微博客、聊天室、通讯群组、公众账号、短视频、网络直播、信息分享、小程序等信息服务或者附设相应功能；

（二）开办提供公众舆论表达渠道或者具有发动社会公众从事特定活动能力的其他互联网信息服务。

[来源：《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》，2018]

根据中国法律的规定，“具有舆论属性或社会动员能力”的算法或生成式人工智能，需要履行相应的备案手续。而在实践中，有关部门对于“具有舆论属性或社会动员能力”的理解存在模糊和不一致，目前尚未有明确的判断标准。

-= K =-

开放共享

Sharing and Opening

电信业务经营者、互联网信息服务提供者进行全部或部分数据复制、分享等行为。

[来源：YD/T 3802-2020 《电信网和互联网数据安全通用要求》]

可接受风险阈值

Acceptable Risk Threshold

设定的重标识风险临界数值。当重标识风险大于该数值时就需要采取缓解措施（包括去标识化处理）和应急措施，实现风险在可控范围内。

[来源：GB/T 42460—2023 《信息安全技术 个人信息去标识化效果评估指南》]

可信执行环境

Trusted Execution Environment*

提供基于硬件级的系统隔离和可信根，支持基于技术信任的数据安全保障能力，保证在安全区域内部加载的代码和数据在保密性和完整性方面得到保护。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：隐私保护计算

可用性

Availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[来源：GB/T 25069—2022《信息安全技术 术语》]

可得性

Availability*

可得性是指信息可根据授权实体要求进行访问和使用的特性，即医疗器械产品自身和相关数据能以预期方式适时进行访问和使用。

[来源：《医疗器械网络安全注册审查指导原则（2022 年修订版）》]

可解释性

Explainability

（1）人工智能决策或行为的机制机理可以被人类理解的特性。注 1：可以通过提供说明、进行理论论证等方式提高可解释性。注 2：不可解释是指部分人工智能具有的，在当前技术发展情况下，人难以理解其全部机制机理的属性。[来源：《网络安全标准实践指南—人工智能伦理安全风险防范指引》，2021]

（2）（人工智能）系统以人能理解的方式,表达影响其(执行)结果的重要因素的能力。注：可解释性理解为对“原因"的表达,而不是尝试以“实现必要的优势特性”做出争辩。[来源：GB/ T 41867- 2022《信息技术 人工智能 术语》]

可携带权

Right to Portability

可携带权，也称“个人信息可携带权”或“数据可携带权”（Right to data portability），它是欧盟《一般数据保护条例》第 20 条首次规定的一种新型的数据主体权利，是指自然人对于其同意数据控制者所处理的数据化形式承载的个人信息即个人数据，有权要求该控制者提供结构化的、通用的、机器可读的、能共同操作的以格式形式加以提供的权利，自然人可以将此等个人数据转移给其他的控制者。

[来源：程啸，《个人信息保护法 理解与适用》，2021]

DLaw Hub 知识库拓展资料： 一卡识数 · 可携带权

可信赖

Trustworthiness

（人工智能）满足利益相关方期望并可验证的能力。

注 1：依赖于语境或行业,也依赖于具体的产品或服务,数据以及所用技术,应用不同的可信赖特征并对其进行验证，以确保利益相关方的期望能得到满足。

注 2：可信赖的特征包括可靠性、韧性、安全性(信息安全、功能安全)、隐私性、可问责、透明性、真实性、质量、实用性等。

注 3：可信赖作为一种属性用于描述服务、产品、技术、数据和信息,在治理中也用于组织。

[来源：GB/ T 41867- 2022《信息技术 人工智能 术语》]

科技伦理风险

Technology Ethics Risk*

从伦理视角识别的科学研究、技术开发等科技活动中的风险。最低风险是指日常生活中遇到的常规风险或与健康体检相当的风险。

[来源：《科技伦理审查办法（试行）》，2023]

科技伦理审查委员会

Technology Ethics Review Committee*

从事生命科学、医学、人工智能等科技活动的单位，研究内容涉及科技伦理敏感领域的，应设立科技伦理（审查）委员会。其他有科技伦理审查需求的单位可根据实际情况设立科技伦理（审查）委员会。

该委员会的主要职责包括：（一）制定完善科技伦理（审查）委员会的管理制度和工作规范；（二）提供科技伦理咨询，指导科技人员对科技活动开展科技伦理风险评估；（三）开展科技伦理审查，按要求跟踪监督相关科技活动全过程；（四）对拟开展的科技活动是否属于科技活动清单范围作出判断；（五）组织开展对委员的科技伦理审

查业务培训和科技人员的科技伦理知识培训；（六）受理并协助调查相关科技活动中涉及科技伦理问题的投诉举报；（七）进行登记、报告，配合地方、相关行业主管部门开展涉及科技伦理审查的相关工作。

[来源：《科技伦理审查办法（试行）》，2023]

扩展业务功能

Extended Business Function

移动互联网应用程序所提供的基本业务功能之外的其他业务功能。

[来源：《GBT 41391-2022 信息安全技术 移动互联网应用程序<App>收集个人信息基本要求》]

关联词：业务功能

联邦学习

Federated Learning*

多个参与方在不共享原始数据的情况下协作完成机器学习任务的方法。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：隐私保护计算

领地公开共享

Enclave Public Sharing

在物理成虚拟的领地范围内共享，数据不能流出到领地范围外。同英文术语 The Endme Model。

[来源：GB/T 37964—2019 《信息安全技术 个人信息去标识化指南》]

关联词：完全公开共享，受控公开共享

漏洞 / 安全漏洞

Vulnerability

（1）在资产或缓解措施中，可被一个或多个威胁利用的弱点。[来源：GB 44495-2024《汽车整车信息安全技术要求》]

（2）由于设计、部署、运行或管理错误引发，可因操作失误或恶意利用，给网络产品本身和相关网络系统带来安全破坏的缺陷或弱点。[来源：工业和信息化部网络安全威胁和漏洞信息共享平台问答]

工信部在“工业和信息化部网络安全威胁和漏洞信息共享平台”的官方问答中解释：

“目前在国内外上，对安全漏洞已有较明确定义。从狭义上看，ISO/IEC 21827:2008、ISO/TR 22100-4:2018、ISO/IEC 27000:2018、ISO/IEC TR 24028:2020、我国国家标准 GB/T 39276-2020 等标准中将安全漏洞定义为存在于资产或内部控制中的，可被威胁利用或触

发的安全缺陷。从广义上看，ISO/IEC TR 24772-1:2019 进一步将漏洞存在的位置拓展到 IT 系统、系统安全过程、内部控制或实施等过程中；IETF RFC 4949 将漏洞定义为“存在于系统设计、部署、运行或管理过程，可被利用来对抗系统安全策略的缺陷或弱点”；NIST 在 FISMA、SP800-30 等系列标准中，将漏洞定义为“存在于系统安全过程、设计、部署或内部控制中，可被意外触发或刻意利用，引发安全破坏或违背系统安全策略”；ENISA 将漏洞定义为“在计算机系统、网络、应用或相关协议中存在的，可导致非预期或有害的安全事件的缺陷、设计或实施错误”。

因此，综合考虑安全漏洞被利用后可能对网络产品和网络系统造成的影响，其定义范围应遵循广义定义，涵盖由于设计、部署、运行或管理错误引发，可因操作失误或恶意利用，给网络产品本身和相关网络系统带来安全破坏的缺陷或弱点。”

DLaw Hub 知识库拓展资料： 网络产品安全漏洞管理

漏洞发布

Vulnerability Release

将漏洞信息向社会或受影响的用户等发布的过程。

[来源：GB/T 30276-2020 《信息安全技术 网络安全漏洞管理规范》]

漏洞收录组织

Vulnerability Repository Organization

提供公开渠道接收漏洞信息，并建有相应工作流程的组织。

[来源：GB/T 30276-2020 《信息安全技术 网络安全漏洞管理规范》]

漏洞收集平台

Vulnerability Repositor Platform

相关组织或者个人设立的收集非自身网络产品安全漏洞的公共互联网平台，仅用于修补自身网络产品、网络和系统安全漏洞用途的除外。

[来源：《网络产品安全漏洞收集平台备案管理办法》，2022]

漏洞验证

Vulnerability Verification

对漏洞的存在性、等级、类别等进行技术验证的过程。

[来源：GB/T 30276-2020 《信息安全技术 网络安全漏洞管理规范》]

漏洞应急组织

Vulnerability Emergency Response Organization

与提供者、网络运营者、漏洞收录组织、网络运营者、安全研究机构、网络安全企业等建有成熟的技术协作体系、负责安全漏洞的响应和处置工作的网络安全应急协调组织。

[来源：GB/T 30276-2020 《信息安全技术 网络安全漏洞管理规范》]

鲁棒性

Robustness

（人工智能）系统在任何情况下都保持其性能水平的特性。

[来源：GB/ T 41867- 2022《信息技术 人工智能 术语》]

-= M =-

密态计算

是指通过综合利用密码学、可信硬件和系统安全的可信隐私保护计算技术，其计算过程实现数据可用不可见，计算结果能够保持密态化，以支持构建复杂组合计算，实现计算全链路保障，防止数据泄漏和滥用。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：隐私保护计算

民航数据

Civil Aviation Data*

是指在发展、监管执法、政务管理、生产运行、服务保障等过程中产生的，或通过收集、监测等方式获取并用于民用航空活动的原始数据及其衍生数据。

[来源：《民航数据管理办法（征求意见稿），2024]

敏感个人信息

Sensitive Personal Information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[来源：《个人信息保护法》，2021]

注：2021 前标准中普遍使用的是“个人敏感信息”，而 2021《个人信息保护法》生效后则多使用“敏感个人信息”。

敏感个人信息的示例具体可见《信息安全技术 个人信息安全规范》附录 B、《网络安全标准实践指南 — 敏感个人信息识别指南》附录 A、《敏感个人信息处理安全要求》（征求意见稿）附录 A。值得注意的是，这些标准所列举的敏感个人信息字段有所不同，

可能在一定程度上体现出监管尺度的变化。譬如：

《信息安全技术 个人信息安全规范》	《网络安全标准实践指南 — 敏感个人信息识别指南》	专家解读
身份证	身份证照片	单独的公民身份证号码不是敏感个人信息，但具有完整身份证信息的身份证照片是敏感个人信息。身份证照片的影印件如果能达到体现清晰完整的身份证照片的效果，信息泄露、滥用将可能对个人财产安全造成危害，则构成敏感个人信息。公民身份证号码如果与其他个人信息汇聚融合后，需要综合考虑是否符合指南 3c)条款。
精准定位信息	补充解释“通过调用个人手机精准位置权限采集的位置信息是精准定位信息，通过 IP 地址等测算的粗略位置信息不是精准定位信息”	连续采集的个人精准定位信息可用于生成行踪轨迹，行踪轨迹信息是敏感个人信息。 个人粗略位置信息在实践中一般不认定为敏感个人信息，美国《保护美国人数据免受外国敌对势力侵犯法案》中对于“地理位置信息”的精确度，明确是足以识别个人或设备的街道位置信息，或者个人或设备在 1850 英尺或更小范围内的位置。指南中也规定了，通过 IP 地址等测算的粗略位置信息不是精准定位信息。

《网络安全标准实践指南 — 敏感个人信息识别指南》中具体规定了敏感个人信息的判断标准。符合以下任一条件的个人信息，应识别为敏感个人信息：

1. 一旦遭到泄露或者非法使用，容易导致自然人的人格尊严受到侵害；（注 1：容易导致自然人人格尊严受到侵害的情形可能包括“人肉搜索”、非法侵入网络账户、电

信诈骗、损害个人名誉、歧视性差别待遇等。歧视性差别待遇可能因个人信息主体的特定身份、宗教信仰、性取向、特定疾病和健康状态等信息泄露导致。 ）

2. 一旦遭到泄露或者非法使用，容易导致自然人的人身安全受到危害；（注 2：例如泄露、非法使用个人的行踪轨迹信息，可能会导致个人信息主体的人身安全受到危害。）

3. 一旦遭到泄露或者非法使用，容易导致自然人财产安全受到危害。（注 3：例如泄露、非法使用金融账户信息，可能会造成个人信息主体的财产损失。）

DLaw Hub 知识库拓展资料： 第二十八条 定义及处理原则

敏感属性

Sensitive Attribute

数据集中需要保护的属性，该属性值的泄露、修改、破坏或丢失会对个人产生损害。

[来源：GB/T 37964—2019 《信息安全技术 个人信息去标识化指南》]

