海问律师事务所

Haiwen & Partners

2020 企业开展数据合规实务指南

2020.10 杨建媛

HAI WEN 海问律师事务所

L-Council简介

L-Council为理购与协同共享企业服务（上海）股份有限公司旗下服务品牌。秉承“专业分享、价值创造”的企业使命，致力于成为国内优质的汇聚知名跨国企业及本土大型企业法务人员的会员制服务机构。**L-Council**以专业人群为依托，结合特定行业，精准聚焦法务经理人，旨在提供最佳实战经验分享及法律信息服务。在中国已有超过1000家会员企业，30，000多位企业法务同行使用和体验**L-Council**的超值分享服务。

CHINA LEGAL
Executive Council

L-Council 电话：021-62705678-1086
邮箱：cs1@lcouncil.com

杨建媛

北京海问律师事务所 合伙人

杨建媛律师是北京海问律师事务所的合伙人，擅长处理复杂合规问题，包括中国境内业务及跨法域事务，特别是在数据合规领域。杨律师作为法律专家积极参与合规领域的立法研究与讨论，包括《网络安全法》落地相关的国家标准。同时，杨律师与企业资深法律专家共同研究个人信息保护前沿问题，为行业合规发展提供可行性建议。协助多家国内外知名企业（涵盖金融、AI及大数据、医疗健康、制造业等行业）开展数据核查、差距分析、搭建数据合规体系，并提供各类数据合规服务，其中涉及内部数据安全管理、第三方数据合作、跨境数据传输、重要数据识别、数据本地化等系列复杂法律问题。杨律师同时具有多年跨境争议解决的经验，是为数不多的可以为客户提供全方位合规服务的律师。

