

2021年网络安全与数据合规 新规评论文章集锦

环球律师事务所数据合规团队编制



2022年1月24日

www.glo.com.cn

中国首家律师事务所
The First Chinese Law Firm

目录

1. 《数据安全法》正式出台，企业合规红线，你了解吗？	2
2. 《关键信息基础设施安全保护条例》要点解读	24
3. “隐私”与“个人信息”别傻傻分不清	38
4. 个人信息保护工作机构及负责人设置要求	45
5. 《个人信息保护法》八步走，落地路径与实务解读	58
6. 《重要数据识别指南》新版草案出台，兼议十二项企业合规义务	76
7. 征信信息已成为保护重点——暨同步解读《征信业务管理办法》	87
8. 互联网信息服务管理办法大修，信息安全监管释放趋严信号	100
9. 《网络交易监督管理办法》压实平台主体责任，企业未来该如何应对？	104
10. 境外上市中的网络安全审查	109
11. 面对网络安全审查，中概股企业需做何准备？	122
12. 企业数据出境评估指引暨《数据出境安全评估办法（征求意见稿）》解读	134
13. 苹果将实施史上最严厉隐私保护要求，定向广告的严冬真的来了？	147
14. 算法相关新型垄断模式的法律风险	161
15. 从《汽车数据安全管理办法》探索汽车数据的合规与发展	169
附件一：《互联网信息服务管理办法》合规义务清单	179
附件二：《网络交易监督管理办法》合规义务清单	194
附件三：App收集使用个人信息企业自评估核对清单	202



《数据安全法》正式出台， 企业合规红线，你了解吗？

环球律师事务所
孟洁 | 张淑怡 | 徐晨

《中华人民共和国数据安全法》

《中华人民共和国数据安全法》

【前言】

随着信息技术和生产生活紧密融合，各行各业的数据迅猛增长，并汇聚融合，对经济、社会和人民生活都产生了革命性的影响。数据安全已成为事关国家安全与社会经济发展的重要课题。基于此，2021年6月10日，第十三届全国人大常委会第二十九次会议审议并通过了《中华人民共和国数据安全法》（以下简称“《数据安全法》”），并于2021年9月1日起施行。

《数据安全法》共七章五十五条，与《中华人民共和国网络安全法》（以下简称“《网络安全法》”）、《数据安全管理办法（征求意见稿）》（以下简称“《数据安全管理办法》”）相比，有较大的创新和突破，从国家法律的层面，对于国家与数据活动实施者两个角色，规定了一系列提升数据安全治理和数据开发利用水平的原则、制度与措施，落实主体责任；为适应电子政务发展的需要，建立数据流通利用与安全管理的要求。正如新华社所评述，“制定数据安全法是维护国家安全的必然要求。数据是国家基础性战略资源，没有数据安全就没有国家安全。”

下文将首先介绍《数据安全法》相较于二审稿的修改之处与亮点，其后总结了《数据安全法》的合规要点，以期帮助企业了解立法精神，梳理合规义务，厘清基本红线。

一、《数据安全法》正式稿相较于 二审稿的修改亮点

（一）建立工作协调机制，完善数据安全领域治理体系

《数据安全法》第五、六条明确了数据安全领域内治理体系的顶层设计，即中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究和制定重大方针政策，统筹协调国家数据安全的重大事项和重要工作，**建立国家数据安全工作协调机制**；各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门承担本行业、本领域数据安全监管职责；并且，由公安机关和国家安全机关承担其范围内的监管职责；最后由国家网信部门统筹协调网络数据安全的监督管理工作，这与国家网信部门的一贯职责与功能是配套和衔接的。

从以上表述可以看出，相较于《数据安全管理办法》和《网络安全法》所涉及的监管部门权属划分，《数据安全法》既有保留也有突破。在网络监管方面，《数据安全法》沿袭了“**网信部门+公安部门+国务院其他下属机构联动**”的监管体系，但值得注意的是，《数据安全法》**首次将数据安全全局决策统筹工作升格至中央国家安全领导机构，与《国家安全法》保持一致，从侧面巩固了数据安全在国家安全体系中的重要地位**，以基本法成文化的方式将数据安全工作上升至国家安全最高监管和行动决策的层级。

尽管我国近年来持续加快对数据以及个人信息保护方面的立法进度，比如《民法典》人格权编中对个人信息保护做出了原则性规定，出台了包括《网络安全法》《数据安全管理办法》《信息安全技术 个人信息安全规范》等一系列法律法规、部门规章和国家标准，但仍然存在法律效力有限、规定分散、体系不完备的问题。《数据安全法》此次将数据安全集中、专门地反映在一部基本法中，完善了我国在数据保护领域的立法架构，也为后续配套文件的跟进提供了坚实的基础。

总体来说，国家从战略和规划层面上重视数据的保护与应用，也意味着企业需要更加谨慎地处理数据，不但需从自身角度，还要从维护国家利益层面上履行数据安全保护义务、承担社会责任，不得危害国家安全与社会、公共利益。

（二）明确关系国家安全、国民经济命脉等重要数据的重要性

《数据安全法》第四条规定，维护数据安全，应当坚持**总体国家安全观**。这一概念是以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托的全方位国家安全体系。这条规定呼应了《国家安全法》第二十五条所提出的，国家应建设网络与信息安全保障体系，提升网络与信息安全防护能力，**维护国家网络空间主权、安全和发展利益**。在各国数据博弈深化的国际背景下，主权已经不再局限于一国领土而是拓展至网络空间中的数据和设施，数据要素已经成为国家基础性和战略性资源，数据安全已经成为国家安全不可或缺的组成部分。**应对数据可能带来的非传统领域的国家安全风险与挑战，切实维护和确立国家数据主权、安全和发展利益，正是当今时代赋予的新课题。**

《数据安全法》第二十一条第二款则进一步强调关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

这一点也在罚则部分有所体现，《数据安全法》最终稿新增的第四十五条第二款明确，违反国家核心数据管理制度，危害国家主权、安全和发展利益的，**由有关主管部门处二百万元以上一千万元以下的罚款**，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

（三）进一步完善保障政务数据的规定

为保障政务数据安全，并推动政务数据开放利用，《数据安全法》第五章对国家机关收集、使用、运用数据的行为、能力提出了要求（第三十七条到四十三条）。国家机关为履行法定职责的需要收集、使用数据时，应当对其在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据依法予以保密，不得泄露或者非法向他人提供（第三十八条）。

其次，第四十条对国家机关委托他人存储、加工或者向他人提供政务数据的审批要求和监督义务做出了规定，**并明确受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据**。国家机关还应按照规定及时准确公开政务数据，制定开放目录，构建互联互通、安全可控的开放平台（第四十一、四十二条）。

《数据安全法》虽未对政务数据进行定义，但可以根据今年6月17日浙江省发布的全国首部公共数据开放办法《浙江省公共数据开放与安全管理暂行办法》（下称《公共数据暂行办法》）对“公共数据”的界定汲取经验。公共数据指各级行政机关以及具有公共管理和服务职能的事业单位，在依法履行职责过程中获得的各类数据资源。联系实际而言，可能包含政府才有权利采集的数据，如资源、税收数据，政府在提供服务过程中所收集的公民消费和档案数据，如社会保险、水电数据，政府履行监管职责所采集的数据，如人口普查、食品药品监管等数据。

政务数据的利用与开放是加快政府数字化转型，推进电子政务建设的重要步骤。在收集、使用数据时，政府必须依法定职责和法律规定，健全安全管理制度，将责任落到实处；监督可能涉及的第三方，保障政务数据安全；遵循公正、公平、便民的原则，及时、准确地公开政务数据，实施“清单式管理”，构建统一互通的政务开放平台，将政务数据赋能价值扩到最大，利用数据更好地服务经济社会发展。

对于企业而言，如果在实践中遇到国家机关委托存储、加工政务数据的情形，受托方应配合国家机关完成审批程序，履行法律法规、合同约定的数据安全保护义务，采取必要的技术和组织措施保障政务数据安全，不得擅自留存、使用、泄露或者向他人提供政务数据，并确保获得委托处理政务数据方的授权同意。当然，关于审批程序与企业关于处理政务数据的具体安全义务，还期待相关法规与标准后续进一步细化与支撑。