明示同意

Explicit Consent

（1）(expressed consent)个人信息主体明确授权同意，并保留证据。[来源：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保护指南》]

（2）个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。[来源：GB/T 35273—2020 《信息安全技术 个人信息安全规范》]

（3）个人通过书面、口头等方式主动作出声明，或者自主作出肯定性动作，对其个人信息进行处理作出明确授权的行为。注： 肯定性动作包括个人主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。[来源：GB/T42574—2023 《信息安全技术 个人信息处理中告知和同意的实施指南》]

默许同意

Tacit Consent

个人信息主体无明确反对的情况下，认为个人信息主体同意。

[来源：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保护指南》]

目的限制原则

Purpose Limitation Principle*

处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

[来源：《个人信息保护法》，2021]

DLaw Hub 知识库拓展资料： 一卡识数 · 目的限制原则

-= N =-

匿名化

Anonymization

（1）个人信息经过处理，是指个人信息经过处理无法识别特定自然人且不能复原的过程。[来源：《个人信息保护法》，2021]

（2）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或者关联，且处理后的信息不能被复原的过程。[来源：GB/T 35273—2020 《信息安全技术 个人信息安全规范》]

（3）是指对个人信息进行加工，使之无法识别特定个人且不能复原。[来源：《信息安全技术 网络数据处理安全规范》（征求意见稿），2020]

注：个人信息经匿名化处理后所得的信息不属于个人信息。

目前实践中尚未有明确的被公认的匿名化措施。

中国信息通信研究院和北京国际大数据交易所在 2023 年发布了《 数据清洗、去标识化、匿名化业务规程（试行）》。该指南认为“匿名化是指数据经过处理，无法识别特定自然人或相关标识符且不能复原的过程。数据匿名化处理在强调标识符的“不可识别性”基础上，要求标识符同时满足“难以复原性”标准，是数据去标识化的进一步处理。”、“去标识化技术和匿名化技术没有严格界分，二者核心都是通过技术手段对标识信息进行脱敏处理，实现对敏感数据内容的保护”。

同时，该指南明确了数据匿名化的目的是**“将原始数据相关标识符的可识别性降低到监管和组织可接受的风险水平。如果信息主体和相关标识符的识别需要不合理的时间、努力或资源，则不视为是可复原的。”**组织需要综合考虑数据因素和环境因素去判断匿名化的效果，例如使用 K-匿名值的计算方法。

DLaw Hub 知识库拓展资料：匿名化与去标识化

关联词：去标识化

-= P =-

披露

Disclosure

将健康医疗数据向特定个人或组织进行转让、共享，以及向不特定个人、组织或社会公开发布的行为。

[来源：GB/T 39725-2020《信息安全技术健康医疗数据安全指南》]

偏好数据标注

Comparison Data Annotation

针对同一个提示信息的正反例或多个不同的响应信息，标注人员根据偏好给出打分或者排序标注的数据标注，通过强化学习等方式提升生成式人工智能模型的性能或安全性。

[来源：《信息安全技术 生成式人工智能数据标注安全规范（征求意见稿）》，2024]

关联词：数据标注

平台 / 互联网平台

Internet Platform*

本指南所称平台为互联网平台，是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。

[来源：《互联网平台落实主体责任指南（征求意见稿）》，2021]

平台经营者

Platform Operator*

向自然人、法人及其他市场主体提供经营场所、交易撮合、信息发布等互联网平台服

务的法人及非法人组织。通过互联网等信息网络从事销售商品或者提供服务的自建网站经营者，可参照平台经营者适用本指南。

[来源：《互联网平台落实主体责任指南（征求意见稿）》，2021]

平台内经营者

Operator on the Platform*

在互联网平台内提供商品或者服务的经营者。平台经营者在运营平台的同时，也可能直接通过平台提供商品或服务。

[来源：《互联网平台落实主体责任指南（征求意见稿）》，2021]

平台灵活就业人员

Platform Flexible Workers*

接受互联网平台经营者提供的工作机会和任务，付出劳动并且获取劳动报酬，在劳动过程中接受互联网平台经营者管理的自然人。

[来源：《互联网平台落实主体责任指南（征求意见稿）》，2021]

-= Q =-

汽车数据

Viechle Data*

包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。

[来源：《汽车数据安全管理若干规定（试行）》，2021]

汽车数据处理者

Viechle Data Processor*

指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

[来源：《汽车数据安全管理若干规定（试行）》，2021]

请求人

Requester

发起个人信息转移请求的主体。包括个人信息主体本人、个人信息主体的监护人及受个人信息主体委托发起转移请求的受托人。

[来源：《数据安全技术 基于个人请求的个人信息转移要求》（征求意见稿），2024]

去标识化

De-identification

（1）个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。[来源：《个人信息保护法》，2021]

（2）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，无法识别或者关联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。[来源：GB/T 35273—2020 《信息安全技术 个人信息安全规范》]

去标识化的技术方式和效果可见 GB/T 37964-2019《信息安全技术 个人信息去标识化指南》，GB/T 42460-2023《信息安全技术 个人信息去标识化效果评估指南》和《 数据清洗、去标识化、匿名化业务规程（试行）(2023)》。

DLaw Hub 知识库拓展资料： 匿名化与去标识化

关联词： 匿名化；标识符

去标识化技术

De-Identification Technique

降低数据集中信息和个人信息主体关联程度的技术。

注 1：降低信息的区分度，使得信息不能对应到特定个人，更低的区分度是不能判定不同的信息是否对应到同一个人。

注 2：断开和个人信息主体的联系，即将个人其他信息和标识信息分离。

[来源：GB/T 37964—2019 《信息安全技术 个人信息去标识化指南》]

去标识化模型

De-Identification Model

应用去标识化技术并能计算重标识风险的方法。

[来源：GB/T 37964—2019 《信息安全技术 个人信息去标识化指南》]

权限

Premission

移动智能终端操作系统向移动互联网应用程序开放的，具有收集个人信息功能的系统权限。

[来源：GB/T 43739—2024 《网络安全技术　应用商店的移动互联网应用程序<App>个人信息处理规范性审核与管理指南 》]

权限申请

System Permission Request

移动互联网应用程序向移动智能终端操作系统声明，并向用户请求授权，以获得访问数据或功能的许可的过程。

[来源：GBT 41391-2022《信息安全技术 移动互联网应用程序<App>收集个人信息基本要求》]

-= R =-

热更新

Hot Update*

在不重新下载和安装 App 的情况下，通过动态加载的方式更新 App 中的代码或资源文件，实现 App 功能的更新。

[来源：《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》，2020]

人工智能

Artificial Intelligence

利用计算机或其控制的设备，通过感知环境、获取知识、推导演绎等方法，对人类智能的模拟、延伸或扩展。

[来源：《网络安全标准实践指南—人工智能伦理安全风险防范指引》，2021]

人工智能生成合成内容

Content Generated by Artificial Intelligence

利用深度学习、虚拟现实等生成合成类算法制作的文本、图像、音频、视频等内容。

[来源：《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》，2024]

人工智能生成合成内容标识

Label of Content Generated by Artificial Intelligence

标识表明某个内容是人工智能生成合成内容的信息。注：标识中还可包含生成合成服务提供者和内容传播服务提供者等信息。

[来源：《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》，2024]

关联词： 显示标识，隐式标识

人脸识别数据

Facial Recognition Data*

可识别自然人身份的人脸图像或人脸特征。

[来源：GB/T 41819—2022《信息安全技术　人脸识别数据安全要求》]

人脸特征

Facial Features*

从人脸图像提取的反映自然人脸部信息特征的参数。

[来源：GB/T 41819—2022《信息安全技术　人脸识别数据安全要求》]

人脸图像

Facial Image*

自然人脸部信息的模拟或数字表示。

[来源：GB/T 41819—2022《信息安全技术　人脸识别数据安全要求》]

人类遗传资源材料

Human Genetic Resource Materials*

（1）含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。[来源：《中华人民共和国人类遗传资源管理条例》，2024]

（2）人类遗传资源材料包括所有类型细胞、全血、组织/组织切片、精液、脑脊液、胸/腹腔积液、血/骨髓涂片、毛发（带毛囊）等，其他不含细胞的人体分泌物、体液、拭子等无需申报。[来源：《中国人类遗传资源国际合作临床试验备案范围和程序》，

2023]

DLaw Hub 知识库拓展资料： 人类遗传资源管理

人类遗传资源信息

Human Genetic Resource Information*

（1）利用人类遗传资源材料产生的数据等信息资料。[来源：《中华人民共和国人类遗传资源管理条例》，2024]

（2)人类遗传资源信息包括利用人类遗传资源材料产生的人类基因、基因组数据等信息资料。前款所称人类遗传资源信息不包括临床数据、影像数据、蛋白质数据和代谢数据。[来源：《人类遗传资源管理条例实施细则》，2023]

（3）人类遗传资源信息包括基因、基因组、转录组、表观组及 ctDNA 等核酸类生物标志物等数据信息，以及与此数据相关的疾病、人种等关联信息，其他不含人类遗传资源基因信息数据类型无需申报。[来源：《中国人类遗传资源国际合作临床试验备案范围和程序》，2023]

DLaw Hub 知识库拓展资料： 人类遗传资源管理

软件开发工具包

SDK

协助软件开发的相关二进制文件、文档、范例和工具的集合，简称 SDK。本指南中的 SDK，是指对实现 App 特定功能的代码进行封装，向外提供简捷的调用接口的二进制文件。

[来源：《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》，2020]

关联词： 第三方软件开发工具包

软件开发工具包提供者

SDK Provider

软件开发工具包的开发者、运营者或所有者，简称 SDK 提供者。

[来源：《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》，2020]

软件升级

Software Update

将某版本的软件通过升级包更新到新版本（包括更改软件的配置参数）的过程。

注 1：“软件升级”也称“软件更新”。

注 2：“软件升级”包含在线升级和离线升级。

[来源：GB 44496-2024《汽车软件升级通用技术要求》]

-= S =-

删除

Delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

[来源：GB/T 35273—2020《信息安全技术 个人信息安全规范》]

目前技术上对于删除的要求，未见较为明确的通用规定。《JR/T 0223-2021 金融数据安全 数据生命周期安全规范》对“数据删除”和“数据销毁”提供了较为具体的规范。我们理解数据销毁比删除的要求更加严格。

DLaw Hub 知识库拓展资料： 第四十七条 删除权

关联词： 销毁

商用密码

Commercial Cipher*

商用密码，是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。

[来源：《商用密码管理条例》，2023]

身份认证信息

Identity Verification Information*

是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。

[来源：《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》，2011]

深度合成技术

Deep Synthesis Technology*

是指利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息的技术，包括但不限于：

（一）篇章生成、文本风格转换、问答对话等生成或者编辑文本内容的技术；

（二）文本转语音、语音转换、语音属性编辑等生成或者编辑语音内容的技术；

（三）音乐生成、场景声编辑等生成或者编辑非语音内容的技术；

（四）人脸生成、人脸替换、人物属性编辑、人脸操控、姿态操控等生成或者编辑图像、视频内容中生物特征的技术；

（五）图像生成、图像增强、图像修复等生成或者编辑图像、视频内容中非生物特征的技术；

（六）三维重建、数字仿真等生成或者编辑数字人物、虚拟场景的技术。

[来源：《互联网信息服务深度合成管理规定》，2022]

深度合成服务技术支持者

Deep Synthesis Service Technical Supporter*

是指为深度合成服务提供技术支持的组织、个人。

[来源：《互联网信息服务深度合成管理规定》，2022]

深度合成服务使用者

Deep Synthesis Service User*

是指使用深度合成服务制作、复制、发布、传播信息的组织、个人。

[来源：《互联网信息服务深度合成管理规定》，2022]