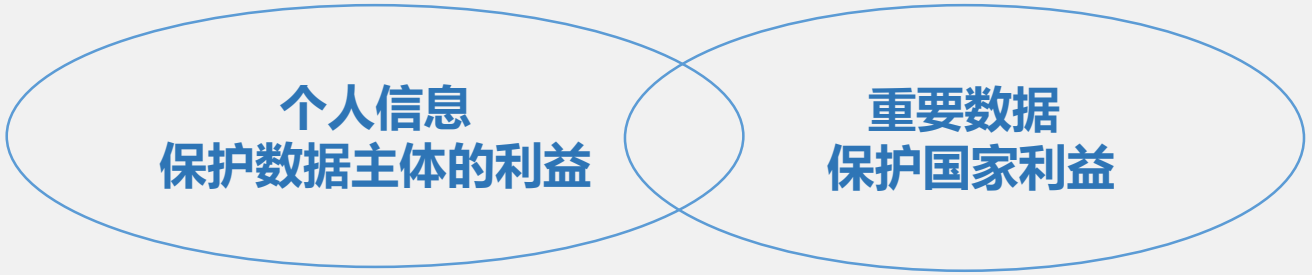
一、《个人信息保护法（草案）》最新亮点

中国数据安全治理结构

第四级

数据伦理

第三级



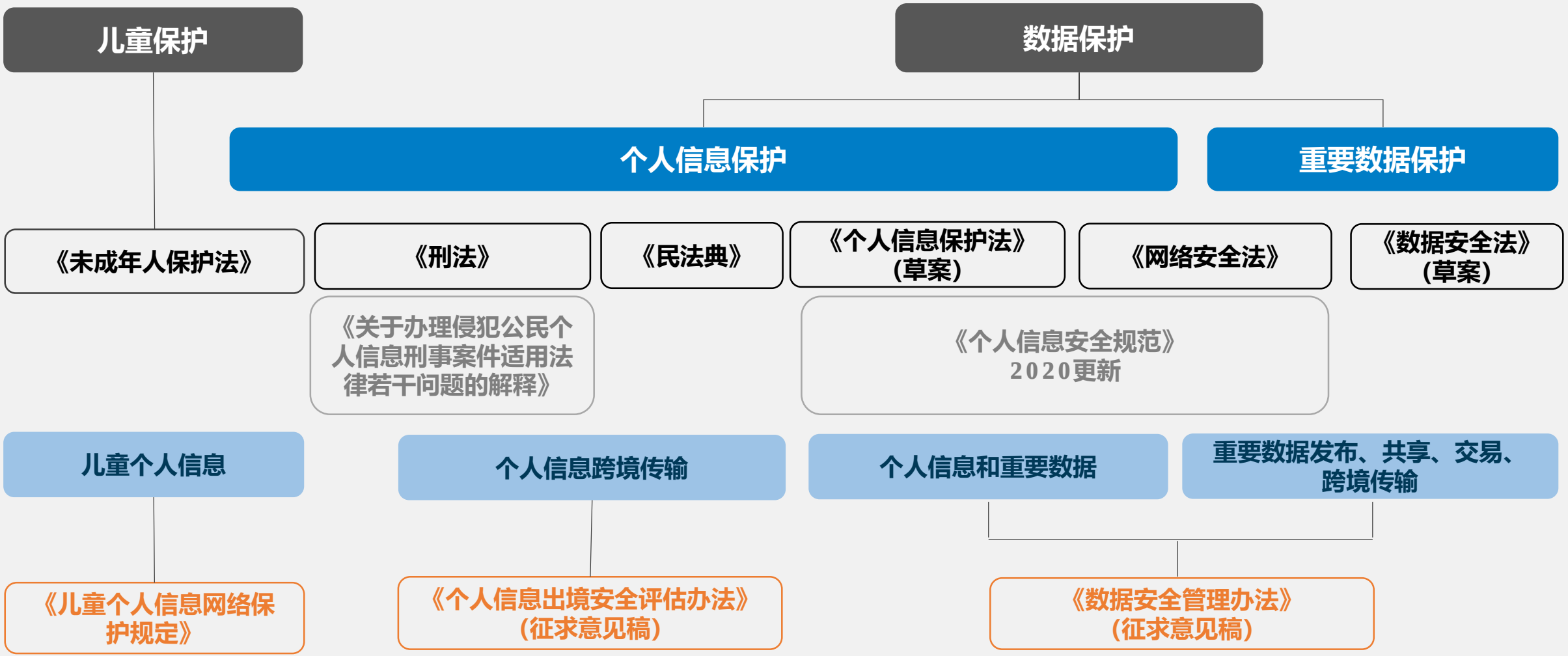
第二级

管理措施

第一级

技术措施

中国数据保护法律框架


儿童保护
数据保护
个人信息保护
重要数据保护
《未成年人保护法》
《刑法》
《民法典》
《个人信息保护法》(草案)
《网络安全法》
《数据安全法》(草案)
《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》
《个人信息安全规范》2020更新
儿童个人信息
个人信息跨境传输
个人信息和重要数据
重要数据发布、共享、交易、跨境传输
《儿童个人信息网络保护规定》
《个人信息出境安全评估办法》(征求意见稿)
《数据安全管理办法》(征求意见稿)

个保法草案的总体架构

两个规则	个人信息处理规则	个人信息跨境提供规则
权利-义务	个人的权利	个人信息处理者的义务
监管体系	主管机关	法律责任

个保法草案的法律适用范围

概念定义

- **个人信息**：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。
- **个人信息的处理**：包括个人信息的收集、存储、使用、加工、传输、提供、公开等活动。

域外管辖

- **必要的域外适用效力**：发生在我国境外的个人信息处理活动，下列情况适用本法
  （1）以向境内自然人提供产品或者服务为目的；
  （2）为分析、评估境内自然人的行为。
- 适用本法的境外个人信息处理者，应当**在我国境内设立专门机构或指定代表**，负责个人信息保护的相关事务。

“告知-同意”为核心的个人信息处理规则

“告知-同意”的一般规则	• **同意的前提**：处理个人信息应当在**事先充分告知**的前提下取得个人同意 • **撤回同意**：个人有权撤回同意；**不得**以个人不同意为由拒绝提供产品或者服务 • **重新同意**：重要事项发生**变更**的，应当重新取得同意
更严格的同意	• **个人敏感信息的处理**：特定的目的 + 充分的必要性 + 个人的**单独同意或者书面同意** • **跨境传输**：安全评估/认证/合同 + 更严格的**同意**
跨境提供规则	• **关键信息基础设施运营者**、处理个人信息达到国家网信部门规定**数量**的处理者：应当通过国家网信部门组织的**安全评估** • **一般的个人信息处理者**：经专业机构**认证**等途径 • **国际司法协助、行政执法协助**：应当依法申请有关主管部门**批准**

个人的权利与个人信息处理者的义务

个人的权利

- **知情权、决定权**
- **查询权**
- **更正权**
- **删除权**
- **要求个人信息处理者建立个人行使权利的申请受理和处理机制**

个人信息处理者的义务

- **必要措施**：内部管理制度和操作规程、安全技术措施等
- **个人信息保护负责人**
- **定期合规审计**
- **事前风险评估**：个人敏感信息，境外提供等
- **个人信息泄露后的补救与通知**
- **与个人权利相对应的义务**

主管机关与法律责任

主管机关

- **国家网信部门**负责个人信息保护工作的**统筹协调**
- **国务院有关部门**在各自职责范围内负责个人信息保护和监督管理工作

法律责任

- **违反本法规定处理个人信息或未采取必要的安全保护措施的**：责令改正，没收违法所得，给予警告；**拒不改正的**，并处100万元以下罚款；对直接责任人员处1~10万元罚款。
- **违法行为情节严重的**：责令改正，没收违法所得，并处**5000万元**以下或**上一年度营业额5%**以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或营业执照；对直接责任人员处10~100万元罚款。

《未成年人保护法（2020修订）》与未成年人个人信息保护

最新版《未成年人保护法（2020修订）》于2020年10月17日发布、2021年6月1日起施行，新设第五章 “网络保护”专章，并特别规定了对未成年人个人信息的保护。

- **第四条**明确规定了“**保护未成年人隐私权和个人信息**” 的原则。

- **第七十二条**专门规定了**未成年人的个人信息保护。**
  - 信息处理者通过网络处理未成年人个人信息的，应当遵循**合法、正当和必要**的原则。
  - 处理不满十四周岁未成年人个人信息的，应当征得未成年人的**父母或者其他监护人同意**，但法律、行政法规另有规定的除外。
  - 未成年人、父母或者其他监护人要求信息处理者**更正、删除**未成年人个人信息的，信息处理者应当及时采取措施予以更正、删除，但法律、行政法规另有规定的除外。