（四）明确对老年人的特殊保护

《数据安全法》相较于二审稿增加了第十五条，即明确提出支持智能化公共服务的发展，且要求应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。这并不是第一次专门针对老年人的利益需求提出特殊要求。例如，工业和信息化部在今年4月就发布《互联网网站适老化通用设计规范》和《App适老化通用设计规范》，助力老年人、残疾人等重点受益对象平等便捷地获取、使用互联网信息，充分体现了国家在发展过程中的人文关怀，保障老年用户的信息安全。

（五）加大对违法行为的处罚力度

《数据安全法》第六章规定了开展数据活动的组织、个人、数据交易中介机构、国家机关、监管工作人员等主体违反法律规定、未履行义务应承担的法律责任。去年公开的《数据安全管理办法》对于违反法律义务作出的是“一刀切”的罚则，即，“依违规情节，给予网络运营者公开曝光、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等处罚；构成犯罪的，依法追究刑事责任。”本次《数据安全法》的规定针对不同违法行为设置不同的罚责，与《网络安全法》体例保持基本一致，规定了各主体违反法律规定可能承担的不同责任。

比如，有关部门发现数据活动存在较大安全风险的，可以按照规定的权限和程序约谈相关组织、个人并要求采取整改措施。这一规定旨在尽可能从源头消除安全隐患，以最低成本预防安全事故的发生。

开展数据活动的组织、个人未履行数据安全保护义务或未采取必要措施的，可能遭到警告和罚款，**直接负责的主管人员个人也可能被处以罚款**；如果违法行为性质恶劣或造成严重后果，**罚款金额可高达一千万人民币**，并可能被责令暂停相关业务、停业整顿、吊销相关业务许可证或者营业执照，与《网络安全法》第六章规定同步。然而这一数字与《欧盟通用数据保护条例》（以下简称“GDPR”）规定的最高两千万欧元罚款尚有一定的距离，对于掌握千万用户数据的产业龙头企业或采买亿万字段信息的大数据巨头而言，威慑力度虽然也较为有限，但至少也是一个良好示范的起步。

另外，为避免非法来源数据交易的乱象，《数据安全法》第四十七条还规定了针对数据交易中介机构的处罚规则，即相关机构可能被没收违法所得、罚款、吊销营业执照，直接责任人也会被处以罚款，重拳出击规制数据交易行为，应引起相关机构的特别关注。

《数据安全法》第四十八条明确了不配合公安机关、国家安全机关因维护国家安全或者侦查犯罪调取数据的处罚以及未经批准向境外司法或者执法机构提供数据的处罚。《数据安全法》第四十六条还明确了非法对外提供重要数据的处罚。除了对开展数据活动的组织、个人、直接负责的主管人员或直接责任人员罚款外，还可对开展数据活动的组织、个人责令“暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照”。

二、《数据安全法》重要规制与红线要求

（一）以国家主权为立法出发点，兼顾数据保护与利用

《数据安全法》第一条指出，本法的立法目的为“保障数据安全，促进数据开发利用，保护公民、组织的合法权益，维护国家主权、安全和发展利益”，从中可以提炼出“保护和利用并举”与“维护国家利益”两项主要的立法宗旨。具体来看：

《数据安全法》第七条明确表示，“国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展”。可见，维护数据安全和促进数据开发利用是相辅相成的车之两轮。数据开发利用为数据安全提供了技术的支持和概念的革新，数据安全为数据开发利用提供了基础的保障和稳固的底盘。通览全文，对于数据，《数据安全法》并非采取久束湿薪似的保护，而是鼓励对其进行合法利用，从数据中挖掘、开发出更大的经济价值。这一点在《数据安全法》第五章“政务数据的安全与开放”中也有突出体现。

《数据安全法》第七条亦明确规定，国家鼓励数据的合理有效利用、保障数据的有序自由流动。可见，从国家层面对数据利用的态度，是审慎且包容的，采用监管与发展并重。既不因噎废食地完全封闭，又非不加甄别地全盘接受，通过激励相容的制度设计，力求达到二者可持续发展的平衡，最终令数据安全和数据利用协调一致。

（二）适用对象：主客体范围广泛

《数据安全法》第二、三条规定了其适用对象为“在我国境内开展的数据处理活动”。其中“数据”是指任何以电子或者其他方式对信息的记录；“数据处理”是指数据的收集、存储、使用、加工、传输、提供、公开等行为。此外，《数据安全法》附则部分还明确，涉及国家秘密和军事数据的活动，应分别适用《保守国家秘密法》和中央军事委员会另行制定的规则。另外，“开展涉及个人信息的数据活动，应当遵守有关法律、行政法规的规定”。考虑到我国《个人信息保护法》也已经提交到全国人大常委会进行第三次审议，《数据安全法》明确规定个人信息也属于数据的一种，将另由特别法律规制，这为即将出台的《个人信息保护法》预留了空间。由此分析，**《数据安全法》适用对象的范围非常广泛，对于在境内实施任何数据收集、存储、使用等行为的组织和个人，不论主体身份，不论处理的数据数量、频率如何，均应遵守这一法律规定。**



1. 适用主体

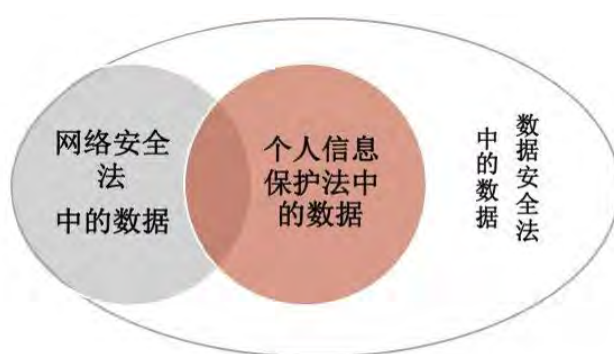
首先，《数据安全法》没有对适用主体进行限制。《数据安全管理办法》规定适用的主体主要是网络运营者，即网络的所有者、管理者和网络服务提供者，《网络安全法》的义务主体亦然。这一表述覆盖的范围可能延展到网络服务的方方面面，已然十分广泛，但《数据安全法》在此基础上更进一步，对适用主体从开展数据活动这一客观行为入手，而非将适用主体限定在某一个类型的主体范围内，更加扩大了适用的范围，最大限度地保障不同层次的数据安全，进而达到数据在有效保护下的合法利用目标。

国际上，对数据安全进行专门立法的情况不多，以色列《数据安全条例》规定适用主体为数据库控制者（Database Controller），再细分为基础、中等、严格三种保护水平。大多数国家的做法是将数据安全作为一个章节规制在个人信息或隐私保护法案中，如《加州消费者隐私保护法》（以下简称“CCPA”）和GDPR对受规制的主体提出具体要求（比如，对企业/组织有一定营业机构/收入的要求）；美国各州法案中也存在保障数据安全的条款，适用对象包括收集使用个人信息的组织（例如：加州民法典）、医疗健康机构（康涅狄格州保险信息和隐私保护法案）、互联网服务提供者（明尼苏达州法典）等。《数据安全法》没有对适用主体做出特别的设定，实际上从客观层面能够达到对数据保护的最大化效果。



2. 适用客体—“数据”与“数据处理”

《数据安全法》对于适用客体即“数据”和“数据处理”进行了较为宽泛的定义。在之前的法律法规或国家标准文件中，如《网络安全法》从关键信息基础设施相关的数据、重要数据、个人信息三个类别对网络运营者进行规制；而后续亟待出台的《个人信息保护法》将侧重对个人信息进行保护。而《数据安全法》则规定，不论呈现形式（电子/其他方式）、不论收集方式（通过网络/非通过网络）、不论数据的内容（可识别身份的个人信息/与国家安全、经济发展以及社会公共利益密切相关的重要数据/其他数据），数据泛指一切对信息的记录。这一定义在我国的立法至今可属创新之举，将“数据”外延界定为摒弃一切修饰词的客观载体，区分了“数据”与“信息”的概念，有效避免了主语与宾语同一的非有效解释。《网络安全法》、《个人信息保护法》和《数据安全法》适用客体的范围类型如下图：