深度合成服务提供者

Deep Synthesis Service Provider*

是指提供深度合成服务的组织、个人。

[来源：《互联网信息服务深度合成管理规定》，2022]

深度合成服务备案

Deep Synthesis Service Filing*

《互联网信息服务深度合成管理规定》要求“具有舆论属性或者社会动员能力”的深度合成服务提供者和技术支持者需要通过线上系统（https://beian.cac.gov.cn/#/index）完成深度合成服务备案。国家网信办会定期公示了完成备案的深度合成算法。

具体可参见 **DLaw Hub 知识库拓展资料：** 中国算法备案统计表（更新中）

生成式人工智能技术

Generative Artificial Intelligence Technology*

是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。

[来源：《生成式人工智能服务管理暂行办法》，2023]

对于生成式人工智能技术，主要的规范文件是《生成式人工智能服务管理暂行办法》、《生成式人工智能服务安全基本要求》、《网络安全技术 人工智能生成合成内容标识方法》（征求意见稿）。

生成式人工智能服务使用者

Generative Artificial Intelligence Service User*

是指使用生成式人工智能服务生成内容的组织、个人。

[来源：《生成式人工智能服务管理暂行办法》，2023]

生成式人工智能服务提供者

Generative Artificial Intelligence Service Provider*

是指利用生成式人工智能技术提供生成式人工智能服务（包括通过提供可编程接口等方式提供生成式人工智能服务）的组织、个人。

[来源：《生成式人工智能服务管理暂行办法》，2023]

生成式人工智能备案

Generative Artificial Intelligence Filing*

又俗称为“大模型备案”。《生成式人工智能服务管理暂行办法》要求“具有舆论属性或者社会动员能力”的生成式人工智能服务提供者在提供服务前进行安全评估并完成备案。目前实践中，服务提供者需要线下向所在地的省级网信办进行备案。国家网信办和地方网信办会定期公示了完成备案的生成式人工智能。

DLaw Hub 知识库拓展资料： 中国算法备案统计表（更新中）

生成式人工智能登记

Generative Artificial Intelligence Registration*

对于通过 API 接口或其他方式直接调用已备案大模型能力的生成式人工智能应用或功能，在满足国家相关法律法规的前提下，经省互联网信息办公室同意，将采用登记方式，发放上线编号后，可直接上线提供服务。后期运行过程中如出现违规行为，将视情通知开展备案。国家网信办和地方网信办会定期公示了完成登记的生成式人工智能。

DLaw Hub 知识库拓展资料： 中国算法备案统计表（更新中）

生物特征识别

Biometric Recognition; Biometrics

基于个体的生物学特性和行为特性对该个体的自动识别。

注 1：在生物特征识别领域“个体”的范围仅指人类。

注 2：Biometrics 的一般含义包括生物科学(包括相关医学科学)中各种类型数据的计数、测量和统计分析。

注 3：生物特征识别包括生物特征验证和生物特征辨识。

注 4：自动识别意味着基于机器的系统用于整个过程或有人类辅助的过程。

注 5：行为和生物学特性无法完全分开,这就是为什么该定义使用“和”而不是“和/或”的原因。例如,指纹图像是由手指脊纹的生物学特性和呈现手指的行为引起的。

注 6：弃用“鉴别"作为“生物特征验证"或“生物特征辨识"的同义词:优先术语是生物特征识别

[来源：GB/T 5271.37-2021《信息技术 词汇 第 37 部分:生物特征识别》]

生物特征数据

Biometric Data

处于任何处理阶段的生物特征样本或生物特征样本的集合，例如，生物特征参考、生物特征探针、生物特征项或生物特征属性。注：生物特征数据不需要归属于特定个体，例如，通用背景模型。

[来源：GB/T 5271.37-2021 《信息技术 词汇 第 37 部分:生物特征识别》]

身份认证信息

Identity Verification Information*

是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。

[来源：《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》]

识别

Identification

在一个特定域中辨认出一个实体区别于其他实体的过程。

注 1：识别过程适用于对所声称的或观察到的属性进行验证。注 2：标别通常是一个域中某一实体和各服务之间交互以及对资源访问的组成部分。实体在域中已知时，识别能发生多次。

[来源：ISO/IEC 24760-1:2011 《信息技术——安全技术——身份管理框架第 1 部分:术语和概念》]

使用

Usage

通过自动或非自动方式对个人信息进行操作，例如记录、组织、排列、存储、改编或变更、检索、咨询、披露、传播或以其他方式提供、调整或组合、限制、删除等。

[来源：《互联网个人信息安全保护指南》，2019]

关联词：个人信息处理/处理

收集

Collection

获得对个人信息的控制权的行为。

注 1： 包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为， 以及通过共享、 转让、搜集公开信息等间接获取个人信息等行为。

注 2： 如果产品或服务的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，如不回传至软件提供者，则不属于个人信息收集行为。又例如手机银行客户端应用软件在终端获取用户指纹特征信息用于本地鉴权后，指纹特征信息不

回传至提供者，则不属于用户指纹特征信息的收集行为。

[来源：GB/T 35273-2020 《信息安全技术　个人信息安全规范》]

关联词：个人信息处理/处理

受控公开共享

Controlled Public Sharing

通过数据使用协议对数据的使用进行约束。例如通过协议禁止信息接收方进行对数据集中个体的重标识攻击，禁止信息接收方关联到外部数据集或信息，禁止信息接收方未经许可共享数据集。

注 2：同英文术语 The Data Use Agreement Models。

[来源：GB/T 37964—2019 《信息安全技术　个人信息去标识化指南》]

关联词：领地公开共享，完全公开共享

受托处理者

Entrusted Processor*

指接受个人信息处理者委托，按照约定处理个人信息的组织、个人。个人信息处理者需要与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。受托处理者不得超出约定的处理目的、处理方式等处理个人信息。

[来源：《个人信息保护法》，2021]

相当于 GDPR 项下中的“数据处理者”（data processor）

关联词：个人信息处理者

授权同意

Consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为。包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

[来源：GB/T 35273—2020 《信息安全技术　个人信息安全规范》]

注：　GB/T 35273—2020 明确将“授权同意”修改为了“同意”，即两者所指一致。

数据

Data

（1）任何以电子或者其他方式对信息的记录。[来源：《数据安全法》，2021]

（2）关于可感知或可想象到的任何事物的事实。[来源：《信息安全事件分类分级指南（征求意见稿），2021]

（3）任何以电子或其他方式对信息的记录。数据在不同视角下表现为原始数据、衍生数据、数据资源、数据产品、数据资产、数据要素等形式。[来源：《数据领域名词解释（征求意见稿）》，2024]

关联词：信息

数据安全

Data Security

（1）通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。[来源：《数据安全法》，2021]

（2）通过采取必要措施，对数据处理活动和数据应用场景进行管理与控制，确保数据始终处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。[来源：《银行保险机构数据安全管理办法（征求意见稿）》，2024]

（3）通过管理和技术措施，确保数据有效保护和合规使用的状态。[来源：GB／ T 37988—2019《信息安全技术　数据安全能力成熟度模型》]

数据安全风险

Data Security Risk

数据安全事件的发生可能性及其对国家安全、公共利益或者组织、个人合法权益造成的影响。

[来源：GB/T 20984-2022《信息安全技术 信息安全风险评估方法》]

数据安全风险评估

Data Security Risk Assessment

对数据和数据处理活动安全进行信息调研、风险识别、风险分析和风险评价的整个过程。

[来源：GB/T 20984-2022《信息安全技术 信息安全风险评估方法》]

数据安全能力

Data Security Capability*

组织在组织建设，制度流程、技术工具以及人员能力等方面对数据的安全保障。

[来源：GB/T 37988-2019《数据安全能力成熟度模型》]

数据安全管理认证

Data Security Management Certification*

是对网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等处理活动进行认证，认证依据是 GB/T 41479《信息安全技术 网络数据处理安全要求》及相关标准规范。

[来源：《数据安全管理认证实施规则》，2022]

DLaw Hub 知识库拓展资料： 数据保护相关认证

数据安全事件

Data Security Incident*

是指数据遭篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成危害的事件。

[来源：《工业和信息化领域数据安全事件应急预案（试行）》，2024]

关联词：网络安全事件；网络安全突发事件；个人信息泄露；信息安全事件

DLaw Hub 知识库拓展资料：数据泄露 / 网络安全事件

数据保护能力

Data Protection Capability

网络运营者在数据的存储、处理、传输过程中确保数据安全的能力。

[来源：《信息安全技术 数据出境安全评估指南（征求意见稿）》，2017]

数据标注

Data Labeling

（1）给数据样本制定目标变量和赋值的过程。[来源：GB/ T 41867- 2022《信息技术 人工智能 术语》]

（2）通过人工操作或使用自动化技术机制，基于对提示信息的响应信息内容，将特定信息如标签、类别或属性添加到文本、图片、音频、视频或者其他数据样本的过程。[来源：《信息安全技术 生成式人工智能数据标注安全规范（征求意见稿）》，2024]

根据《信息安全技术 生成式人工智能数据标注安全规范（征求意见稿）》，数据标注分为功能性数据标注、安全性数据标注、微调训练数据标注和偏好数据标注。

关联词：功能性数据标注；安全性数据标注；微调训练数据标注；偏好数据标注。

数据仓库

Data Warehouse*

是指一个面向主题的、集成的、相对稳定的、反映历史变化的数据集合，通常用于支持企业或组织的决策分析处理。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据产品

Data Product*

基于数据加工形成的，可满足特定需求的数据加工品和数据服务。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据出境 / 数据跨境流动

Cross Border Data Transfer (CBDT)

（1）数据出境行为包括：（一）数据处理者将在境内运营中收集和产生的数据传输至境外；（二）数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；（三）符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他数据处理活动。[来源：《数据出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》，2024]

（2）境外数据经由中华人民共和国中转，未经任何变动或加工处理的情形不属于数据出境。[来源：《信息安全技术 数据出境安全评估指南》（征求意见稿），2017]

数据出境安全评估

CBDT Security Assessment*

个人信息与重要数据出境的合法途径之一。2024 年 3 月发布的《规范和促进数据跨境流动规定》明确了两种应当申报数据出境安全评估的条件：（一）是关键信息基础设施运营者向境外提供个人信息或者重要数据。（二）是关键信息基础设施运营者以

外的数据处理者向境外提供重要数据，或者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息。

DLaw Hub 知识库拓展资料： “数据出境安全评估”

数据出境标准合同备案

CBDT SCC Filing*

个人信息与重要数据出境的合法途径之一。2024 年 3 月发布的《规范和促进数据跨境流动规定》明确，同时符合下列情形的应当向所在地省级网信部门备案：（一）关键信息基础设施运营者以外的数据处理者；（二）自当年 1 月 1 日起，累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）的；且（三）自当年 1 月 1 日起，累计向境外提供不满 1 万人敏感个人信息的。

DLaw Hub 知识库拓展资料： “数据出境标准合同”

数据处理

Data Processing

在数据处理活动中自主决定处理目的和处理方式的个人和组织。

相当于“个人信息处理”。

数据处理者

Data processor

数据收集、存储、使用、加工、传输、提供、公开、删除等活动。

相当于“个人信息处理者”。

数据分类分级

Data Classification and Grading

《中华人民共和国数据安全法》明确规定“国家建立数据分类分级保护制度”，提出“根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、损毁、泄露或者非法获取、非法使用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。”

关联词：核心数据；重要数据

数据分析

Data Analysis*

是指利用技术手段，对数据进行分析，发挥数据作用、释放数据价值的过程。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据湖

Data Lake*

是指一种高度可扩展的数据存储架构，它专门用于存储大量原始数据，这些数据可以来自各种来源并以不同的格式存在，包括结构化、半结构化和非结构化数据。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据交互

Data Interaction*

主体之间以数据的形式进行交流和协作的过程。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据交易

Data Transactions*

数据供方和需方之间进行的，以数据或者数据各类形态为标的的交易行为。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据交易所

Data Exchange*

（1）为数据集中交易提供场所和基础设施，组织和管理数据交易活动的组织机构。简称交易所。[来源：《信息安全技术 数据交易服务安全要求》征求意见稿，2023]