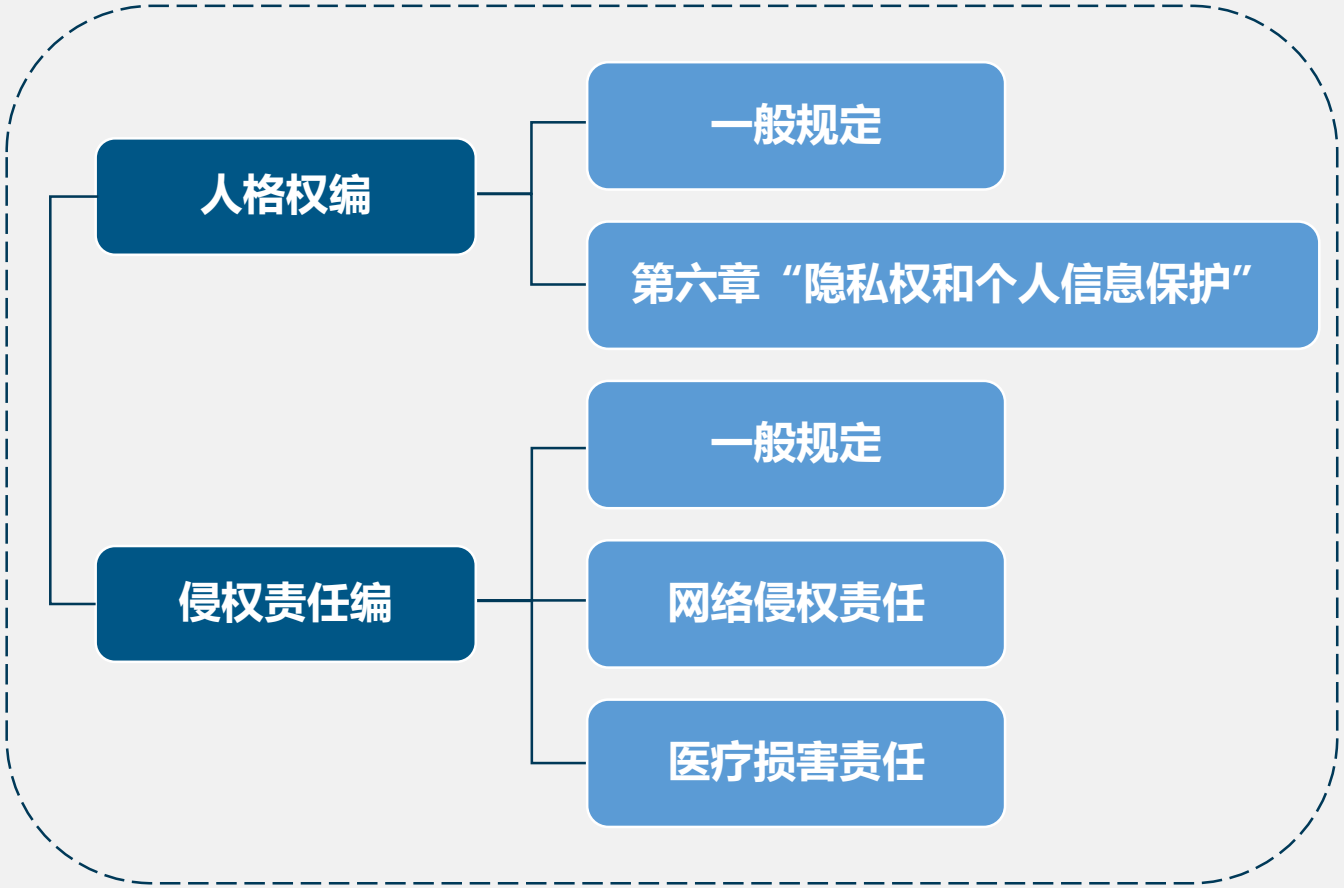
《民法典》

自2021年1月1日起施行的《民法典》，在人格权编中专章规定了隐私权和个人信息保护问题。具体体现在：

- 调整了“个人信息”和“隐私”的定义和范围
- 确立了个人信息处理的基本原则
- 确立了自然人对其个人信息的查阅、复制等权利
- 规定了信息处理者的个人信息保护义务