《数据安全法》中对“数据处理”的内涵采取了列举式定义法，提出“收集、存储、使用、加工、传输、提供、公开”等一系列行为及活动。这一定义的逻辑，基本参考了《民法典》的定义逻辑。

联系对比GDPR中数据“处理（process）”的概念以及《信息安全技术 个人信息安全规范》中数据全生命周期的理解，《数据安全法》没有明确涵盖数据“共享”、“删除”及“销毁”这几种典型的数据处理活动。其次，“加工”、“交易”等名词可能源于企业实务中的说法，但在法律层面上，对这些概念的内涵及适用情形有待后续在配套的法规、国家标准中进一步明确。

如上所述，《数据安全法》所规定的适用范围非常广泛，除了大数据公司等视数据为“血液”进行运营的企业需要特别关注以外，**一切可能处理数据的政府、组织和个人也都落在了《数据安全法》规制的范围之内。**

技术的更新与普及使人们普遍享受到大数据带来的快捷与便利，但一些组织为了获得更多的经济利益，将数据采集、加工和利用等准入门槛却越降越低。如果监管缺乏有力的法律依据，更难以实现对数据市场有效的调控和管理。因此，《数据安全法》的出台将所有与数据有关的活动均纳入调整范围之中，**能在基本法层级系统、集中地规范数据安全和利用，为有效监管数据活动提供强有力的法律基础。**

同时，《数据安全法》亦规定了一定的域外适用性，以应对国际空间中数据成为各国在合作与抗衡上的博弈，具体请见下文分析。

（三）明确域外效力

《数据安全法》第二条规定，“在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任”。**这一规定体现了维护国家安全和数据主权的立法宗旨，赋予《数据安全法》以必要的域外适用效力。**

随着数据竞争的日益激烈，各国都在试图扩大数据方面的管辖权。2018年3月，美国通过《澄清域外合法使用数据法》（The Clarifying Lawful Overseas Use of Data Act, CLOUD Act，以下简称“《云法案》”），使得执法部门可依据搜查令直接调取境外数据。从美国司法部对外公布的白皮书对《云法案》适用范围作出的官方解释中^[1]可以看出，《云法案》绝不仅仅适用于在美国注册成立的公司，境外的公司只要在经营活动中与美国有足够的联系（contacts），就可能触发美国法律的管辖权。欧盟则于2019年7月发布了《美国云法案对于欧盟个人信息保护法律框架以及欧盟-美国关于跨境电子取证协议谈判影响的初步法律评估》（Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence，以下简称“《评估》”）。《评估》明确指出，根据欧盟GDPR的规定，《云法案》并不能成为向美国传输个人数据的合法性基础。

除此之外，去年11月，欧洲数据保护委员会（EDPB）对GDPR第三条进行统一解释，并发布了GDPR地域适用的指南，明确了符合“营业机构”标准或“目标指向”标准其中之一的数据处理者和控制者，均需要遵守GDPR的规定。向欧盟居民提供服务、对欧盟居民进行监控、数据处理活动由设立在欧盟境内的营业机构进行或与其有紧密联系的情形均受到GDPR制约。因此，数据处理活动不以物理边界为限，具有抽象的超越国界和领土的特质。各国为有效保障数据安全、维护国家利益，除了通过国际条约与双边/多边协议进行约定，还通过扩大其国内法的适用范围，以求最大程度地降低跨境数据活动给本国带来的安全风险。

全球各国政府跨法域调取数据的情况也越来越常见，根据苹果公司2020年的透明度报告，仅2020年上半年，苹果公司就收到来自超过50个国家及地区的执法机构，共计28,276个数据调取请求。越来越多的中国科技公司走向世界，在主要的经济区都拥有重要的市场份额，故进一步完善对于境外执法机构调取数据的规制尤为重要。

《数据安全法》现行规定以“后果论”为标准，即如果数据活动造成了对我国国家、社会、公民利益损害的，相关组织和个人应被追究法律责任，**确认了我国掌握主动权，以国家利益为主导监管各类数据活动的鲜明立场**。然而，《数据安全法》未规定我国执法机构能对境外组织或个人调取信息或要求协助配合的权限，且相比美国《云法案》（即只要在经营活动中与美国有足够的联系（contacts）便可触发美国法律的管辖权）与GDPR（即向欧盟数据主体提供商品或服务或监控欧盟数据主体）的“行为论”，这一规定并没有将我国对数据管辖权的手臂伸得那么长。

然而，《数据安全法》未对第二条适用范围中的“境内开展数据活动”概念进行定义，笔者认为**为可能会在具体执行上存在一定问题**。例如某一德国公司开发的App在我国境内投放运营后，用户在使用过程中出现软件崩溃，发送故障报告至德国公司的过程即构成在我国境内收集数据的活动。虽然德国公司属于境外组织，其主要营业机构、存储服务器均不在国内，但仍然可能受到《数据安全法》的约束。《数据出境安全评估指南（征求意见稿）》将“境内运营”定义为在中华人民共和国境内开展业务，提供产品或服务的活动，而不论运营者是否在境内注册。另外，还提出了几项参考因素以帮助判断，包括但不限于：使用中文；以人民币作为结算货币；向中国境内配送物流等。笔者认为，对“境内开展数据活动”的理解可以基于该理解类推借鉴，但期待在后续制定相关的配套政策和办法中进行进一步明确。

（四）提出“数据分类分级保护制度”，明确重要数据的界定责任

一审稿即提出了国家应对数据实行分类分级保护，二审稿进而明确提出了“数据分类分级保护制度”的建立及重要数据目录的确定，发布的正式稿对“数据分类分级保护制度”及“重要数据目录”做出了更为清晰的规定。对数据进行分类分级的主要标准为“数据在经济社会发展中的重要程度、以及一旦遭到篡改、破坏或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度”，这也呼应了《数据安全法》以维护国家安全和网络空间主权为根本的基调，这在数据主权博弈激烈的当下显得尤为重要。同时，根据第二十一条，重要数据是数据分类分级中一个类别，由于其关键性和敏感性需要额外的保护。数据分类分级保护制度的提出是现有数据保护制度框架的一个重要补充。相信在后续配套的法律法规及国家标准出台后，数据分类分级保护制度将与网络安全等级保护制度等类似，成为数据保护工作纲领性的要求与指引。

第二十一条明确了国家将统筹协调有关部门在宏观层面确定重要数据目录，并且要求各地区、各部门应制定适应于地区、部门及相关行业的重要数据具体目录，这种双层保护结构也与《重要数据识别指南（征求意见稿）》的思路相一致。这对于厘清何为重要数据并进一步推进重要数据保护工作而言至关重要。此前，《网络安全法》中虽然提到了重要数据，但并未对其进行展开的阐释或定义，《数据安全管理办法（征求意见稿）》和《信息安全技术 数据出境安全评估指南（草案）》虽有对重要数据有定义，但定义也没那么清晰且两者都未生效，指南也不具有法律效力。这对于企业进行重要数据保护工作而言造成了较大的不确定性和操作上的困难。相信随着本法的通过，后续各地区、各部门制定的重要数据具体目录能成为有效的参考，进一步增强数据分类分级保护制度的落地性与实践性。



（五）对于外国歧视性行动的反制裁措施，维护中国企业利益

《数据安全法》第二十六条强化了应对态度，将根据实际情况采取“对等措施”。当下，腾讯、华为等企业不时面临境外采取的限制性或者歧视性经济制裁措施，意图打压中国企业在外国的发展，该条款明确了我国维护中国企业利益的决心，无疑给中国企业打了一枚强心剂。

随着我国科技企业的兴起和5G等尖端技术的开发，各国针对我国企业的限制性措施层出不穷。仅在过去的一周内，美国联邦通信委员会（FCC）将中国两大电信巨头企业列为国家安全威胁名单，禁止美国公司利用八十三亿美元的政府资金购买这两家公司的设备；印度电子信息技术部以“有损印度主权、国防、国家安全和公共秩序”为由宣布禁用TikTok、微信等59款中国应用，且严格管控检查所有从中国购买的电力设备，以确认其中是否存在恶意软件或木马病毒。