（2）数据交易场所是指经依法批准设立，组织开展数据交易活动的交易场所。[来源：《贵州省数据流通交易促进条例》，2024]

数据可视化

Data Visualization*

是指将数据以图表、图形、地图等可视化形式展示，以便更好地理解和分析数据。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据流通

Data Circulation*

数据在不同主体之间流动的过程，包括数据开放、共享、交易、交换等。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据挖掘

Data Mining*

是数据分析的一种手段，是从大量数据中通过算法搜索隐藏于其中信息的过程。

[来源：《数据领域常用名词解释（第一批）》，2024]

数据脱敏

Data Desensitization

（1）网络运营者对某些敏感数据通过脱敏规则进行数据变形处理，实现对敏感隐私数据的可靠保护。[来源：《信息安全技术 数据出境安全评估指南（征求意见稿）》，2017]

（2）通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。[来源：GB/T 37988-2019《数据安全能力成熟度模型》]

（3）对某些敏感信息通过一定规则进行数据的变形，实现敏感隐私数据的可靠保护。[来源：YD/T 3802-2020 《电信网和互联网数据安全通用要求》]

关联词：匿名化，去标识化

数据要素

Data Elements*

能直接投入到生产和服务过程中的数据，是用于创造经济或社会价值的新型生产要素。

[来源：《数据领域常用名词解释（第一批）》，2024]

DLaw Hub 知识库拓展资料：数据权与数据要素

数据要素市场化配置

Marketization of Data Element Allocation*

通过市场机制来配置数据这一新型生产要素，旨在建立一个更加开放、安全和高效的数据流通环境，不断释放数据要素价值。

[来源：《数据领域常用名词解释（第一批）》，2024]

DLaw Hub 知识库拓展资料：数据权与数据要素

数据治理

Data Governance*

（1）是指银行业金融机构通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值的动态过程。[来源：《银行业金融机构数据治理指引》，2018]

（2）提升数据的质量、安全、合规性，推动数据有效利用的过程，包含组织数据治理、行业数据治理、社会数据治理等。[来源：《数据领域常用名词解释（第一批）》，2024]

数据资产

Data Assest

（1）企业过去的交易或者事项形成的，合法拥有或控制的，能进行计量的，预期会给企业带来经济利益的数据资源；[来源：《数据资产化实践指南》，2024]

（2）特定主体合法拥有或者控制的，能进行货币计量的，且能带来直接或者间接经济利益的数据资源。[来源：《数据领域常用名词解释（第一批）》，2024]

DLaw Hub 知识库拓展资料： 数据资产

数据资产入表

Write Data Assets Into the Balance Sheet*

数据资产入表是指将数据确认为企业资产负债表中“资产”（无形资产 / 存货）一项，在财务报表中体现其真实价值与业务贡献。根据《企业数据资源相关会计处理暂行规定》，企业应当按照企业会计准则相关规定，根据数据资源的持有目的、形成方式、业务模式，以及与数据资源有关的经济利益的预期消耗方式等，对数据资源相关交易和事项进行会计确认、计量和报告。

数据资源

Data Resources*

具有使用价值的数据，是可供人类利用的新型资源。

[来源：《数据领域常用名词解释（第一批）》，2024]

书面同意

Written Consent*

书面形式是合同书、信件、电报、电传、传真等可以有形地表现所载内容的形式。以电子数据交换、电子邮件等方式能够有形地表现所载内容，并可以随时调取查用的数据电文，视为书面形式。

[来源：《中华人民共和国民法典》，2024]

数字产业化

Industrialization of Digital*

新一代移动通信、人工智能等数字技术向数字产品、数字服务转化，数据向资源、要素转化，形成数字新产业、新业态、新模式的过程。

[来源：《数据领域常用名词解释（第一批）》，2024]

数字消费

Digital Consumption*

数字新技术、新应用支撑形成的消费活动和消费方式，既包括对数智化技术、产品和服务的消费，也包括消费内容、消费渠道、消费环境的数字化与智能化，还包括线上线下深度融合的消费新模式。

[来源：《数据领域常用名词解释（第一批）》，2024]

双清单

Two Lists*

又名“个人信息保护双清单”，是指“个人信息清单”和“与第三方共享个人信息清单”。最早由《工业和信息化部关于开展信息通信服务感知提升行动的通知》在 2021 年提出，要求企业设立双清单，并在 APP 二级菜单中展示，方便用户查询。后该项要求也被《网络数据安全管理条例》继承，成为更加普遍的要求。

算法推荐技术

Algorithm Recommendation Technology*

是指利用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术向用户提供信息。

[来源：《互联网信息服务算法推荐管理规定》，2022]

此外，团体标准 T/TAF 138—2022《App 推荐算法用户权益保护技术要求及测评规范》的附录 A 列举了常见的推荐算法应用。

关联词：个性化展示；个性化推荐；定向推送；自动化决策；用户画像

算法备案

Algorithm Filing*

广义上的算法备案包括：互联网信息服务算法备案、深度合成服务备案和生成式人工智能备案。

狭义上的算法备案则专门指互联网信息服务算法备案。《互联网信息服务算法推荐管理规定》要求“具有舆论属性或者社会动员能力”的算法推荐服务提供者需要通过线上系统（https://beian.cac.gov.cn/#/index）完成互联网信息服务算法备案。国家网信办会定期公示了完成备案的算法推荐应用。

DLaw Hub 知识库拓展资料：中国算法备案统计表（更新中）

关键词：深度合成服务备案；生成式人工智能备案

特定身份信息

Personal Information of Specific Identities

对个人人格尊严和社会评价有重大影响的身份信息。注：主要包括民族、种族、犯罪记录、残障人士身份信息、身份证件号码等。

[来源：《敏感个人信息处理安全要求（征求意见稿）》，2023]

提供

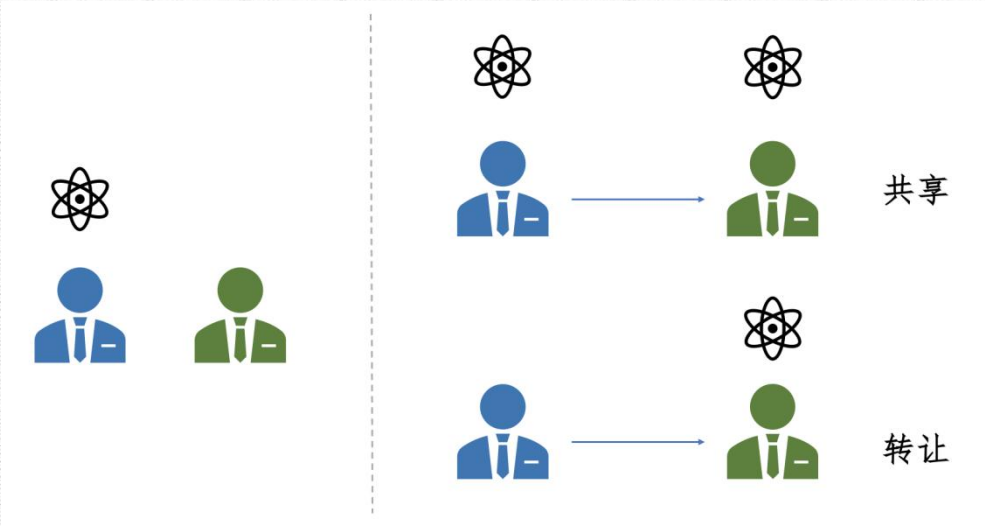
Provide

个人信息处理者通过共享、转移等方式将个人信息传输或披露给其他个人信息处理者的行为。委托第三方处理个人信息的，不属于向其他个人信息处理者提供个人信息的行为。

[来源：GB/T 42574—2023《信息安全技术 个人信息处理中告知和同意的实施指南》]

例如，在 APP 与 SDK 之间处理信息的关系中，App 在完成支付业务功能时，需要向嵌入 App 中的支付 SDK 发送相关的支付订单信息，支付 SDK 服务商独立以自己的名义露出、向用户提供支付服务，该过程可视为 App 向“向其他个人信息处理者提供其处理的个人信息”。[来源：CCIA 数据安全工作委员会，《如何理解和规范 App 接入的第三方服务处理个人信息的情形？》]

此外，“提供”行为还经常容易和“共享”与“转移/转让”之间产生混淆。这三个概念都是用来描述数据从一方流向另一方的过程。GB/T 35273—2020《信息安全技术 个人信息安全规范》规定了“共享”和“转让/转移”，而《个人信息保护法》规定了“提供”。而根据 GB/T 42574—2023《信息安全技术 个人信息处理中告知和同意的实施指南》上述的定义，我们倾向于认为“共享”和”转让”都是“提供”的方式之一。其中，转让是指个人信息控制权发生了变化，从 A 到了 B；而共享是指个人信息控制权没有发生变化，个人信息处理者从 A 变成了 A，B（如果 AB 之间存在共同处理的意思，则双方构成共同处理）。



DLaw Hub 知识库拓展资料： 第二十三条 个人信息提供

关联词： 共享；转让；委托处理；共同处理

同意

Consent

个人对其个人信息进行处理自愿、明确作出授权的行为。 包括通过积极的行为作出授权（即明示同意），或者通过个人的行为而推定其作出授权。

[来源：GB/T 42574—2023《信息安全技术 个人信息处理中告知和同意的实施指南》]

GB/T 35273—2020 明确将“授权同意”修改为了“同意”，即两者所指一致。

关联词： 明示同意；单独同意；书面同意

推理

Inference

从给定的前提进行论证并得出结论。

注 1：在人工智能领域中，一个前提是一个事实、一个规则、一个模型、一个特征或原始数据。

注 2：术语“推理”既指过程也指结果。

[来源：GB/ T 41867- 2022《信息技术 人工智能 术语》]

推荐算法

Recommendation Algorithm

利用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术向用户提供信息。 、

[来源：《App 推荐算法用户权益保护技术要求及测评规范》，2021]

注：常见的推荐算法应用可见《App 推荐算法用户权益保护技术要求及测评规范》附录A。

-= W =-

未成年人

Minors*

> 未满十八周岁的公民。
>
> [来源：《未成年人保护法》，2020]

虽然《个人信息保护法》将特殊保护的年龄从十八岁下降到了十四岁，但是更宏观的网络法律层面，中国也出于未成年人保护的目的提出了很多特殊的合规要求，例如未成年人模式。

DLaw Hub 知识库拓展资料： 未成年/儿童个人信息保护

完全公开共享

Completely Public Sharing

> 数据一旦发布，很难召回，一般通过互联网直接公开发布。
>
> [来源：GB/T 37964—2019 《个人信息去标识化指南》]

关联词： 领地公开共享；受控公开共享

完整性

Integrity

> （1）准确和完备的特性。[来源：GB/T 29246—2017]
>
> （2）完整性是指信息的创建、传输、存储、显示未以非授权方式进行更改（含删除、添加）的特性，即医疗器械相关数据是准确和完整的，且未被篡改。[来源：《医疗器械网络安全注册审查指导原则（2022 年修订版）》]

网络

Internet / Network*

由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

[来源：《网络安全法》，2017]

网络安全

Cybersecurity*

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：《网络安全法》，2017]

网络安全保险

Cybersecurity Insurance

财产保险的一种，承保因发生网络安全事件所造成的经济损失以及需承担的法定赔偿责任。 注：网络安全保险属于广义的财产保险范畴，数字资产等无形资产可作为该险种的保险标的。

网络安全保险是组织实现网络安全风险转移的手段，通过补偿组织因网络安全事件可能导致的经济损失，帮助组织管理风险，增强风险应对能力。网络安全事件所造成的经济损失既包含组织自身的损失，也包含对第三者的赔偿责任。与传统财产保险以有形财产及其相关经济利益为保险标的不同，网络安全保险的保险标的既包括有形财产，也包括无形财产。网络安全保险主要承保网络空间的安全风险，如网络攻击、恶意程序、 系统功能错误或失效等。

网络安全保险的作用包括：a）补偿网络安全事件所导致的经济损失，降低潜在影响；b）预防和减少网络安全事件造成的损失和危害； c）为应急响应及恢复提供资金支持； d）协助组织恢复正常运营； e）提高对网络安全事件的韧性； f）降低网络安