侵害个人信息的免责事由：合理处理该自然人自行公开或其他已经合法公开的信息，但是该自然人明确拒绝或处理该信息侵害重大利益的除外。

《民法典》隐私权和个人信息相关条款



《数据安全法》（草案）

《数据安全法》（草案）是数据安全领域的基础性法律，于2020年7月3日对外公布征求意见

适用范围	• 适用于所有“数据活动”：收集、存储、加工、使用、提供、交易、公开等 • 有限的域外适用 • 适用于所有数据，不区分数据具体的表达形态。**个人信息、企业经营信息、重要数据、国家秘密。**
主管机构	• **中央国家安全委员会**负责决策和统筹协调 • 工信、交通、金融、卫生等行业主管部门负责本行业、本领域数据安全监管 • 网信部门负责网络数据相关的统筹协调和监督，公安、国安在职责范围内负责数据安全监管
数据安全制度 **（责任主体：国家）**	• **数据分级分类**制度、确定重要数据保护目录 • 数据安全风险评估、报告、共享和监测预警 • 数据安全应急处置 • 数据国家安全审查 • 数据出口管制、贸易反制
数据安全保护义务 **（责任主体：开展数据活动的单位）**	• **全流程数据安全管理制度**：培训、技术措施和其他必要措施、数据安全负责人和管理机构（重要数据处理者） • 风险监测与应急 • 定期风险评估（重要数据处理者） • 数据交易中介服务机构：要求数据提供方说明数据来源，审核双方身份，留存审核和交易记录 • 向境外执法机构提供需事先报告 • 符合伦理
政务数据安全开放 **（责任主体：国家机关）**	• 在履行法定职责范围内收集、使用数据 • 建立数据安全管理制度，落实安全保护责任 • **委托处理或者对外加工政务数据应经过严格批准程序，并监督接收方履行数据安全保护义务** • 制定政务数据开放目录

二、企业开展数据合规实操建议

数据合规制度

职责分配以及文件留存

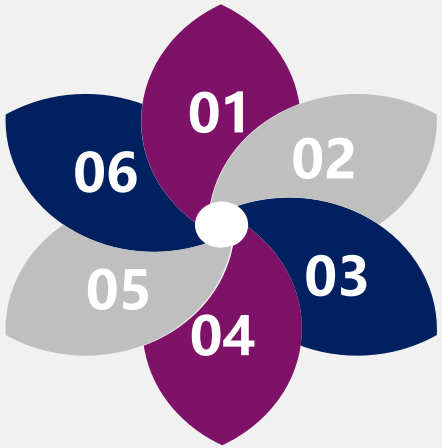
分配企业内部的数据保护工作职责，设立相关部门并明确工作分工。必要时指派个人信息保护合规官，在体系内各项合规活动留存书证。

数据识别与分类

对收集到的信息类型进行识别，明确个人信息中的敏感信息范围。

符合透明性原则

在间接收集数据时，重点核查合作企业是否履行了告知义务。在产品设计时充分考虑应用场景可能对个人产生的影响，为客户进行人工干预提供渠道。



第三方与供应商管理

对所有可能分享个人数据的第三方及可能通过其收集数据的第三方均进行严格管理，构造全生态管控，避免数据控制者因第三方不当行为承担责任。

员工数据保护纪律及员工同意函

员工泄露敏感信息或将使公司面临承担刑事、行政责任或名誉受损的风险，明确员工违反数据合规制度的责任及惩戒措施是实现良好内控的关键环节。

跨境传输机制

在接收境外跨国公司用户的个人信息传输时，应将这些业务板块进行整体的跨境传输机制的论证，并且留存相应的自评估报告等。

信息管理的各环节 – 收集信息

信息收集	常见误区
直接收集： 明确告知个人信息主体公司收集、使用个人信息的规则；获得个人信息主体明确的授权同意；收集的个人信息均是在实现收集目的最小范围内	× 不说明原因，直接发邮件要求员工提供健康宝信息 × 为了工作或业务原因只需要电话号码，但将电话号码、家庭住址一起收集 × 未征得员工同意，直接拿走该员工办公桌上的身份证复印件
间接收集： 要求第三方提供书面文件说明个人信息来源并确认合法性；了解该第三方机构已获得的个人信息处理的授权同意范围，超范围收集需要征得信息主体同意	× 从另一家公司拿到消费者电话，不询问来源和合法性 × 从另一家公司拿到消费者电话，得知了合法性，但未问清个人授权的使用范围，便给消费者拨打电话
未成年人个人信息收集： 对于年满14岁的未成年人个人信息的收集，应征得未成年人或其监护人的明示同意；对于14岁以下未成年人个人信息的收集，除遵循以上要求外，还须进一步保证在收集其个人信息之前已经获得了监护人的明示同意。	× 要求员工填写其10岁孩子的信息用于上保险，但并未向员工告知计划的使用目的

信息管理的基本措施 – 存储信息

信息存储	常见误区
公司在境内运营中收集和产生的个人信息应在境内存储。	× 收集到的个人信息，未经合规核准，直接传给海外办公室
应对保存的个人信息根据收集、使用目的遵照最小化原则设置相应的保存期限，超出这一期限后，应当将个人信息进行删除或匿名化处理。	× 某员工离职后，除了法律规定应保存的信息（例如劳动合同文本）外，未合理删除与该员工相关的其他个人信息或采取其他保护措施
在存储和传输个人信息期间，应当采取一定的安全措施保障个人信息的完整性，防止个人信息泄露、毁损和丢失。	× 用私人邮箱传输员工/消费者个人信息 × 用Excel表格收集个人信息，未作加密处理 × 把身份证复印件等重要信息直接放在桌面上 × 离开时工位不锁电脑屏幕