一方面可见，数据安全、网络安全已经成为国际社会普遍认可的国家安全版图之一；另一方面可见，我国所面临的挑战和困难也是十分艰巨的。数据已经成为“黄金”、“石油”，也必然成为新兴“兵家必争之地”。全球围绕数据的争夺日益深化，《数据安全法》的制定不仅需要解决国内数据安全管理的問題，还要为数据出境、跨境合作设计等相关规则制定策略。

针对歧视的反制裁措施在国际私法、贸易等领域已有先例，此次在涉及数据安全、国家安全的基本法中重申这一原则，既表明我国拥护数据自由流动、跨境安全的坚定立场，又对他国如有不正当的歧视待遇行为做出了有力的回应。

此外，《数据安全法》第三十六条对处理外国司法或者执法机构关于提供数据的请求做出了规定。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。即企业在面临境外监管机构的直接执法时，不能直接提供境外监管机构要求的数据，而是需要先行上报给我国主管机关，获得批准后方可提供。例如，当中国企业虽未在欧盟设有实体，但直接向欧盟境内的数据主体提供商品或监控欧盟数据主体时，受到GDPR域外管辖。在此情况下，如欧盟的数据保护机构依据其职权对企业进行调查，要求企业提供存储于我国境内的相关数据时，中国企业在向我国主管机关报批获准后方可提供。从实践的角度来说，受限于管辖的限制，即便GDPR规定了自身的域外效力，考虑到现实执法的困难程度，实践中也少有案例直接对在欧盟境内没有实体的公司进行处罚。《数据安全法》的第三十六条无疑显示出对部分国家域外长臂管辖执法进行有礼有节的回应态度。只是日后，需要相关部门规章或者国家标准进一步细化具体报批的机关以及相关流程。

（六）强调对数据出口的管制

《数据安全法》第三十条明确了有关关键信息基础设施运营者以及关键信息基础设施运营者以外的其他重要数据处理者将所收集的重要数据出境的规定，要求适用国家网信部门会同国务院有关部门制定的管理办法。我们在《各国个人信息出境实况——兼评<个人信息出境安全评估办法（征求意见稿）>》文中提到过，个人信息与重要数据出境将采用“二轨制”评估的方式，但此前，重要数据出境监管制度并未特别详细地得到明确，且多为征求意见稿的状态，除了《网络安全法》第三十七条较为概括地要求重要数据本地化，只有有极其特殊情况下方才申请主管部门审批出境（实践中估计也鲜有行业主管部门有审批的流程和经验），其他尚无现行有效的法律法规、国家标准明确数据出境的具体合规方案，从而给企业带来了较大的不确定性。在尚无针对重要数据的专门评估办法出台前，各企业预备重要数据评估的，目前仍然参考的是《个人信息和重要数据出境安全评估办法（征求意见稿）》。

其中，第九条规定了六类涉及重要数据出境时应提交行业主管部门或监管部门进行安全评估得情境，包括：

- 含有或累计含有50万人以上的个人信息；
- 数据量超过1000GB；
- 包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；
- 包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；
- 关键信息基础设施运营者向境外提供重要数据；
- 其他行业主管或监管部门认为可能影响国家安全和社会利益的。



上述规定仍需要企业及相关组织进行全面的自我评估，但具体出境情况是否适用上述规定存在较大的不确定性，对于企业进行重要数据出境安全管理工作带来较大的挑战。数据安全法通过区分主体的方式，对于重要数据出境的监管办法进行了进一步的明确和补充。关键信息基础设施运营者出境重要数据适用《网络安全法》的规定，其他主体出境重要数据则适用国家网信部门会同国务院制定的管理办法，这样的监管思路也使得数据分类分级保护制度能够更好地与关键信息基础设施保护要求相协调。

此外，该条款明确制定数据出境规则的主体为“国家网信部门会同国务院有关部门”，可以体现未来对于数据出境进行规制的法律文件其法律位阶与效力基本是在部门规章的级别，从而加强企业遵守相关义务的必要性。

值得注意的是，除了《网络安全法》及《数据安全法》，一些重要数据的出境还需要重点关注行业监管的要求。比如，《国家健康医疗大数据标准、安全和服务管理办法（试行）》规定健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。《中国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》第六条更是规定，在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行，且除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

根据《数据安全法》第四十六条规定，非法向境外提供重要数据的，“由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款”。

（七）明确企业合规义务

《数据安全法》第四章落实了数据活动主体的具体安全保护义务与责任，列举了一系列需要遵守的合规义务，包括开展安全培训、完善制度建设、风险评估监测、报告安全事件、落实数据分类分级等制度等。具体请参见本文第三部分的分析。

（八）强调数据新技术应当符合社会公德与伦理

《数据安全法》第二十八条要求开展数据活动以及研究开发数据新技术应当符合社会公德与伦理，这一条款则对应了近些年诸多颇具争议的数据新技术，例如医疗AI、Deepfake、ZAO换脸技术等。不可否认的是该等技术的背后是数据活动方面的蓬勃创新，但其所导致的伦理道德问题也一直是社会讨论的重点。例如，2017年一位匿名用户使用“Deepfake”技术将《神奇女侠》中女主盖尔·加朵的脸移植到了一部成人电影的女主身上，再辅以技术手段将其完美的融合，之后将其上传到了Reddit成人交流社区，最终因侵犯个人隐私导致视频下架；2019年3月报道，犯罪分子利用Deepfake技术，冒充英国某能源公司母公司CEO的声音，成功诈骗了二十二万欧元。《数据安全法》的第二十八条正是针对此种新技术所带来的身份冒用、侵犯隐私、造成严重社会负面影响等问题进行了回应。然而，《数据安全法》本身没有对违反此条款规定法律责任，可能实际震慑力较为有限。

(九) 明确数据处理活动不应排除、限制竞争

对于违反其他法律、行政法规的援引条款，《数据安全法》第五十一条明确开展数据处理活动“限制、排除竞争”的场景。

当下，随着《国务院反垄断委员会关于平台经济领域的反垄断指南》的出台以及罚款金额的震慑性，平台反垄断也成为企业的热点话题，该条款明确了数据处理活动也不应该排除、限制竞争，对于怎样的数据处理活动可以产生排除、限制竞争的效果，留待反垄断局或在个案中进一步说明。

(十) 建立与网络安全等级保护制度相衔接的数据安全管理制度

《数据安全法》第二十七条同时强调了数据安全管理体系的建立和网络安全等级保护制度，这使得《数据安全法》能够更好地与现有的数据保护相关法律法规及規制思路相配适。已经建立网络安全等级保护制度的企业能够更好地衔接数据安全管理体系的要求，进一步提升整体的网络安全及数据保护水平。

(十一) 鼓励行业自律，建立行业规范

《数据安全法》第十条指出“相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展”，强调了行业自律在数据安全规范方面的作用，提出了行业数据安全行为规范这一概念，并鼓励各行业组织积极制定适用于本行业的数据安全行为规范，加强行业自律，通过行业内的指导进一步提升数据保护水平。

笔者认为这虽然不是一个强制要求，但也将是未来数据安全保护监管及合规自证体系中一个重要的部分。由于数据处理活动本身对应的场景极具多样性与专业性，法律法规进行落地时可能会存在天然的障碍。该条款通过凸显行业自律的作用，让行业作为规制的一环，从而加强规则的适用性以及与时俱进的能力。

行业自律也为世界其他主要法域国家常见的规制手段。例如，GDPR第四十条及四十一条就早已提出了行为准则（Code of Conduct）这一理念，鼓励有起草行为准则的行业协会或者其他实体制定适合行业的最佳实践。这样的行业最佳实践在通过认证之后，可以成为一个有效的自愿性问责工具。除此之外，这对于一些小微企业而言也是一个能够有效降低合规成本的方案。数据安全法这一概念的提出，也是数据安全监管思路与框架向国际社会中的数据保护监管水平较高的地区看齐的重要一步。