全风险管理的总体成本。

[来源：《信息安全技术 网络安全保险应用指南（征求意见稿）, 2023]

网络安全从业人员

Cybersecurity Workforce

从事网络安全工作，承担相应网络安全职责，并具有相应网络安全知识和技能的人员。

[来源：GB/T 42446-2023《信息安全技术 网络安全从业人员能力基本要求]

网络安全审查

Cybersecurity Review

为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，由国家互联网信息办公室会同其他有关主管部门，针对法律规定的特定对象，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。

[来源：《网络安全审查办法》, 2021]

网络安全审查是中国政府为了确保网络安全和数据安全，依据《网络安全审查办法》施行的审查制度。该制度重点对（可能）影响国家安全的行为进行审查，包括：（1）关键信息基础设施运营者采购网络产品和服务；（2）数据处理者开展数据处理活动；（3）掌握超过 100 万用户个人信息的网络平台运营者赴国外上市。

DLaw Hub 知识库拓展资料： 一卡识数 · 网络安全审查

网络安全事件

Cybersecurity Incident

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

[来源：《国家网络安全事件应急预案》，2017]

《国家网络安全事件应急预案》和《网络安全事件报告管理办法》（征求意见稿）附件的《网络安全事件分级指南》都将网络安全事件划为“特别重大”、“重大”、“较大”和“一般”四个级别，并提供了分级标准。

关联词：数据安全事件；网络安全突发事件；个人信息泄露；信息安全事件

DLaw Hub 知识库拓展资料：数据泄露 / 网络安全事件

网络安全事件应急演练

Cybersecurity Incident Emergency Exercises

有关政府部门,企事业单位,社会团体组织相关人员,针对设定的突发事件模拟情景,按照应急预案所规定的职责和程序,在特定的时间和地域,开展应急处置的活动。

[来源：GB/T 38645-2020《信息安全技术 网络安全事件应急演练指南》]

网络安全突发事件

Cybersecurity Emergency Incident*

突然发生的，由网络攻击、网络入侵、恶意程序等导致的，造成或可能造成严重社会危害或影响，需要电信主管部门组织采取应急处置措施予以应对的网络中断（拥塞）、系统瘫痪（异常）、数据泄露（丢失）、病毒传播等事件。

[来源：《公共互联网网络安全突发事件应急预案》，2017]

根据社会影响范围和危害程度，《公共互联网网络安全突发事件应急预案》将公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件，并且提供了详细的分级标准。

我们倾向于认为网络安全突发事件与网络安全事件均是对同一事物的描述。

关联词：数据安全事件、网络安全事件、个人信息泄露

DLaw Hub 知识库拓展资料：数据泄露 / 网络安全事件

网络产品和服务

Network Products and Services*

主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。

[来源：《网络安全审查办法》，2021]

网络数据

Network Data*

（1）通过网络收集、存储、传输、处理和产生的各种电子数据。[来源：《网络安全法》，2017]

（2）通过网络收集、存储、使用、加工、传输、提供、公开的各种数据。示例：个人信息、重要数据等。[来源：GB/T 41479—2022《信息安全技术 网络数据处理安全要求》]

（3）通过网络处理和产生的各种电子数据， 简称“数据”。[来源：《网络安全标准实践指南—网络数据安全风险评估实施指引》，2023]

网络音视频服务

Online Audio and Video Service

通过互联网站、应用程序等网络平台,向社会公众提供音视频信息制作、发布、传播的服务。

注 1：也称网络音视频信息服务。

注 2：不包括音视频编辑工具、本地播放器和具有即时通信属性的在线直播（如在线会议）服务。

[来源：GB/T 42016-2022《信息安全技术 网络音视频服务数据安全要求》]

网络运营者

Network Operator

网络的所有者、管理者和网络服务提供者。

[来源：《网络安全法》，2017]

违法不良信息

Illegal and Unhealthy Information

《网络信息内容生态治理规定》中指出的11类违法信息以及9类不良信息的统称。

违法信息包括：（一）反对宪法所确定的基本原则的；(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；(三)损害国家荣誉和利益的；(四)歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；(五)宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；(六)煽动民族仇恨、民族歧视，破坏民族团结的；(七)破坏国家宗教政策，宣扬邪教和封建迷信的；(八)散布谣言，扰乱经济秩序和社会秩序的；(九)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；(十)侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；(十一)法律、行政法规禁止的其他内容。

不良信息包括：（一）使用夸张标题，内容与标题严重不符的；(二)炒作绯闻、丑闻、劣迹等的；(三)不当评述自然灾害、重大事故等灾难的；(四)带有性暗示、性挑逗等易使人产生性联想的；(五)展现血腥、惊悚、残忍等致人身心不适的；(六)煽动人群歧视、地域歧视等的；(七)宣扬低俗、庸俗、媚俗内容的；(八)可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的；(九)其他对网络生态造成不良影响的内容。

[来源：TC260《生成式人工智能服务安全基本要求》，2024]

微数据

Microdata

一个结构化数据集，其中每条（行）记录对应一个个人信息主体，记录中的每个字

段（列）对应一个属性。

[来源：GB/T 37964—2019《信息安全技术　个人信息去标识化指南》]

关联词：标识符

微调

Fine-tuning

为提升人工智能模型的预测精确度，一种先以大型广泛领域数据集训练，再以小型专门领域数据集继续训练的附加训练技术。

注：常用于解决过拟合问题。

[来源：GB/ T 41867- 2022《信息技术 人工智能 术语》]

微调训练数据标注

Fine-tuning Data Annotation

训练生成式人工智能模型具备完成特定任务或输出安全响应信息能力的数据标注。

[来源：《信息安全技术 生成式人工智能数据标注安全规范（征求意见稿）》，2024]

关联词：数据标注

委托处理

Entrusted Processing*

数据处理者委托第三方按照约定的目的和方式开展的数据处理活动。

[来源：《信息安全技术 重要数据处理安全要求（征求意见稿）》，2023]

例如，在 APP 与 SDK 之间处理信息的关系中，SDK 收集个人信息时无法独立决定对 App 用户数据处理的目的、方式，需遵照与 App 运营者的约定处理个人信息，属于 App 运营者委托 SDK 提供者处理的情形。此时，App 运营者是个人信息处理者、SDK 服务商是受托处理者，告知同意的职责由 App 运营者承担。App 运营者委托 SDK 提供者定

制（包括基于免费版本定制）开发 SDK 的，同样需要满足以上情形，才构成“委托处理”关系。［来源：CCIA 数据安全工作委员会，《如何理解和规范 App 接入的第三方服务处理个人信息的情形？》］

DLaw 知识库链接： 第二十一条 委托处理个人信息

关联词： 共享，受托处理者

唯一设备识别码

Unique Device Identifier

可唯一标识移动智能终端的编码。

注 1：也称设备唯一标识符，可分为可变更的唯一设备识别码和不可变更的唯一设备识别码。

注 2：可变更的唯一设备识别码，是指用户可重置,变更或关闭追踪的唯一设备识别码。不可变更的唯一设备识别码，是指不因设备恢复出厂设置、应用安全卸载或用户操作而改变的硬件标识符。

［来源：GB/T 41391-2022《信息安全技术 移动互联网应用程序<App>收集个人信息基本要求》］

常见的可变更或不可变更的唯一设备识别码可参见《信息安全技术 移动互联网应用程序<App>收集个人信息基本要求》的附录 F 和《APP 收集使用个人信息最小必要评估规范第 5 部分：设备信息》的表格 A，包括：

不可变更的唯一设备识别码	IMEI、IMSI、PEI（5G 系统）、MEID、设备硬件序列号、固定 MAC 地址、固定蓝牙地址、SN、ICCID（SIM Serial Number）等
可变更的唯一设备识别码	Android ID、IDFA、IDFV、GAID、OAID、CAID 等

对于唯一设备识别码，国标要求“定向推送信息和用户画像场景采用唯一设备识别码标识用户时,应使用可变更的唯一设备识别码,且不应将其与用户身份信息或不可变更的唯一设备识别码关联。”

位置轨迹数据

Location Tracking Data*

基于卫星定位、通信网络等各种方式获取的汽车定位和途经路径相关的数据。

[来源：《汽车采集数据处理安全指南》，2021]

物理隔离

Physical Disconnection

处于不同安全域的网络之间不能以直接或间接的方式相连接。注：在一个物理网络环境中，实施不同安全域的网络物理断开，在技术上应确保信息在物理传导、物理存储错上的断开。

[来源：GB/T 20279-2015《信息安全技术 网络和终端隔离产品安全技术要求》]

关联词：协议隔离

物联网

Internet of Things (IOT)

通过感知设备,按照约定协议,连接物、人,系统和信息资源,实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。

[来源：GB/T 33745-2017《物联网术语》]

系统（敏感）权限

System Sensitive Permission

又名“权限”或“系统权限”

关联词：权限

系统损失

System Loss

指由于信息安全事件对信息系统的软硬件、功能及数据的破坏，导致系统业务中断，网络安全受到损害，从而给公民、法人和组织造成的损失。

[来源：《信息安全事件分类分级指南（征求意见稿）》，2021]

消费者金融信息

Consumer Financial Information*

是指银行、支付机构通过开展业务或者其他合法渠道处理的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或者服务相关的信息。

[来源：《中国人民银行金融消费者权益保护实施办法》，2020]

小程序

Mini Program

基于应用程序开放接口实现的,用户无需安装即可使用的移动互联网应用程序。

注：应用程序通过公开其应用程序编程接口（API）或函数，使外部的程序可以增加该应用程序的功能或使用该应用程序的资源，而不需要更改该应用程序的源代码。

[来源：GB/T 41391-2022《信息安全技术 移动互联网应用程序 App 收集个人信息基本要求》]

销毁

Destruction*

（1）通过清除、消磁、粉碎等技术手段使电子信息载体中存储的信息不可再用，且不可恢复的过程。[来源：YD/T 3956-2021《电信网和互联网数据安全评估规范》]

（2）数据销毁是指金融业机构在停止业务服务、数据使用以及存储空间释放再分配等场景下，对数据库、服务器和终端中的剩余数据以及硬件存储介质等采用数据擦除或者物理销毁的方式确保数据无 复原的过程。其中，数据擦除是指使用预先定义的无意义、无规律的信息多次反复写入存储介质的存储数据区域；物理销毁是指采用消磁设备、粉碎工具等设备以物理方式使存储介质彻底失效。[来源：JR/T 0223-2021《金融数据安全 数据生命周期安全规范》]

JR/T 0223-2021《金融数据安全 数据生命周期安全规范》对“数据删除”和“数据销毁”由具体的规范。注意，数据销毁比删除的要求更加严格。

关联词：删除

显式标识

Explicit Label

在人工智能生成合成内容或交互场景界面中添加的，以文字、声音、图形等方式呈现并可被用户直接感知到的标识。

[来源：《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》，2024]

关联词：人工智能生成合成内容标识，隐式标识

协议隔离

Protocol Separation

处于不同安全域的网络在物理上是有连接的，通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。

[来源：GB/T 20279-2015 《信息安全技术 网络和终端隔离产品安全技术要求》]

关联词：物理隔离

信息

Information

（1）有意义的数据。[来源：GB/T 19000-2016 《质量管理体系 基础和术语(高清版)》]

（2）关于客体(如事实、事件、事物、过程或思想，包括概念)的知识，在一定的场合中具有特定的意义。[来源：JR/T 0197-2020《金融数据安全 数据安全分级指南》]

关联词：数据，个人信息

信息安全事件

Information Security Incident

指由于自然或者人为以及软硬件本身缺陷或故障的原因，可能对信息系统造成损害，或对社会造成负面影响的事件。

[来源：《信息安全事件分类分级指南（征求意见稿）》，2021]

关联词：数据安全事件；网络安全事件；网络安全突发事件；个人信息泄露

信息化突发事件

Information Technology Emergency Event*

是指信息系统或信息化基础设施出现故障、受到网络攻击，导致保险中介机构在同一省份的营业网点、电子渠道业务中断 3 小时以上，或在两个及以上省份的营业网点、电子渠道业务中断 30 分钟以上；或者因网络欺诈或其它信息安全事件，导致保险中介机构或客户资金损失 1000 万元以上，或造成重大社会影响；或者保险中介机构丢