信息管理的基本措施 – 访问信息

信息访问	常见误区
最小授权：被授权访问个人信息的内部数据操作人员，只能访问职责或工作所需的最少够用的个人信息，且仅具备完成职责、工作所需的最少的数据操作权限。	× 销售部和人事部访问个人信息权限完全相同
按需审批：对个人信息的访问与其他操作（如批量修改、拷贝、下载等）由安全部协助各业务线数据管理员设置内部权限审批、记录流程。	× 无需审批，所有员工信息一键下载 × U盘拷贝个人信息，公司不作记录登记
职责分离：一名员工不能同时承担多个存在职责冲突的角色，以防止获得过大的权限，如对个人信息进行处理、权限配置和操作审计的人员角色应分离设置。	× 一人收集信息，并在处理、 配置此信息时有最终决定权

信息管理的基本措施 – 使用信息

信息使用	常见误区
在使用个人信息时不能超出个人信息主体授权同意的使用目的和范围。如果拟将所收集的个人信息用于已向个人信息主体明示的收集之外的其他目的和用途，应当再次向个人信息主体进行说明，并获得个人信息主体的同意。	× 员工提供新冠肺炎确诊信息，只供筛查接触人使用；人事将该员工确诊所有信息发给所有其他员工
在个人信息使用过程中能够采取一定的技术手段实现个人信息的匿名化。	× 北京办公室 业务部 王平（全名） 查出新冠肺炎阳性 ✓ 北京办公室 某同事 确诊新冠肺炎；并私下通知可能受影响的人

数据泄露引发执法的要点

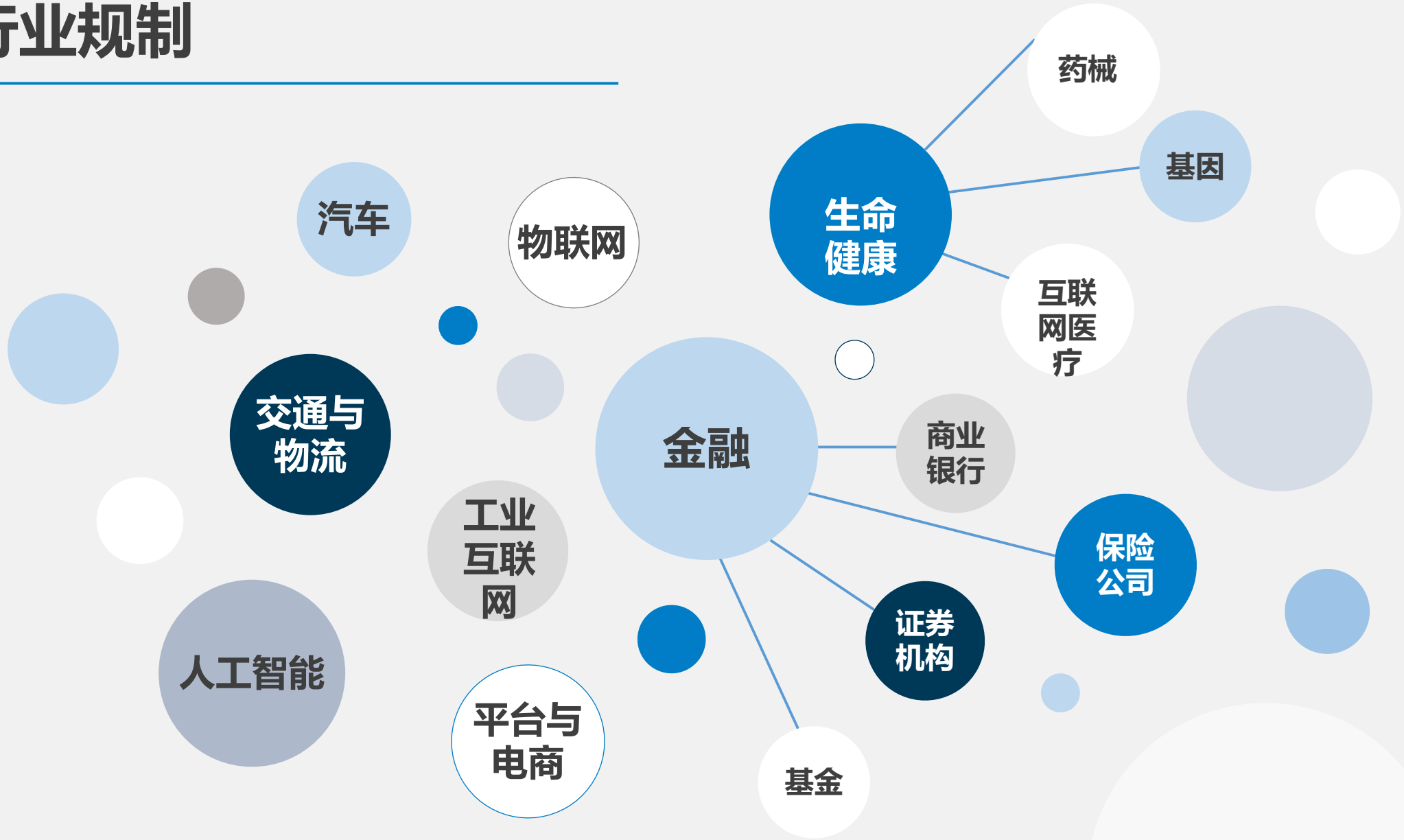
- 何为数据泄露?
- 何为必须汇报给有关主管部门的数据泄露或者网络安全事件?
- 是否存在数据泄露就意味着企业存在过错?
- 是否存在数据泄露就直接推定数据泄露与损害结果之间有必然的因果关系?
- 是否履行了安全保障义务就履行了法定的注意义务?
- “技术措施”以及“其他必要措施”的内涵是否等于各种国家推荐的标准?
- 是否每一种类的个人信息都会导致对数据主体的损害?