（十）建立与网络安全等级保护制度相衔接的数据安全管理制度

《数据安全法》第二十七条同时强调了数据安全管理体系的建立和网络安全等级保护制度，这使得《数据安全法》能够更好地与现有的数据保护相关法律法规及规制思路相适配。已经建立网络安全等级保护制度的企业能够更好地衔接数据安全管理体系的要求，进一步提升整体的网络安全及数据保护水平。

（十一）鼓励行业自律，建立行业规范

《数据安全法》第十条指出“相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展”，强调了行业自律在数据安全规范方面的作用，提出了行业数据安全行为规范这一概念，并鼓励各行业组织积极制定适用于本行业的数据安全行为规范，加强行业自律，通过行业内的指导进一步提升数据保护水平。

笔者认为这虽然不是一个强制要求，但也将是未来数据安全保护监管及合规自证体系中一个重要的部分。由于数据处理活动本身对应的场景极具多样性与专业性，法律法规进行落地时可能会存在天然的障碍。该条款通过凸显行业自律的作用，让行业作为规制的一环，从而加强规则的适用性以及与时俱进的能力。

行业自律也为世界其他主要法域国家常见的规制手段。例如，GDPR第四十条及四十一条就早已提出了行为准则（Code of Conduct）这一理念，鼓励有起草行为准则的行业协会或者其他实体制定适合行业的最佳实践。这样的行业最佳实践在通过认证之后，可以成为一个有效的自愿性问责工具。除此之外，这对于一些小微型企业而言也是一个能够有效降低合规成本的方案。数据安全法这一概念的提出，也是数据安全监管思路与框架向国际社会中的数据保护监管水平较高的地区看齐的重要一步。



三、企业配套合规义务

对于企业在《数据安全法》项下的合规义务，可以区分为一般企业的合规义务以及处理重要数据的企业额外义务。

（一）一般企业的合规义务

1. 明确企业自身所控制的受规制数据

如前所述，《数据安全法》所规制的数据极为广泛，不仅包括电子的数据，还包括其他形式的的数据，例如员工填表所得的数据。因此，企业首先需要明确企业自身所受《数据安全法》约束的数据范围，并在“数据”这一基本类型的基础上，识别除《数据安全法》外是否须额外受《网络安全法》、日后出台的《个人信息保护法》的规定。

2. 确保数据收集的合法、正当与必要性

根据《数据安全法》第三十二条的规定，任何组织、个人收集数据，都必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据，不得超过必要的限度。除了直接收集外，企业需要特别注意从第三方间接收集数据时，也需要核实第三方数据来源的合法性、正当性，例如进行前期安全尽调、要求第三方签订承诺书、保证书等，并审查自身获取数据是否符合必要性要求。

未能履行合法、正当、必要收集数据要求的企业，则根据《数据安全法》第五十一条的规定，窃取或者以其他非法方式获取数据，开展数据活动排除、限制竞争，或者损害个人、组织合法权益的，按照有关法律、行政法规的规定处罚，从而进一步援引至《网络安全法》、《刑法》、《反垄断法》以及未来出台的《个人信息保护法》等规定。

3. 数据中介服务机构确定交易主体与交易合法性

根据《数据安全法》第三十三条的规定，从事数据交易中介服务的机构在提供服务时，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。《数据安全法》本身并没有对何为“数据交易中介服务”的定义进行规定，我们结合相关实践，初步分析可能是指《信息安全技术 数据交易服务安全要求》中的“数据交易服务平台”（例如上海数据交易中心等提供数据交易平台的企业）等企业。对于此类企业，根据《数据安全法》的规定，需要数据交易一方说明数据来源，审查交易双方的主体身份以及过往是否存在违规交易记录，并对交易记录进行留存。未能按照《数据安全法》要求进行交易数据提供方的背景审核、记录留存的，则根据《数据安全法》第四十七条的规定，导致非法来源数据交易的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得的，处十万元以上一百万元以下罚款，并可以由有关主管部门吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

从落地的角度来说，“数据交易中介服务”概念（例如是否支持民营企业做成数据交易中介等）、交易记录留存时间等尚未明确规定，可能对实践带来一定的障碍，建议相关企业密切关注相关配套法规动态，以便完成相关合规举措。

4. 设立数据安全管理制度，采取技术和必要措施保障数据安全

根据《数据安全法》第二十七条的规定，开展数据活动应依照法律法规规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全，利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。对于企业而言，一方面需要在企业内部设置相应的数据安全管理制度，例如《数据访问权限管理制度》、《IT管理制度》《外部人员访问审批管理流程》等，对涉及处理数据的员工进行专项培训等；另一方面，需要采取相应的技术措施和其他必要措施，保障数据安全，例如采取进行网络安全等级保护认证，采取数据分类分级存储、加密传输、保存等措施。在这里法案并没有要求公司采取企业所能实现的“最高的”技术措施，而是采取“相应的”措施，没有为企业的合规落地设置过高的要求与挑战。因此，企业可能需要结合不同类别数据的情况、风险等级、技术手段与成本，对数据采取技术和安全保障措施。

根据《数据安全法》第四十五条的规定，未能设立数据安全负责人和管理机构的重要数据处理者，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

5. 对数据分类分级保护

对于数据分类分级制度，《数据安全法》借鉴了今年2月工信部印发的《工业数据分类分级指南（试行）》，以一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度作为标准之一，辅以该数据在经济社会发展中的重要程度，对数据进行分类分级保护。相对应地，企业在开展业务的过程中也针对数据的重要程度、敏感程度对数据进行分类分级的保护，例如对儿童的个人信息应当加密存储。信安标委也正在研发《重要数据分类分级指南》；各行业也在研制本行业的数据分类分级标准，企业也可以关注相关动态，以便提前规划合规义务的落地。

6. 按照要求进行安全检测与评估认证

《数据安全法》第十八条指明了国家对安全检测评估、认证服务的支持态度。目前我国是通过中国网络安全审查技术与认证中心，将强制测评与自愿测评相结合进行定期和年度检测认证或自愿认证，企业可以根据自身业务所对应的要求进行相关检测与评估。笔者认为，对于自愿认证的项目，未来也可考虑采取类似司法鉴定机构清单式管理的做法，由国家有关部门对机构的资质、能力进行考核，认证，并将有权开展评估服务的专业机构予以公告。



7. 发生数据安全事件的报告义务

根据《数据安全法》第二十九条的规定，开展数据活动应当加强风险监测，在发现数据安全缺陷、漏洞等风险时，应当立即采取处置措施；发生数据安全事件时，应当按照规定及时告知用户并向有关主管部门报告。

《数据安全法》本身并没有对“数据安全事件”进行明确的规定，可参考其他法律法规、国家标准。《网络安全法》第四十二条说明“在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告”。《数据安全管理办法》第三十五条也采取了类似的表述，即发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，网络运营者应当立即采取补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体，并按要求向行业主管监管部门和网信部门报告。

《数据安全法》本条款目前的写法虽然呼应了《网络安全法》、《数据安全管理办法》的表述，但可能存在以下问题：

“数据安全缺陷、漏洞等风险”与“数据安全事件”之间的关系较为模糊：如果前者只需要立即采取补救措施而不需要上报主管机构的话，那么在《数据安全法》并未对“数据安全事件”作出明确定义的前提下，对于企业落实相关的上报/告知要求存在一定的不确定性；

此外，这里没有明确“数据安全事件”是否仅局限于中国境内运营所发生的数据安全事件。如果中国企业在境外发生了数据安全事件是否需要上报？从《网安法》角度看，可能并不需要上报，但如果事件结果也同时影响了中国境内用户呢？

再则，《数据安全法》尚未对上报的时间进行要求，而是采用了较为模糊的“及时告知”的表述。作为参考，GDPR在规制数据泄露时，则明确要求数据控制者在可行的情况下，应当在知悉数据泄露事件后的 72 小时内告知。如果仅停留在“及时”上报的层面可能难以有效实现对国家有效控制数据安全事件的目的。

期待《数据安全法》后续的配套法律法规、国家标准等文件能够对前述问题进一步澄清与细化。

根据《数据安全法》第四十五条的规定，未能设立数据安全负责人和管理机构的重要数据处理者，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