失或泄露大量重要数据或客户信息等，已经或可能造成重大损失、严重影响。

[来源：《保险中介机构信息化工作监管办法》，2021]

信息技术系统服务机构 / 信息技术服务机构

Information Technology System Service Provider*

（1）信息技术系统服务机构是指为证券期货业务活动提供重要信息系统的开发、测试、集成、测评、运维及日常安全管理等产品或者服务的机构。[来源：《证券期货业网络和信息安全管理办法》，2023]

（2）信息技术服务机构是指为证券基金业务活动提供信息技术服务的机构。信息技术服务的范围如下：（一）重要信息系统的开发、测试、集成及测评；（二）重要信息系统的运维及日常安全管理；（三）中国证监会规定的其他情形。[来源：《证券基金经营机构信息技术管理办法》，2023]

信息科技外包

Information Technology Outsourcing*

（1）是指银行保险机构将原本由自身负责处理的信息科技活动委托给服务提供商进行处理的行为。[来源：《银行保险机构信息科技外包风险监管办法》，2022]

（2）银行保险机构应当将数据委托处理纳入信息科技外包管理范围，在实施过程中不得将信息科技管理责任、数据安全主体责任外包，涉及信息科技战略管理、信息科技风险管理、信息科技内部审计及其他有关信息科技核心竞争力的职能不得外包。[来源：《银行保险机构数据安全管理办法》（公开征求意见稿），2024]

银行保险机构应对信息科技外包活动及相关服务提供商进行分级管理，对重要外包和一般外包采取差异化管控措施。

信息科技外包服务类型参考：

- 咨询规划类。包括但不限于：信息科技战略规划（含中长期规划）咨询，数据中心（机房）整体建设咨询和规划，信息科技治理（含数据治理）、信息科技风险管理体系、信息安全管理体系、业务连续性管理体系等管理类咨询和规划，重要信息系统架构和建

设相关的咨询和规划，新兴技术应用咨询和规划。

- 开发测试类。包括但不限于：软硬件开发和测试外包（含人力外包），软件即服务形式的外包。

- 运行维护类。包括但不限于：数据中心（机房）物理环境的托管或运行维护，软硬件基础设施托管或运行维护，应用系统运行维护，电子机具运行维护，终端等办公设备的运行维护，以及涉及以上运行维护的人力外包。

- 安全服务类。包括但不限于：安全运营服务，安全加固服务，安全设备运行维护，安全日志处理与分析，安全测试服务，密钥管理及运行维护，数据安全服务，以及涉及以上服务的人力外包。

- 业务支持类。包括但不限于：市场拓展、业务运营（集中作业、呼叫中心等）、企业管理、资产处置、数据处理、数据利用等业务外包或第三方合作当中涉及银行保险机构的重要数据或客户个人信息处理的信息科技活动，法律法规另有要求的除外。

信息系统

Information System

（1）应用 、服务 、信息技术资产或其他信息处理组件。注 1：信息系统通常由计算机或者其他信息终端及相关设备组成，并按照一定的应用目标和规则进行信息处理或过程控制。注 2： 即典型的信息系统如办公自动化系统 、云计算平台/系统、物联网、工业控制系统以及采用移动互联技术的系统等。[来源：GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》]

（2）另注：本文件中信息系统是个广义的概念，包含通信网络设施和数据资源，信息系统既包括办公自动化系统、电信网、广播电视传输网等基础信息网络，也包括云计算平台/系统，物联网、工业控制系统、大数据系统以及采用移动互联技术的系统等。[来源：《信息安全事件分类分级指南（征求意见稿）》，2021]

信息系统安全保障

Information System Security Assurance

信息系统的安全属性及功能、效率进行保障的一系列适当行为或过程。

[来源：GB/T 20274.1-2023《信息安全技术 信息系统安全保障评估框架 第1部分：简介和一般模型》]

信息系统生命周期

Information System Lifecycle*

信息系统的各个生命阶段，包括规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段。

[来源：GB/T 31509-2015《信息安全技术 信息安全风险评估实施指南》]

训练数据 / 训练语料

Training Data

（1）是指被用于训练机器学习模型的标注或者基准数据集。[来源：《互联网信息服务深度合成管理规定》，2022]

（2）所有直接作为模型训练输入的数据，包括预训练、优化训练过程中的输入数据。[来源：TC260《生成式人工智能服务安全基本要求》，2024]

衍生个人信息

Derived Personal Information

根据对个人信息的分析、计算、处理等方式得出的、与个人相关的新数据。这些数据可能与原始数据不同，但仍然属于个人信息，并保留了与个人关联的特性。

[来源：《数据安全技术 基于个人请求的个人信息转移要求》（征求意见稿），2024]

衍生数据

Derived Data

经过统计、关联、挖掘、聚合、去标识化等加工活动而产生的数据。

[来源：GB/T 43697-2024《数据安全技术 数据分类分级规则》]

业务

Business

组织为实现某项发展规划而开展的运营活动。注： 该活动具有明确的目标， 并延续一段时间。

[来源：GB/T 20984-2022《信息安全技术 信息安全风险评估方法》]

业务功能

Business Function

（1）满足个人信息主体的具体使用需求的服务类型。[来源：GB/T 35273—2020《信息安全技术 个人信息安全规范》]

（2）满足用户具体使用目的的功能。一种服务类型通常包括多个业务功能。[来源：《信息安全技术 互联网平台及产品服务隐私协议要求（征求意见稿）》，2022]

注：App 的业务功能可以分为基本业务功能和扩展业务功能。

关联词：基本业务功能；扩展业务功能

业务影响分析

Business Impact Analysis

对业务功能及其相关信息系统资源进行分析，评估特定信息安全事件对各种业务功能的影响的过程。

[来源：GB/T 24363-2009 《信息安全技术 信息安全应急响应计划规范》]

一般数据

General Data

（1）一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人、组织合法权益造成危害，但不会危害国家安全、公共利益的数据。[来源：《网络安全标准实践指南——网络数据分类分级指引》，2021]

（2）核心数据、重要数据之外的其他数据。[来源：GB/T 43697-2024《数据安全技术 数据分类分级规则》]

关联词：重要数据，核心数据

医疗器械网络安全

Medical Device Cybersecurity*

医疗器械网络安全是指保护医疗器械产品自身和相关数据不受未授权活动影响的状态，其保密性（Confidentiality）、完整性（Integrity）、可得性（Availability）相关风险在全生命周期均处于可接受水平。

其中，保密性是指信息不被未授权实体（含产品、服务、个人、组织）获得或知悉的特性，即医疗器械产品自身和相关数据仅可由授权用户在授权时间以授权方式进行访问和使用。完整性是指信息的创建、传输、存储、显示未以非授权方式进行更改（含

删除、添加）的特性，即医疗器械相关数据是准确和完整的，且未被篡改。可得性是指信息可根据授权实体要求进行访问和使用的特性，即医疗器械产品自身和相关数据能以预期方式适时进行访问和使用。

除保密性、完整性、可得性三个基本特性外，医疗器械网络安全还包括真实性（Authenticity）、抗抵赖性（Non-Repudiation）、可核查性（Accountability）、可靠性（Reliability）等特性。其中，真实性是指实体符合其所声称的特性，抗抵赖性是指实体可证明所声称事件或活动的发生及其发起实体的特性，可核查性是指实体的活动及结果可被追溯的特性，可靠性是指实体的活动及结果与预期保持一致的特性。

保密性、完整性、可得性等网络安全特性通常是相互制约的关系，在同等条件下，某一特性的能力提升可能会使得另一特性或多个特性的能力下降，如可得性的提升可能会降低保密性和完整性，因此需要基于产品特性进行平衡兼顾。注册申请人需结合医疗器械的预期用途、使用场景、核心功能进行综合考量，从而确定医疗器械网络安全特性的具体要求。

此外，尽管信息安全、网络安全、数据安全的定义和范围各有侧重，既有联系又有区别，不尽相同，但本指导原则从医疗器械安全有效性评价角度出发对三者不做严格区分，统一采用网络安全进行表述，即从网络安全角度综合考虑医疗器械的信息安全和数据安全。

[来源：《医疗器械网络安全注册审查指导原则（2022 年修订版）》，2022]

医疗器械相关数据

Medical Device-Related Data*

医疗器械相关数据可分为医疗数据和设备数据。

医疗数据是指医疗器械所产生的、使用的与医疗活动相关的数据（含日志），从个人信息保护角度又可分为敏感医疗数据、非敏感医疗数据，其中敏感医疗数据是指含有个人信息的医疗数据，反之即为非敏感医疗数据。个人信息是指以电子或者其他方式记录的能够单独或与其他信息结合识别自然人个人身份的各种信息，如自然人的姓名、出生日期、身份证件号码、个人生物识别信息（含容貌信息）、住址、电话号码等。

设备数据是指记录医疗器械运行状况的数据（含日志），用于监视、控制医疗器械运行或者医疗器械的维护与升级，不得含有个人信息。

注册申请人需基于医疗器械相关数据的类型、功能、用途，结合网络安全特性考虑医疗器械网络安全要求。同时，保证敏感医疗数据所含个人信息免于泄露、滥用和篡改，以及医疗数据和设备数据的有效隔离（如访问权限控制等方法）。

[来源：《医疗器械网络安全注册审查指导原则（2022 年修订版）》，2022]

医疗卫生机构数据

Healthcare Institution Data*

医疗卫生机构通过网络收集、存储、传输、处理和产生的各种电子数据，包括但不限于各类临床、科研、管理等业务数据、医疗设备产生的数据、个人信息以及数据衍生物。

[来源：《医疗卫生机构网络安全管理办法》，2022]

移动互联网应用程序

App

（1）通过预装、下载等方式获取并运行在移动智能终端上、向用户提供服务的应用软件，简称 App。[来源：《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》，2020]

（2）App 包括移动智能终端预置、下载安装的应用软件，基于应用软件开放平台接口开发的、用户无需安装即可使用的小程序。[来源：《常见类型移动互联网应用程序必要个人信息范围规定》，2021]

（3）运行在移动智能终端上向用户提供信息服务的应用软件。[来源：《移动互联网应用程序信息服务管理规定》，2022]

移动互联网应用程序提供者

App Provider

（1）移动互联网应用程序的开发者、运营者或所有者，简称 App 提供者。[来源：《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》，2020]

（2）提供信息服务的移动互联网应用程序所有者或者运营者。[来源：《移动互联网应用程序信息服务管理规定》，2022]

移动互联网应用程序分发平台

APP Distribution Platform*

提供移动互联网应用程序发布、下载、动态加载等分发服务的互联网信息服务提供者。

[来源：《移动互联网应用程序信息服务管理规定》，2022]

移动互联网应用程序（App）安全认证

APP Security Certification*

2019 年 3 月 13 日，市场监管总局、中央网信办发布《关于开展 APP 安全认证工作的公告》，推出 APP 安全认证制度。这是对移动互联网应用程序（以下称“App”）的数据安全认证，认证依据为《信息安全技术个人信息安全规范》及相关标准、规范。

DLaw Hub 知识库拓展资料： 数据保护相关认证

移动智能终端

Smart Mobile Terminal

具有能够提供应用程序开发接口的开放系统，并能够安装和运行第三方应用软件的移动终端。

[来源：GB/T 39720-2020《信息安全技术 移动智能终端安全技术要求及测试评价方法》]

应用程序分发服务

APP Distribution Service*

指通过互联网提供应用程序发布、下载、动态加载等服务的活动，包括应用商店、快应用中心、互联网小程序平台、浏览器插件平台等类型。

[来源：《移动互联网应用程序信息服务管理规定》，2022]

应用（程序）分发平台

APP Distribution Platform

应用分发平台，包括网站、应用商店、APP 等承担下载、安装、升级等分发服务的各类平台。

[来源：TTAF 125—2023《应用分发平台 APP 审核规范》]