如何应对数据安全事件

- **数据合规重在预防有两层含义：（1）合规可有效预防重大监管风险的发生；（2）建立完善的危机管理和应对机制有助于迅速、从容地应对危机，避免损失扩大。**

- ✓ 明确危机应对的部门、人员及责任，密切配合。
- ✓ 全面了解客观真相、法律后果，法律合规是准绳。
- ✓ 诚恳积极地表达态度，正面、不逃避、解决问题。
- ✓ 配合执法、拥抱监管，从哪里跌倒就从哪里爬起。

行业规制


汽车
物联网
生命健康
药械
基因
互联网医疗
交通与物流
金融
商业银行
工业互联网
保险公司
证券机构
人工智能
平台与电商
基金

公司上市过程中的数据合规监管

数据合规性是申报IPO的审核关注重点，近年来在IPO的审核过程中，监管机构对数据合规问题多有关注，要求发行人对数据的获取、使用、管理、安全性等方面进行详细说明和披露。数据合规开展不充分不但影响IPO审核的进程，而且可能导致上市失败。

蚂蚁集团
(申请科创板上市)

- 蚂蚁与阿里集团的**数据共享**是否存在侵害客户合法利益的情况；
- 数据的获取、管理和使用的合法合规性；
- 蚂蚁与阿里集团的数据平台的独立性。

微众信科
(申请科创板上市)

- 三种**数据获取来源**（客户提供、向供应商采购及自行搜集信息）的具体实现方式、授权有效性、**合法合规性及纠纷解决机制**；
- 采取的安全措施和保护制度。

每日互动
(创业板上市成功)

- 作为SDK收集终端用户的获取途径和授权方式，**使用是否超过授权权限**；
- 终端用户数据的权属问题；
- 新的技术手段是否额外采集了用户的个人信息。

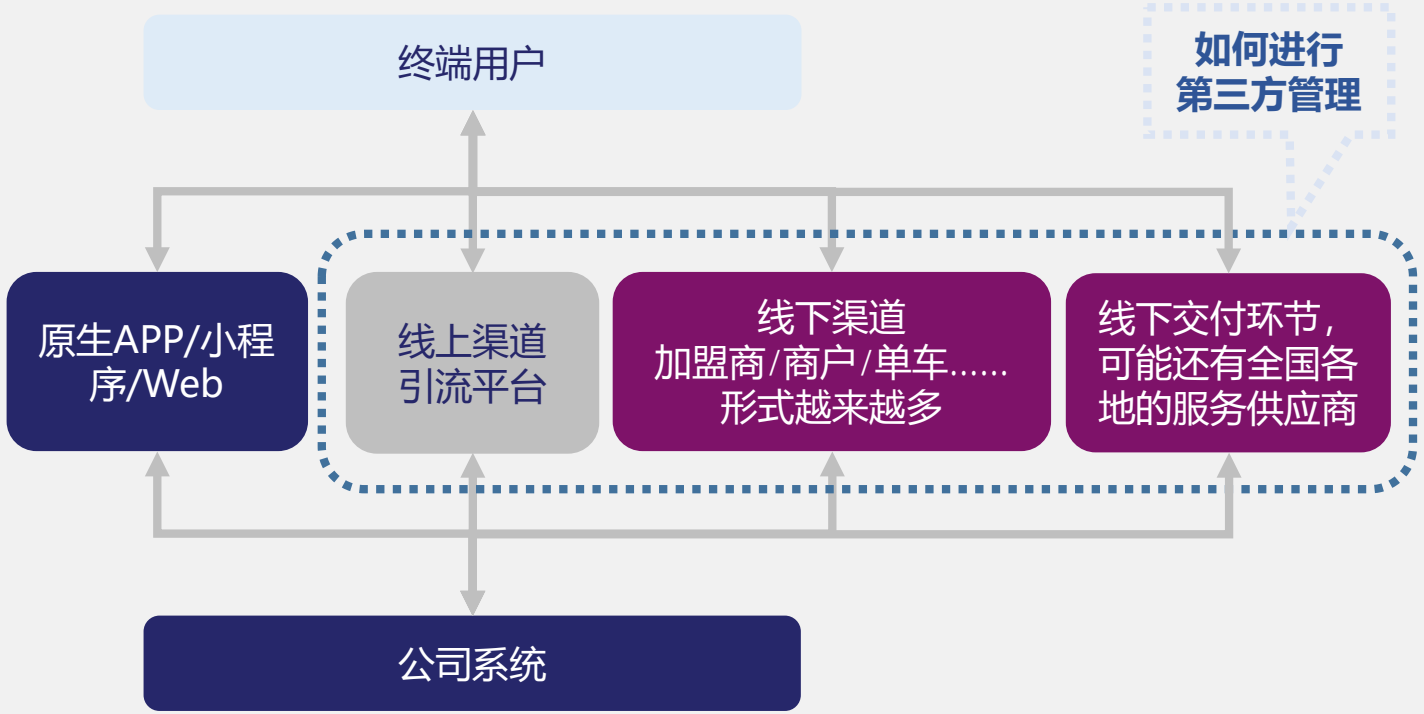
墨迹天气
(上市失败)