8. 境内执法的配合义务

根据《数据安全法》第三十五条规定，公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，有关组织、个人应当予以配合。此条款则是从法律的层面明确企业面临公安机关、国家安全机关执法调查时的配合义务。需要提示的是，企业在收到来自公安等其他有关部门协助调查的请求时，应要求其出具相关的执法函件，比如企业可以要求出具《协查函》等方式让公安等文件后进行存档，以便日后作为企业履行企业配合义务提供数据的证明、而非不经查验轻易对外提供用户个人信息。

根据《数据安全法》第四十八条第一款规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款。

9. 遇域外执法时的先行报告义务

根据《数据安全法》第三十六条规定，境外执法机构要求提供数据的请求，非经中华人民共和国主管机关批准，我国境内的组织、个人不得提供。例如，当中国企业直接向欧盟境内的数据主体提供商品、须受到GDPR域外管辖时，如欧盟的数据保护机构依据其职权对企业进行调查，要求企业提供相关的数据时，不能径直接照境外执法机构的要求，提供相关的数据，应当先向主管机关报批方可提供。

根据《数据安全法》第四十八条第二款规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。



（二）处理重要数据的企业额外义务

1. 设立数据安全负责人和管理机构义务

根据《数据安全法》第二十七条的规定，重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。《数据安全法》将必须明确数据安全负责人的企业限定在掌握“重要数据”这个范畴。对于设立数据安全负责人和管理机构义务虽非一项崭新规定，但在设置的要求与对应规制的对象上，与以往的法规还是有所不同。《网络安全法》第二十一条规定网络运营者应当确定网络安全负责人；第三十四条要求关键基础信息设施的运营者应当设定专门的安全管理机构和安全管理负责人；《关键信息基础设施安全保护条例（征求意见稿）》第二十四条要求关键基础信息设施的运营者设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查；《信息安全技术 个人信息安全规范》（2020版）第11.1条则要求个人信息控制者应任命个人信息保护负责人和个人信息保护工作机构。

如前所述，《数据安全法》并没有对受《数据安全法》规制的公司或个人作明确的限定，“重要数据的处理者”、“关键基础信息设施的运营者”、“个人信息的控制者”所涵盖的范围，相互间既有所交织，又略有不同，因此企业在落地实践中，应当更加明确自身处理的数据类型，将主要数据类型视为重点合规的对象，设置相关的负责人与保护机构。当然，在企业内部，为了避免多头设置不同类型数据保护的虚拟部门与负责人员，可以设置一套机构管理企业内部不同类型的数据安全。具体可以参阅《国内企业的DPO工作现状与能力发展》一文。

2. 定期开展风险评估义务设立

根据《数据安全法》第三十条的规定，重要数据的处理者应当按照规定对其数据活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括本组织掌握的重要数据的种类、数量、收集、存储、加工、使用数据的情况、面临的数据安全风险及其应对措施等。

企业如果处理的是重要数据，则需要按照要求定期开展风险评估，并向主管部门报告。因此实施本条仍然是定义并识别重要数据为前提。

未能履行此义务的，根据《数据安全法》第四十五条的规定，未能设立数据安全负责人和管理机构的重要数据处理者，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款；对直接负责的主管人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

3. 合法开展数据出境活动义务

《数据安全法》第三十一条明确了重要数据出境时的合规义务，对于属于关键信息基础设施的企业，则需要根据《网络安全法》的要求，履行相关合规义务；对于其他主体出境重要数据则适用国家网信部门会同国务院制定的管理办法。由于目前与数据出境相关的配套法规、国家标准尚处于征求意见状态，建议公司密切关注相关立法动态，特别是行业内对于本行业数据出境的特殊要求（例如对于特定数据的本地化存储要求）。

根据《数据安全法》新增的第四十六条的规定，违法向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

注释：

[1] 网安寻路人美国司法部“云法案”白皮书中文全文翻译。

“美国对外国公司管辖权的法律限制是基于美国宪法中的约束，并且是美国法院多年来制定的。当公司位于美国时，属人管辖权是最容易确立的。位于美国境外但在美国提供服务的外国公司是否与美国有足够的联系且受美国管辖，是基于对个案中该公司与美国的联系的性质、数量和质量 的考查。公司越是有目的地将其行为引导到美国，法院就越有可能认定该公司受美国管辖。例如，美国法院将这一分析应用于涉及网站的民事案件，重点关注网站与其辖区内的客户的互动程度，同时考虑到网站的功能和机制、对客户的任何特定促销、通过网站招揽业务以及客户的实际使用情况等因素。”

《关键信息基础设施安全保护条例》 要点解读

环球律师事务所
孟洁 | 高亚鹏



【前言】

2021年4月27日，国务院第133次常务会议通过《关键信息基础设施安全保护条例》（以下简称“《关基条例》”）。2021年7月30日，国务院第745号令公布了《关基条例》，并将于2021年9月1日起与《中华人民共和国数据安全法》一起正式实施。《关基条例》的出台，旨在落实《中华人民共和国网络安全法》（以下简称《网络安全法》）有关关键信息基础设施运营者（以下简称“CIIO”）的合规要求，为我国深入开展关键信息基础设施（以下简称“CII”）安全保护工作提供有力保障。

由于《关基条例》最终稿方才面世，本文将主要从如何认定CII、监管部门有哪些、企业义务有哪些、违规责任是什么，以及保障促进措施怎么做等角度进行第一时间的解读。

一、如何认定关键信息基础设施（CII）？

根据《关基条例》第二条开宗明义，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。这与《中华人民共和国网络安全法》第31条的定义方式保持了一致，采用的仍是举例+后果概括的方式，修正了2017年国家互联网信息办公室公布的《关键信息基础设施安全保护条例（征求意见稿）》（以下简称“《关基条例（征求意见稿）》”）对行业进行具体列举的方式，有利于对更大范围的基础网络设施及重要信息系统进行保护。

针对关键信息基础设施边界的认定，此前已陆续公布过《信息安全技术 关键信息基础设施边界确定方法》征求意见稿。《关基条例》此次从行政法规的角度给出了详细指南，第九条规定，《关基条例》第二条涉及的重要行业和领域的主管部门、监督管理部门需要根据本行业、本领域实际，制定关键信息基础设施**认定规则**，并报国务院公安部门**备案**。主要考虑因素包括：

（一）正向角度：网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）负向角度：网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）关联角度：对其他行业和领域的关联性影响。因为关键信息基础设施的对象是一个整体的系统，在不同的行业呈现不同的形态结构。有些系统自身的安全等级不高，但会影响关键业务的整体安全，因此由主管部门与监管部门动态裁减不同行业不同领域在实际状况中针对CII自身安全基线的要求可能比较实际可行。采取风险管理的思维贯穿关键信息基础设施保护的全生命周期，包括识别、防护、监测、预警等，从而构建全局的、整体的具体有韧性的安全防护体系。

关键信息基础设施

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重要网络设施、信息系统。

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。

由于企业的业务形态调整、网络设施与信息系统配置的优化以及威胁与风险的动态变化，在CII所有网络基础设施中，不同的网络设施、信息系统对于保障关键核心业务的运行有不同的效力。厘清CII边界和后续对CII保护工作的开展至关重要，并且当CII运营者的组织结构、业务架构、从属关系等发生重大调整时，应在调整后重新组织边界识别工作。本次公布的《关基条例》特别明确了重新认定关键信息基础设施的期限，即关键信息基础设施发生较大变化，可能影响认定结果的，保护工作部门应当自收到关键信息基础设施运营者报告之日起**3个月**内完成重新认定。