根据《移动互联网应用程序信息服务管理规定》，应用程序分发平台应当在上线运营三十日内向所在地省、自治区、直辖市网信部门备案。自 2023 年 9 月 27 日，国家网信办会定期公布已备案的应用程序分发平台。

应用程序信息服务

APP Information Service*

指通过应用程序向用户提供文字、图片、语音、视频等信息制作、复制、发布、传播等服务的活动，包括即时通讯、新闻资讯、知识问答、论坛社区、网络直播、电子商务、网络音视频、生活服务等类型。

[来源：《移动互联网应用程序信息服务管理规定》，2022]

应用商店

App Store

提供移动互联网应用程序下载、安装、升级等分发服务的各类平台。

注：包括应用市场、分发网站、具有分发能力的移动互联网应用程序等。

[来源：GB/T 43739-2024《数据安全技术 应用商店的移动互联网应用程序（App）个人信息处理规范性审核与管理指南》]

隐式标识

Implicit Label

在人工智能生成合成内容数据中添加的，不能被用户直接感知、但能通过技术手段提取的标识。

[来源：《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》，2024]

关联词：人工智能生成合成内容标识，显式标识

隐私保护计算

Privacy Computing*

是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私保护计算的常用技术方案有多方安全计算、联邦学习、可信执行环境、密态计算等；常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

[来源：《数据领域常用名词解释（第一批）》，2024]

关联词：多方安全计算，联邦学习，可信执行环境，密态计算

隐私政策

Privacy Policy

又名“个人信息保护政策”。

用户个人信息

User Personal Information*

是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。

[来源：《电信和互联网用户个人信息保护规定》，2013]

用户标签

User Tag

通过高度概括、容易理解的特征来描述用户在进行信息服务交互过程中形成的标识。

[来源：TTAF 138—2022《App 推荐算法用户权益保护技术要求及测评规范》]

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，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，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。

[来源：GB/T 35273—2020《信息安全标准 个人信息安全规范》]

关联词：个性化展示；个性化推送；定向推送；算法推荐；自动化决策

有用性

Usefulness

数据对于应用有着具体含义、具有使用意义的特性。注：去标识化数据应用广泛，每

种应用将要求去标识化数据具有某些特性以达到应用目的，因此在去标识化后需要保证对这些特性的保留。

[来源：GB/T 37964—2019 《信息安全技术　个人信息去标识化指南》]

关联词：去标识化

预置应用软件

Pre-installed Application

由生产企业预置，在移动智能终端主屏幕和辅助屏界面内存在用户交互入口，为满足用户应用需求而提供的、可独立使用的软件程序。

[来源：GB/T 43445-2023《信息安全技术 移动智能终端预置应用软件基本安全要求》]

元数据

Metadata*

（1）用来定义和描述数据的数据，通过定义和描述数据，可以支持对其所描述的数据对象的定位、查询、交换、追踪、访问控制、评价和保存等诸多管理工作。[来源：《药品记录与数据管理要求（试行）》，2020]

（2）关于数据或数据元素的数据（可能包括其数据描述），以及关于数据拥有权、存取路径、访问权和数据易变性的数据。[来源：《数据领域名词解释》，2024]

原始数据

Raw Data*

（1）初次或源头采集的、未经处理的数据。[来源：《药品记录与数据管理要求（试行）》，2020]

（2）初次或源头收集的、未经加工处理的数据。[来源：《数据领域名词解释》，2024]

云计算

Cloud Computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池,并按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[来源：GB/T 31168-2023《信息安全技术 云计算服务安全能力要求》]

运行数据 / 汽车运行数据

Vehicle Operation Data*

通过车速传感器、温度传感器、轴转速传感器、压力传感器等从动力系统、底盘系统、车身系统、舒适系统等电子电气系统采集的数据。

注 1：运行数据包含整车控制数据、运行状态数据、系统工作参数、操控记录数据等。

[来源：《汽车采集数据处理安全指南》，2021]

-= Z =-

在线升级

Over-the-air Update；OTA Update

通过无线方式而不是使用电缆或其他本地连接方式将升级包传输到车辆的软件升级。

注 1：“在线升级”也称“远程升级”。

注 2：“本地连接方式”一般指通过车载诊断（OBD）接口、通用串行总线（USB）接口等进行的物理连接方式。

[来源：GB 44496-2024《汽车软件升级通用技术要求》]

真实性

Authenticity

（1）确保主体或资源的身份正是所声称的特性。[来源：GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》]

（2）实体符合其所声称的特性。[来源:《医疗器械网络安全注册审查指导原则（2022年修订版）》，2022]

证券期货业网络安全事件

Securities and Futures Industry Cybersecurity Incident*

是指由于人为原因、 软硬件缺陷或故障、自然灾害等，对证券期货业网络和信息 系统或者数据造成影响，发生网络和信息系统服务能力异常 或者数据损毁、泄露，对国家金融安全、社会秩序、投资者 合法权益造成损害的事件。

[来源：《证券期货业网络安全事件报告与调查处理办法》，2021]

政务数据

Government Data

各级政务部门及其技术支撑单位在履行职责过程中依法采集、生成、存储、管理的各类数据资源。

[来源： GB/T 38664.1—2020《信息技术 大数据 政务数据开放共享 第 1 部分:总则》]

支付敏感信息

Payment Sensitive Information

支付信息中涉及支付主体隐私和身份识别的重要信息。注：支付敏感信息包括但不限于银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等用于支付鉴权的个人金融信息。

[来源：JR/T 0171—2020《个人金融信息保护技术规范》]

知情同意原则

Principle of Informed Consent*

基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。

[来源：《个人信息保护法》，2021]

DLaw Hub 知识库拓展资料： 一卡识数 · 知情同意原则

直接标识符

Direct Identifier

微数据中的属性，在特定环境下可以单独识别个人信息主体。注 1：特定环境：指个人被使用的具体场景，例如，在一个具体的学校，通过学号可以直接识别一个具体的学生。

[来源：GB/T 37964—2019《信息安全技术 个人信息去标识化指南》]

直接标识符的是指在特定环境下可以单独识别个人信息主体的字段。因此理论上，直接标识符能够帮助处理者快速判断处理的数据集是否构成个人信息。

GB/T 37964—2019《信息安全技术 个人信息去标识化指南》和 GB/T 42460—2023《信息安全技术 个人信息去标识化效果评估指南》都提供了常见的直接标识符的示例，包括但不限于：姓名、公民身份证号、护照号、驾驶证号、详细地址、电子邮件地址、电话号码（包括手机号码和固定电话号码）、传真号码、银行账号、车辆标识符和序列号（包括车牌号）、社会保障号码、健康卡号码、病历号码、设备标识符和序列号、生物识别码（包括指纹和声纹等识别码）、全脸图片图像和其他任何可比对的图像、账号、证书或许可证号、互联网协议（IP）地址号等。

相比较下，两份标准提供的示例之间存在着一些差异。这似乎能体现出监管侧的理解的变化。主要的差异如下：

调整	“地址”调整为“详细地址”
	“车辆识别号码”调整为“车辆标识符和序列号（包括车牌号）”
	“设备标识符”调整为“设备标识符和序列号”；
	“生物识别码”调整为“生物识别码(包括指纹和声纹等识别码)”
增加	增加了“全脸图片图像和其他任何可比对的图像”
	增加了“账号、证书号或许可证号”
删除	删除了“网络通用资源定位符（URL）”

关联词：去标识化；标识符；准标识符

智能网联汽车

Intelligent Connected Vehicles*

是具备环境感知、智能决策和自动控制，或与外界信息交互，乃至协同控制功能的汽车。

[来源：《国家车联网产业标准体系建设指南（智能网联汽车）》，2023]

重要数据

Important Data / Key Data

（1）特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。[来源：GB/T 43697-2024《数据安全技术 数据分类分级规则》]

（2）注 1： 重要数据不包括国家秘密；注 2： 重要数据一般不包括个人信息和企业内部管理信息，但达到一定规模的个人信息或者基于海量个人信息加工形成的衍生数据，如其一旦遭到篡改、破坏、泄露或者非法获取、非法利用可能危害国家安全、公共利益，也应满足重要数据保护要求。[来源：《网络安全标准实践指南——网络数据分类分级指引》，2021]

自《数据安全法》起，中国明确规定了数据分类分级保护制度，但在实践层面却长期缺少关于数据分类分级的通用规则。而在 2024 年 3 月 15 日，国家标准化管理委员会批准发布了国家标准 GB/T 43697-2024《数据安全技术 数据分类分级规则》，为数据分类分级管理工作的落地执行提供重要指导。该规则规定了数据分类分级的原则、框架、方法和流程，给出了重要数据识别指南，不仅适用于行业与地区主管部门制定本行业本领域的数据分类分级标准规范，也为数据处理者开展数据分类分级工作提供了参考。

根据《数据安全法》第 21 条，由国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，各地区、各部门按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

在相关标准、指南的指引下，金融、工业与电信、汽车等各行业主管部门以及各地方主管部门已经陆续出台了关于数据分类分级的法律文件，制定着重要数据具体目录。

DLaw Hub 知识库拓展资料： 重要数据和数据分类分级

重要信息系统

Critical Information Systems*

（1）是指承载证券期货业关键业务活动， 如出现系统服务异常、数据泄露等情形，将对证券期货市场和投 资者产生重大影响的信息系统。[来源：《证券期货业网络和

信息安全管理办法》，2023]

（2）是指支持证券基金经营机构和证券基金专项业务服务机构关键业务功能、如出现异常将对证券期货市场和投资者产生重大影响的信息系统。包括集中交易系统、投资交易系统、金融产品销售系统、估值核算系统、投资监督系统、份额登记系统、第三方存管系统、融资融券业务系统、网上交易系统、电话委托系统、移动终端交易系统、法人清算系统、具备开户交易或者客户资料修改功能的门户网站、承载投资咨询业务的系统、存放承销保荐业务工作底稿相关数据的系统、专业即时通信软件以及与上述信息系统具备类似功能的信息系统。[来源：《证券基金经营机构信息技术管理办法》，2023]

重要网络设施和信息系统

Key Network Infrastructure and Information System

一旦遭到破坏、丧失功能或者数据泄露，可能危害国家安全、国计民生、公共利益的网络设施、信息系统等，包括:

a）省级及以上骨干公共电信网和互联网；

b）卫星通信网；

c）二级及以上域名解析系统

d）最大数据存储量在 500PB 以上或服务器机架数 10000 台以上的数据中心（含互联网数据中心、云平台、大数据平台）；

e）上年底市值(估值)在 100 亿元以上或上年度活跃用户规模达到 1 亿以上的电信数据处理者建设运营的通信网络定级达到三级及以上的网络设施和信息系统；

f）电信领域关键信息基础设施；

g）主管部门认定的其他重要网络设施和信息系统。

[来源：YD/T 3867-2024《电信领域重要数据识别指南》]

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。

[来源：GB/T 35273—2020《信息安全技术　个人信息安全规范》]

又名“转移”

关联词：提供；共享

准标识符

Quasi-Identifier

（1）微数据中的属性，结合其他属性可唯一识别个人信息主体。注：常见的准标识符：性别、出生日期或年龄、事件日期（例如入院、手术、出院、访问人地点）、地点（例如邮政编码、建筑物名称、地区）、民族血统、出生国、语言、公民身份、可见的少数民族地位、职业、婚姻状况、受教育水平、上学年限、犯罪历史、总收入和宗教信仰等。[来源：GB/T 37964—2019《信息安全技术 个人信息去标识化指南》]

（2）任何在相应环境下无法单独唯一识别个人信息主体，但结合其他信息可唯一识别个人信息主体的属性属于准标识符。常见的准标识符包括但不限于：性别；出生日期或年龄；事件日期（例如入院、手术、出院、访问相关日期）；地理范围（例如邮政编码、建筑名称、地区）；族裔血统；国籍、籍贯；语言；原住民身份；可见的少数民族地位；职务、工作单位、部门等职业信息；婚姻状况；受教育水平；上学年限；总收入；宗教信仰。[来源：GB/T 42460—2023《信息安全技术 个人信息去标识化效果评估指南》]