发审委会议提出的主要问题：

- 存在未经其许可违规发布互联网新闻信息，要求说明整改的情形；
- 存在收集使用个人信息过程中**侵害用户隐私**的问题，要求说明整改情形。

第三方数据合规管理

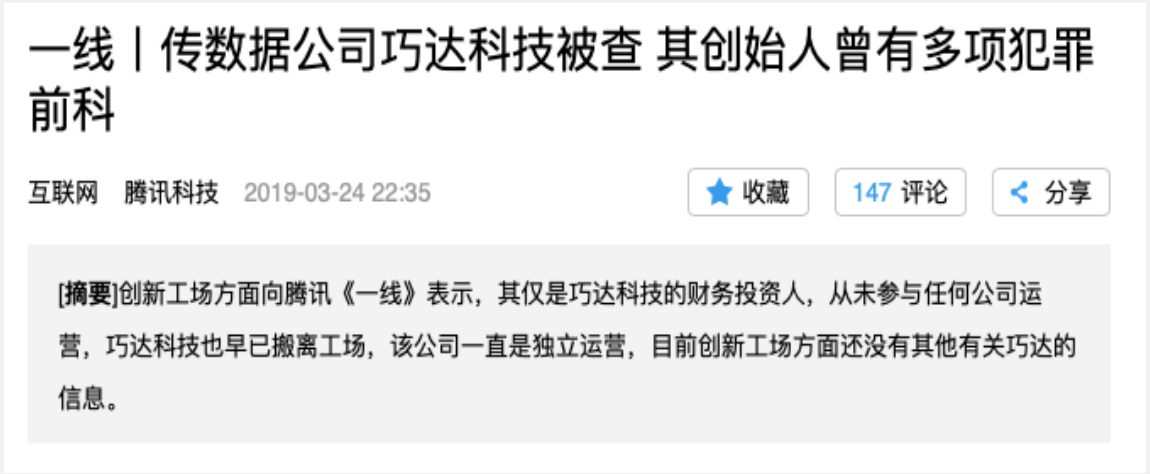
我们在此前的众多项目中发现，很多公司正在逐步完善自身的系统安全，但权限管理仍然较为混乱，对第三方的安全管控亦存在不足，数据泄露的风险较高，个别合作伙伴已经出现了严重的数据泄露事件。



建议采取的措施	
合同	在合作协议中部署数据安全条款
政策	制定并发布约束第三方账号与权限管理的政策，对第三方各地区、各网点系统管理员的选择、角色划分、及各类角色的赋权等给与指导
流程	对涉及个人信息的重要操作设置内部审批流程，包括批量修改、拷贝、下载等，审批权限尽量集中化
技术措施	尽量采取技术授权确保上述组织措施的实现，例如增加验证、设置异常操作限制或报警等
监督巡查	采取监督或巡查手段，及时发现第三方及其人员的违规现象
问责	制定并执行第三方数据安全问责制度，对故意违反目标安全策略和规定的人员及该第三方进行惩戒

数据合规尽职调查

- **巧达案**：2019年3月，巧达科技（北京）有限公司因非法爬取、兜售用户数据被查封， 公司法人王某某等36人被检察机关依法批准逮捕。巧达科技成立于2014年7月，号称拥有中国最大的简历数据库，获创新工场等数千万投资。



一线丨传数据公司巧达科技被查 其创始人曾有多项犯罪前科

互联网　腾讯科技　2019-03-24 22:35　收藏　147 评论　分享

[摘要]创新工场方面向腾讯《一线》表示，其仅是巧达科技的财务投资人，从未参与任何公司运营，巧达科技也早已搬离工场，该公司一直是独立运营，目前创新工场方面还没有其他有关巧达的信息。

BOSS直聘　首页　职位　公司　APP　资讯　上传简历

巧达科技

B轮 · 20-99人 · 互联网

公司简介　招聘职位(0)

巧达科技简介

巧达数据是中国最大的用户画像关键数据服务提供商，专注于大数据及人工智能领域前瞻性产品研发，客户覆盖互联网行业及泛金融领域。巧达核心团队由中国互联网元老级产品专家和技术极客组成，成立以来已经获得数千万美元风险投资，股东包括中信产业基金、嘉悦金实、百度风投管理合伙人齐玉杰、创新工场等著名投资者。