就关键信息基础设施的定义、方法、程序等在，《关基条例（征求意见稿）》和《关基条例》的规定如下：

	2017 年《关基条例（征求意见稿）》	2021 年《关基条例》终审稿
定义范围	第十八条 下列单位运行、管理的网络设施和信息系统，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，应当纳入关键信息基础设施保护范围： （一）国家机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位； （二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位； （三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位； （四）广播电台、电视台、通讯社等新闻单位； （五）其他重点单位。	第二条 本条例所称关键信息基础设施，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。
认定方法	第十九条 国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南。 国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。 关键信息基础设施识别认定过程中，应当充分发挥有关专家作用，提高关键信息基础设施识别认定的准确性、合理性和科学性。	第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。 制定认定规则应当主要考虑下列因素： （一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度； （二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度； （三）对其他行业和领域的关联性影
认定程序		第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。
重新认定	第二十条 新建、停运关键信息基础设施，或关键信息基础设施发生重大变化的，运营者应当及时将相关情况报告国家行业主管或监管部门。 国家行业主管或监管部门应当根据运营者报告的情况及时进行识别调整，并按程序报送调整情况。	第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起 3 个月内 完成重新认定，将认定结果通知运营者，并通报国务院公安部门。



二、何为关基主管部门及保护工作部门？

《网络安全法》第三十九条规定国家网信部门负责统筹协调工作。《关基条例》第三条对应上述条款，明确关键信息基础设施安全保护工作由**国家网信部门**统筹协调，**国务院公安部门**负责指导监督。

《网络安全法》第三十二条规定，按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。而《关基条例》第三条也同时要求，**国务院电信主管部门和其他有关部门**依照《关基条例》和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。**省级人民政府有关部门**依据各自职责对关键信息基础设施实施安全保护和监督管理。



由于企业的业务形态调整、网络设施与信息系统配置的优化以及威胁与风险的动态变化，在CII所有网络基础设施中，不同的网络设施、信息系统对于保障关键核心业务的运行有不同的效力。厘清CII边界和后续对CII保护工作的开展至关重要，并且当CII运营者的组织结构、业务架构、从属关系等发生重大调整时，应在调整后重新组织边界识别工作。本次公布的《关基条例》特别明确了重新认定关键信息基础设施的期限，即关键信息基础设施发生较大变化，可能影响认定结果的，保护工作部门应当自收到关键信息基础设施运营者报告之日起**3个月**内完成重新认定。

相对于2017年《关基条例（征求意见稿）》，本次公布的《关基条例》明确提出了“**保护工作部门**”的概念。即第二条涉及的重要行业和领域的主管部门、监督管理部门为负责关键信息基础设施安全的保护工作部门。《关基条例》依据《网络安全法》的规定，按照“谁主管谁负责”的原则，明确了行业主管部门对于本行业、本领域关键信息基础设施的安全保护责任。

对于具体义务的释明，可以进一步参考全国信息化标准委员会正在制定中的几个国家标准，如《信息安全技术 关键信息基础设施网络安全保护基本要求（送审稿）》、《信息安全技术 关键信息基础设施安全控制措施（报批稿）》、《信息安全技术 关键信息基础设施安全检查评估指南（报批稿）》、《信息安全技术 关键信息基础设施安全保障指标体系（报批稿）》的细化规定。此外，《关基条例》中明确，省级政府有关部门负责对关键信息基础设施实施安全保护和监督管理，修改了《关基条例（征求意见稿）》中县级政府有关部门对于安全保护工作的要求，加大了监管的力度与高度。

	《关基条例（征求意见稿）》	《关基条例》
部门职责	第四条 国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。 国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门在各自职责范围内负责相关网络安全保护和监督管理工作。 县级以上地方人民政府有关部门按照国家有关规定开展关键信息基础设施安全保护工作。	第三条 在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。 省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。
		第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

《关基条例》规定，国家网信部门作为统筹协调部门，应当建立**网络安全信息共享机制**，统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。由于对CII进行重点防护意义非凡，有些情况下对CII的综合防御能力要针对最强大的对手进行设计、提升和创新，因此需要在国家层面形成最高级别的威胁情报收集，打造成一体化的风险识别、监测预警和应急响应机制，同时实现资源共享、安全威胁情报共享，实现快速威胁响应和联动防御机制。基于此，在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

对于具体义务的释明，可以进一步参考全国信息化标准委员会正在制定中的几个国家标准，如《信息安全技术 关键信息基础设施网络安全保护基本要求（送审稿）》、《信息安全技术 关键信息基础设施安全控制措施（报批稿）》、《信息安全技术 关键信息基础设施安全检查评估指南（报批稿）》、《信息安全技术 关键信息基础设施安全保障指标体系（报批稿）》的细化规定。此外，《关基条例》中明确，省级政府有关部门负责对关键信息基础设施实施安全保护和监督管理，修改了《关基条例（征求意见稿）》中县级政府有关部门对于安全保护工作的要求，加大了监管的力度与高度。

	《关基条例（征求意见稿）》	《关基条例》
部门职责	第四条 国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。 国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等有关部门在各自职责范围内负责相关网络安全保护和监督管理工作。 县级以上地方人民政府有关部门按照国家有关规定开展关键信息基础设施安全保护工作。	第三条 在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。 省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。
		第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

《关基条例》规定，国家网信部门作为统筹协调部门，应当建立**网络安全信息共享机制**，统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。由于对CII进行重点防护意义非凡，有些情况下对CII的综合防御能力要针对最强大的对手进行设计、提升和创新，因此需要在国家层面形成最高级别的威胁情报收集，打造成一体化的风险识别、监测预警和应急响应机制，同时实现资源共享、安全威胁情报共享，实现快速威胁响应和联动防御机制。基于此，在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

而针对**保护工作部门**，根据《关基条例》的具体规定，其在相关行业和领域内的职责主要包括：

1. 制定关键信息基础设施认定规则并组织认定；
2. 制定关键信息基础设施安全规划和网络安全监测预警制度；
3. 建立健全网络安全事件应急预案并组织演练、提供指导；
4. 定期组织开展关键信息基础设施网络安全检查检测，监督整改；
5. 发生特别重大网络安全事件或者发现特别重大网络安全威胁时，在收到运营者报告后，及时向国家网信部门、国务院公安部门报告；并对违规CIIO进行处罚。

具体涉及条文如下：

上文职责所对应 序号	《关基条例》法条内容
1	第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。 制定认定规则应当主要考虑下列因素： （一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度； （二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度； （三）对其他行业和领域的关联性影响。 第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。 第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起 3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。
2	第二十二條 保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。 第二十四條 保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。
3	第二十五條 保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。
4	第二十六條 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。
5	第十八條 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。 发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。 第四十條 运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。



三、运营者有哪些合规义务？

《关基条例》在《网络安全法》对网络运营者一般合规义务的基础上，进一步细化了对于CIIO有关规定，强化和落实了关键信息基础设施运营者主体责任，以保证关键信息基础设施安全。

《关基条例》在总则部分第六条总括性地规定了CIIO的网络安全合规义务，即：CIIO依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术**保护措施**和其他必要措施，应对网络安全事件，**防范**网络攻击和违法犯罪活动，**保障**关键信息基础设施安全稳定运行，**维护**数据的完整性、保密性和可用性，在保证系统稳定的同时，维系业务的连续性。

同时，在第三章进一步细化了的CIIO的合规义务，具体包括：

1. 同步规划、建设和使用

根据《关基条例》第十一条，安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用，这一条与《网络安全法》第三十三条是一致的。因此，建议企业在关键信息基础设施规划之初，就将安全保护措施纳入规划的范畴。

2. 设立专门安全管理机构，并履行对专门安全管理机构负责人和关键岗位人员的审查义务

《网络安全法》第二十五条规定了一般网络运营者的上报义务，即网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

《关基条例》第十八条规定明确关键信息基础设施运营者的上报条件、义务和上报机构。根据《网络安全法》第二十一条规定，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，其中包括制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。除第二十一条外，《网络安全法》在第三十四规定CIIO还需履行额外的安全保护义务，其中包括设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查。根据《关基条例》第十二条和第十三条，CIIO的主要负责人对关键信息基础设施安全保护负总责，即实行“一把手负责制”。同时，《关基条例》响应《网络安全法》第三十四条第（一）款的规定，要求CIIO设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