准标识符的识别方法具体可参见 GB/T 42460—2023《信息安全技术 个人信息去标识化效果评估指南》的附录 C。

关联词：标识符；直接标识符

自动化决策

Automated Derision-making

（1）通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。[来源：《个人信息保护法》，2021]

（2）我国现行法律法规对自动化决策的界定中强调“对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等”的“分析、评估”应是通过计算机程序自动完成，意在突出个人信息处理者为了实现特定的目的而事先自行开发并部署(或使用第三方开发的)特定的计算机程序。例如为了完成精准广告投放，个人信息处理者有意识地通过在网站或 App 页面上“埋点”收集个人的点击或浏览等行为信息，并通过预设的特征模型计算出特定个人的特征信息。除了特征生成由计算机程序完成之外，决策也可以由计算机程序辅助人工完成，或完全由计算机程序根据特征生成形成的个人特征信息而作出。[来源：《信息安全技术 基于个人信息的自动化决策安全要求》（征求意见稿），2023]

其与其他相近概念的比较可参见个性化推荐

关联词：个性化展示；个性化推送；定向推送；算法推荐；用户画像

DLaw Hub 知识库拓展资料：个性化推荐；第二十四条 自动化决策

自然资源领域数据

Natural Resources Data*

是指在开展自然资源活动中收集和产生的数据，主要包括基础地理信息、遥感影像等地理信息数据，土地、矿产、森林、草原、水、湿地、海域海岛等自然资源调查监测数据，总体规划、详细规划、专项规划等国土空间规划数据，用途管制、资产管理、耕地保护、生态修复、开发利用、不动产登记等自然资源管理数据。

[来源：《自然资源领域数据安全管理办法》，2024]

自然资源领域数据处理者

Natural Resources Data Processor*

是指开展自然资源领域数据处理活动的自然资源行业各类单位。

[来源：《自然资源领域数据安全管理办法》，2024]

组织数据

Organization Data

（1）组织在自身的业务生产、经营管理和信息系统运维过程中收集和产生的数据。[来源：《网络安全标准实践指南——网络数据分类分级指引》，2021]

（2）在某个行业领域依法履行工作职责或业务运营活动中收集和产生的数据。[来源：《信息安全技术 网络数据分类分级要求（征求意见稿）》，2022]

（3）组织在自身生产经营活动中收集、产生的不涉及个人信息和公共利益的数据。[来源：GB/T 43697-2024《数据安全技术 数据分类分级规则》]

座舱数据

Cabin Data

通过摄像头、红外传感器、指纹传感器、麦克风等传感器从汽车座舱采集的数据，以及对其进行加工后产生的数据。

注 1：座舱数据可能包含驾驶员和乘员的人脸、声纹、指纹、心律等敏感个人信息。

注 2：座舱数据不包括对汽车采集数据处理产生的操控记录数据。

[来源：《汽车采集数据处理安全指南》，2021]

对于座舱数据，目前国家标准如 GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》要求除实现语音识别、远程查看车内情况、云存储功能以及依据相关规定向监管或执法机构传输数据的情形外，汽车不应向车外提供座舱数据。

-= 数据合规黑话字典 =-

数据合规人间对话总喜欢说黑话，比如：

（1）尽管 35273 已经相关要求了，但还是 42574 的颗粒度更细一些；

（2）26 号文是 23 年 APP 监管的重点，对 524 行动进一步细化。

上述语句对于一个数据合规小白而言并不是那么友好。

而说出这些缩写的朋友也可能是用久了习惯使然。

一定要把“26 号文”的全称“《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》”说出来，效率也很低。

“数据何规”公众号在 2024 年年初的时候发起《数据合规黑话字典》在线文档共建的活动，旨在消除信息壁垒，让初识数据合规的朋友能够快速上手，了解常用概念或者作为手册备查。

鸣谢以下朋友提供语料与思路：叮咚、洪松、得无度、狐狸、江沢湖海、林中天、三文鱼、玄机、月岛文、bok、Lewis、Tang、Layla、Bingo、Huxian、Annaxy、Leah、程一寒、刘宇、贾大圣、黄春林、showtime、Dyan、史宇航、阿慧、六阳真人、Rinzel

《数据合规黑话字典》在线文档可见：

https://docs.qq.com/sheet/DSEJNYXBFV1ptaWdR

一、机构

（一）国内

1、CAC，又称 **WXB**，全称 Cybersecurity Administration of China，即**国家网信办**，是数据合规监管领域的最主要监管。

2、MIIT，全称 Ministry of Industry and Information Technology，即**工信部**，与工业、信息化、互联网相关的数据合规也都管。**各地派出机构为通信管理局。**

3、SAMR，全称 State Administration for Market Regulation，即**国家市场监督管理局**，平台经济、反不正当竞争、反垄断、各种标准、消费者保护都关注。

4、TC260，又称**信安标委**，全称全国信息安全标准化技术委员会，是从事信息安全标准化工作的技术工作组织。**信息安全领域重要的国标都是他们发的。**

5、CCRC，全称 China Cybersecurity Review, Certification and Market Regulation Big Data Center，即中国网络安全审查认证和市场监管大数据中心，原“**中国网络安全审查技术与认证中心**”，是国家市场监督管理总局直属正司局级事业单位，承担网络安全审查技术与方法研究、网络安全审查技术支撑工作，开展与网络安全相关认证和培训、检验检测等工作。**支撑网络安全审查。**

6、CERT，又称 **CNCERT/CC**，全称 National Computer Network Emergency Response Technical Team/Coordination Center of China，即国家计算机网络应急

技术处理协调中心，为非政府、非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。

7、CAICT，又称**信通院**，即中国信息通信研究院，为工业和信息化部直属科研事业单位，在行业发展的重大战略、规划、政策、标准和测试认证等方面发挥了有力支撑作用。**云大所、泰尔实验室、安全所都是他们的。**

8、TAF，全称为 Telecommunication Terminal Industry Forum Association，即电信终端产业协会，是信通院联同国内电信运营商、电信终端设备制造商、系统设备制造商、认证检测机构和研究机构共同发起的自愿性、非营利的国家级社会组织。**发布了很多电信行业标准。**

9、CCSA，全称为 China Communications Standards Association，即中国通信标准化协会，是由信息产业部电信研究、中国电信、中国移动、中国联通、烽火通信、华为、中兴等单位联合发起，组织国内 100 余家企事业单位成立的新通信标准化工作平台。**发布了很多 YDT 标准。**

（二）国外

1、EDPB，全称 European Data Protection Board，即**欧盟数据保护委员会**，发布了很多解释 GDPR 的指南。

2、CJEU，全称 Court of Justice of the European Union，即**欧盟法院**，很多解释

GDPR 的著名案例都是他们判的。

3、IAPP，全称 International Association of Pricacy Professionals，即**国际隐私专业协会**，知名的 **CIPP**/E/A/US（欧洲/亚洲/美国），CIPM（管理），CIPT（技术）认证都是他们旗下的产品，CIPP/CIPM/CIPT 三者集齐两个即可召唤 **FIP**。注：CIP=Certified Information Pricacy，FIP=Fellow of Information Privacy。

4、NIST，全称 National Institute of Standards and Technology，即美国国家标准与技术研究院，美国很多数据合规相关的**标准、指南**都是他们发的。

5、ISO，全称 International Organization for Standardization，即国际标准化组织，很多烧钱的**数据合规认证**都要找他们，也不限于数据合规。

6、FTC，Federal Trade Commission，美国联邦贸易委员会，负责执行美国的隐私保护法律，如《儿童在线隐私保护法案》（**COPPA**）等。

7、CNIL，Commission Nationale de l'Informatique et des Libert é s，法国国家信息与自由委员会，负责监督法国的数据保护法律。**他们罚款不少。**

8、ICO，Information Commissioner's Office，英国信息专员办公室，负责监管英国的数据保护法规，包括 GDPR 在内的相关规定。**他们指南很多。**

9、**DPC**，Data Protection Commission，爱尔兰数据保护委员会，负责监管爱尔兰的数据保护法规，并在欧盟范围内发挥重要作用。**爱尔兰作为避税天堂，很多国际企业的总部都在这里，巨额罚款也超多。**

二、法规

（一）国内

1、法律

（1）**PIPL**，又称《个保法》，全称 Personal Information Protection Law，即《个人信息保护法》。

（2）DSL，又称《数安法》，全称 Data Security Law，即《数据安全法》。

（3）CSL，又称《网安法》，全称 Cyber Security Law，即《网络安全法》。

2、APP 监管那些带数字的文

（1）337 号文，全称《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知》（工信部信管函〔2019〕337 号）。

（2）191 号文，全称《App 违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191 号）。

（3）164 号文，全称《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）。

（4）14 号文，全称《常见类型移动互联网应用程序必要个人信息范围规定》（国信办秘字〔2021〕14 号）。

（5）165 号文，全称《关于开展互联网行业市场秩序专项整治行动的通知》（工

信部信管函〔2021〕165 号文）。

（6）292 号文，又称 524 行动，全称《工业和信息化部关于开展信息通信服务感知提升行动的通知》（工信部信管函〔2021〕292 号）。

（7）26 号文，全称《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》（工信部信管函〔2023〕26 号）。

3、一串数字的标准

（1）35273，全称《信息安全技术 个人信息安全规范》（GB/T 35273—2020），**个保法出台前的小个保法。**

（2）39335，全称《信息安全技术 个人信息安全影响评估指南》（GB/T 39335—2020 ），**PIA 必参考的国标。**

（3）41391，全称《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》（GB/T 41391-2022），**APP 合规新要求，完全落实成本很高。**

（4）42574，全称《信息安全技术 个人信息处理中告知和同意的实施指南》GB/T 42574—2023）。**落实个保法“告知-同意”义务的最佳落地参考。**

（5）**0171**，全称《个人金融信息保护技术规范》（JR/T 0171—2020），**人行出台的金融标准适用于所有金融机构，C1/C2/C3 的分类影响颇深。**《金融数据安全 数据安全分级指南》（JR/T 0197—2020）及《金融数据安全 数据生命周期安全规范》（JR/T 0223—2021）亦有重大参考价值，主要适用于银行保险机构，证监会有另一套数据分类分级规则。

（二）国外

1、欧盟

（1）**GDPR**，General Data Protection Regulation，《通用数据保护条例》。

（2）**DPD**，Data Protection Directive，《数据保护指令》。

（3）**DMA**，Digital Markets Act，《数字市场法案》。

（4）**DSA**，Digital Services Act，《数字服务法案》。

（5）**DGA**，Data Governance Act，《数据治理法案》。

（6）**Data Act**，《数据法案》。

2、美国

（1）**COPPA**，Children's Online Privacy Protection Act，《儿童在线隐私保护法案》。

（2）**CCPA**，California Consumer Privacy Act，《加利福尼亚消费者隐私法案》。

（3）**HIPAA**，Health Insurance Portability and Accountability Act，《健康保险携带和责任法案》。

（4）**GLBA**，Gramm-Leach-Bliley Act，《格雷厄姆-利奇-布莱利法案》。

（5）**FCRA**，Fair Credit Reporting Act，《公平信用报告法案》。

3、认证

（1）**27001**，ISO/IEC 27001，《信息安全管理体系》（Information Security Management System）。

（2）**27002**，ISO/IEC 27002，《信息安全控制实践指南》（Information Security Control Practice Guide）。

（3）27701，ISO/IEC 27701，《隐私信息管理体系》（Privacy Information Management System）。这是一项国际标准，专注于隐私信息的管理，补充并扩展了 ISO/IEC 27001 和 ISO/IEC 27002 标准，为组织提供了处理个人信息的指导。

（4）27005，ISO/IEC 27005，《信息安全风险管理》（Information Security Risk Management）。

（5）20000，ISO/IEC 20000，《信息技术服务管理》（Information Technology Service Management）。

（6）22301，ISO/IEC 22301，《业务连续性管理系统》（Business Continuity Management System）。

（7）38500，ISO/IEC 38500，《信息技术治理》（Information Technology Governance）。

参考资料

- 合规社，《105 个数据安全必备词汇》
- GB/ T 41867- 2022《信息技术 人工智能 术语》
- GB/T 25069-2022《信息安全技术 术语》
- 《数据领域常用名词解释（第一批）》