工商信息

巧达科技（北京）有限公司　来源：企查查

数据合规尽职调查

- 投资模式：是否与目标公司发生数据对接?
- 行业风险：目标公司是否为数据密集型产业，如互金公司?
- 公开检索：目标公司是否有数据安全或隐私保护的重大负面报道?
- 其他风险因素：数据跨境与境外司法管辖、第三方共享及程度……
- 风险缓解因素：目标公司获得数据安全与隐私保护的相关认证……

数据合规尽职调查

基金投资中的数据合规尽职调查（DCDD）

五、帮助投资人及时采取补救措施

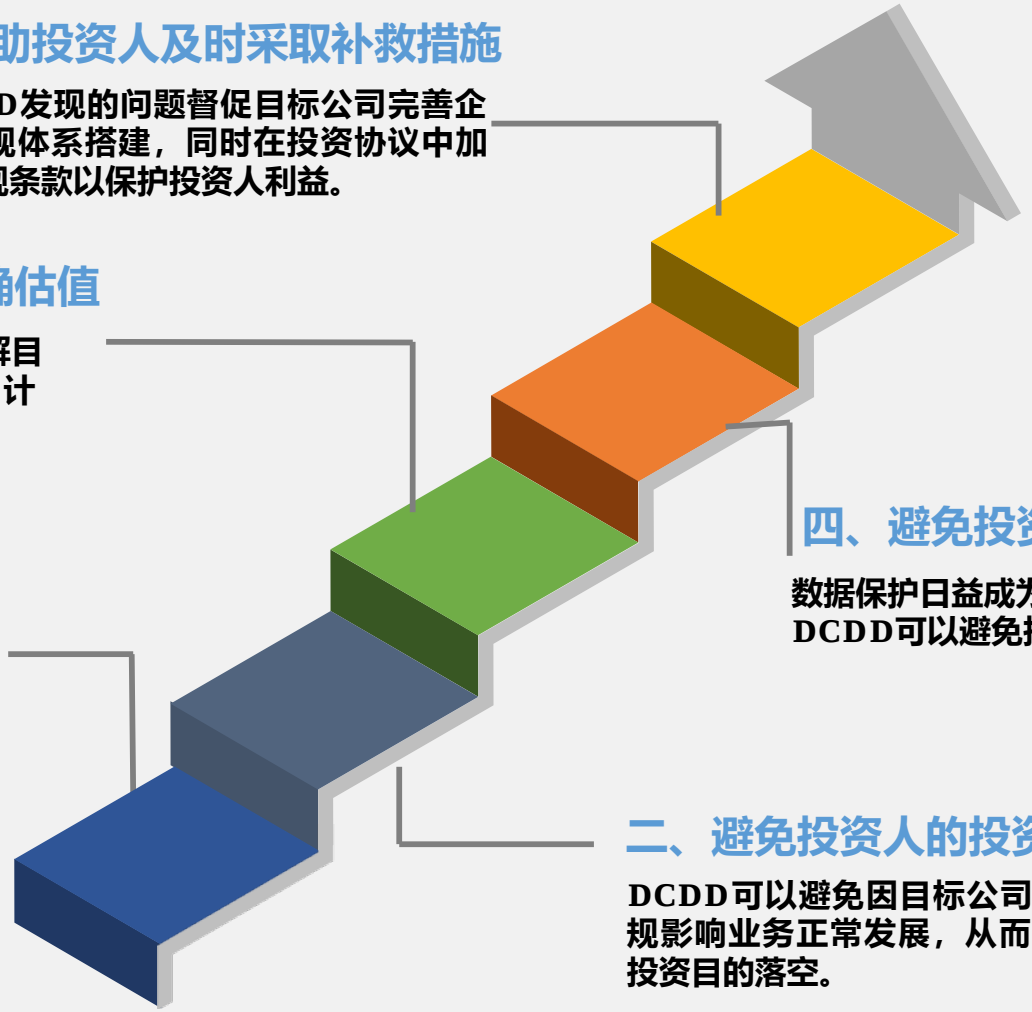
基于DCDD发现的问题督促目标公司完善企业内部合规体系搭建，同时在投资协议中加入数据合规条款以保护投资人利益。

三、帮助投资人对目标公司准确估值

在交易中，投资人可以通过DCDD了解目标公司的数据合规情况，进而作为项目计划、交易条件及价格的重要参考。

一、降低投资人被执法风险

非法提供、获取个人信息为公安机关重点打击的对象。侵犯个人信息罪为行为犯，不需要产生损害后果即可构罪，现实中存在将获取的个人信息用于合法经营仍被刑事调查的案例。



四、避免投资人的声誉风险

数据保护日益成为企业的核心竞争力之一，DCDD可以避免投资人遭受重大声誉损失。

二、避免投资人的投资目的落空

DCDD可以避免因目标公司商业模式不合规影响业务正常发展，从而导致投资人的投资目的落空。

谢谢聆听！
如有任何问题，欢迎讨论。

yangjianyuan@haiwen-law.com

HAI WEN

海问律师事务所

行海之容 知问之道

谢谢聆听！
如有任何问题，欢迎讨论。

yangjianyuan@haiwen-law.com