《关基条例》在《网络安全法》对网络运营者一般合规义务的基础上，进一步细化了对于CIIO有关规定，强化和落实了

根据《关基条例》第十五条，企业设立安全管理机构后，主要职责的职责包括：

- (1) 拟订关键信息基础设施安全保护计划；
- (2) 开展网络安全监测、检测和风险评估；
- (3) 制定本单位网络安全事件应急预案，定期开展应急演练，处置网络安全事件；
- (4) 认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；
- (5) 组织网络安全教育、培训；
- (6) 履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；
- (7) 对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；
- (8) 按照规定报告网络安全事件和重要事项。

3. 网络安全检测和风险评估义务

根据《关基条例》第十七条规定，CIIO应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。这一条与《网络安全法》第三十八条保持一致。

4. 重大网络事件上报制度

《关基条例》第十八条规定了，关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，CIIO应当按照有关规定向保护工作部门、公安机关报告。对于特别重大的事件和重大威胁，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。第十八条中的重大事件和重大威胁指的是发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等。

5. 采购产品和服务要求时，合同义务和安全审查义务

第十九条和第二十条分别响应《网络安全法》第三十五条和第三十六条的规定，要求CIIO采购产品和服务要求时安全保密和安全审查义务。即CIIO应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查，这点也与7月10日修订的《网络安全审查办法（修订征求意见稿）》的精神保持一致；运营者应当对外包开发的系统、软件，接受捐赠的网络产品，在其上线应用前进行安全检测；发现网络产品、服务存在安全缺陷、漏洞，应及时采取措施消除风险，重大风险汇报；采购、使用的网络关键设备、网络安全专用产品应当符合国家法律、法规、标准的强制性要求。根据第二十条规定，CIIO采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

6. 合并、分立和解散报告义务

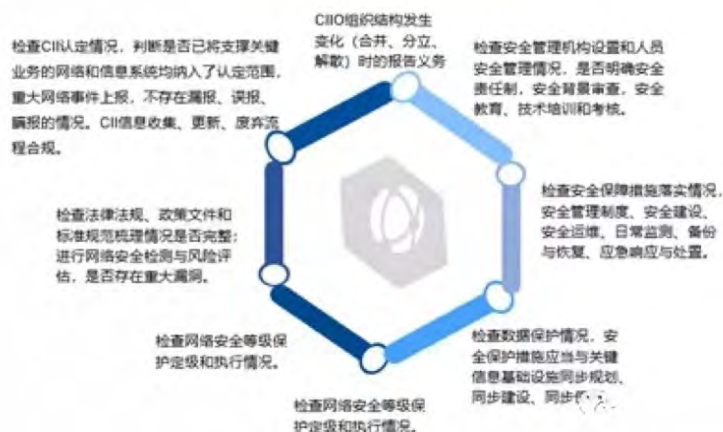
第二十一条规定了CIIO发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。此条义务为《关基条例》在《网络安全法》基础上对CIIO的新增义务。

7. 其他义务

《网络安全法》第三十七条规定，CIIO在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。第三十四条第（三）款规定，关键信息基础设施的运营者还应当履行对重要系统和数据库进行容灾备份的义务。尽管《关基条例》未再次重申《网络安全法》所提及的上述义务，但上述义务依然属于法律规定的合规义务，因此，相关CIIO依然需要重点关注。

■ 数据保护合规体系的建议

CIIO的保护合规体系，我们建议从如下方面着手建立和完善。



四、具有哪些法律责任？

《关基条例》在第五章法律责任部分规定了四类主体的罚则，分别为（1）CIIO；（2）网络攻击者；（3）网信部门、公安机关等保护机关及其工作人员；及（4）电子政务关键信息基础设施的运营者。

1. CIIO罚则

CIIO的罚则与第三章CIIO的义务责任相对应，规定了CIIO在不履行相关义务责任时的相关罚则。

第三十九条规定了未履行“同步规划、建设和使用义务”“设立专门安全管理机构，并履行对专门安全管理机构负责人和关键岗位人员的审查义务”“网络安全检测和风险评估义务”和“合并、分离和解散报告义务”义务的罚则。

《关基条例》第三十九条与《网络安全法》第五十九条第二款规定的罚则一致，即CIIO有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款：

- (1) 在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；
- (2) 安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；
- (3) 未建立健全网络安全保护制度和责任制的；
- (4) 未设置专门安全管理机构的；
- (5) 未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；
- (6) 开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；
- (7) 专门安全管理机构未履行本条例第十五条规定的职责的；
- (8) 未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；
- (9) 采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；
- (10) 发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

第四十条规定了对于未履行“重大网络事件上报义务”的罚则，即CIIO在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

第四十和第四十一条规定了未履行“采购产品和服务要求时，合同义务和安全审查义务”的罚则。除上述第四十条规定外，根据第四十一条规定，CIIO采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额1倍以上10倍以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款。这一点与《网络安全法》第六十五条的规定基本一致。

最后，第四十二条规定了CIIO配合检查义务时的罚则。根据此条规定，CIIO对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节严重的，依法追究相应法律责任。

2. 网络攻击者罚则

《关基条例》对“实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪”的网络攻击者的罚则，并对个人违法行为和单位违法行为进行了区分。

对于个人违法行为，根据《关基条例》第四十三条规定，将依照《网络安全法》有关规定，由公安机关没收违法所得，处5日以下拘留，可以并处5万元以上50万元以下罚款；情节严重的，处5日以上15日以下拘留，可以并处10万元以上100万元以下罚款。违反第五条第二款实施非法侵入、干扰、破坏关键信息基础设施的活动，危害关键信息基础设施安全或第三十一条对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动，受到治安管理处罚的人员，5年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

对于单位违法行为，根据《关基条例》第四十三条规定，将由公安机关没收违法所得，处10万元以上100万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。”

3. 网信部门、公安机关等监管机关及其工作人员罚则

第四十四条、第四十五条和第四十六条规定了网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行监督管理、廉洁、数据安全等相关义务时的罚则。

监管机关及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

监管机关或其他部分在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

监管机关或其他部门在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

此外，第四十七条规定了关键信息基础设施发生重大和特别重大网络安全事件的追责制度，对于上述事件经调查确定为责任事故的，除应当查明CIIO责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

4. 电子政务关键信息基础设施的运营者罚则

《关基条例》第四十八条规定电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《网络安全法》有关规定予以处理。即《网络安全法》第五十九条第二款，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

5. 兜底条款

《关基条例》第四十九条为兜底条款，根据此条规定，违反《关基条例》规定，给他人造成损害的，依法承担民事责任。违反《关基条例》规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

五、如何实施保障与促进措施？

《关基条例》第四章单独规定了保障和促进措施，即保障关键信息基础设施安全，需要统筹资源和力量，全方位实施保护。

在保障方面，第一，明确要求监管机关建立网络安全信息共享机制（第二十三条），并规定工作中获取的信息只能用于维护网络安全，不得泄露、出售或者非法向他人提供（第三十条）。第二，对国家有关部门开展安全检查作出规定，要求避免不必要的检查和交叉重复检查，检查不得收费，不得要求被检查单位购买指定产品和服务（第二十七条）；同时规定任何个人和组织未经授权不得对关键信息基础设施进行探测测试等活动（第三十条）。第三，规定国家网信部门和国务院电信主管部门、公安部门等根据保护工作需要，提供技术支持和协助（第二十九条）。第四，明确国家对能源、电信等关键信息基础设施安全运行实施优先保障（第二十二条）。第五，规定公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动（第三十三条）。六是明确国家出台安全标准，指导规范关键信息基础设施安全保护工作（第三十四条）。

《关基条例》在支持促进方面，从人才培养（第三十五条）、技术创新和产业发展（第三十六条）、网络安全服务机构建设与管理（第三十七条）、军民融合（第三十八条）、表彰奖励（第七条）等方面均作了相应规定。

【总结】

整体而言，《关基条例》对于关键信息基础设施安全工作的主要问题，在《网络安全法》确立的制度下，就关键信息基础设施的相关制度措施进行了细化，并与《网络安全法》《网络安全审查办法》《网络产品安全漏洞管理规定》等相关法律法规相衔接。同时明确分工职责，充分发挥政府监督等各方面主体作用，并强化和落实CIIO主体责任。建议相关企业对于CIIO的身份进行预判和识别，并落实CIIO相关合规义务和责任。

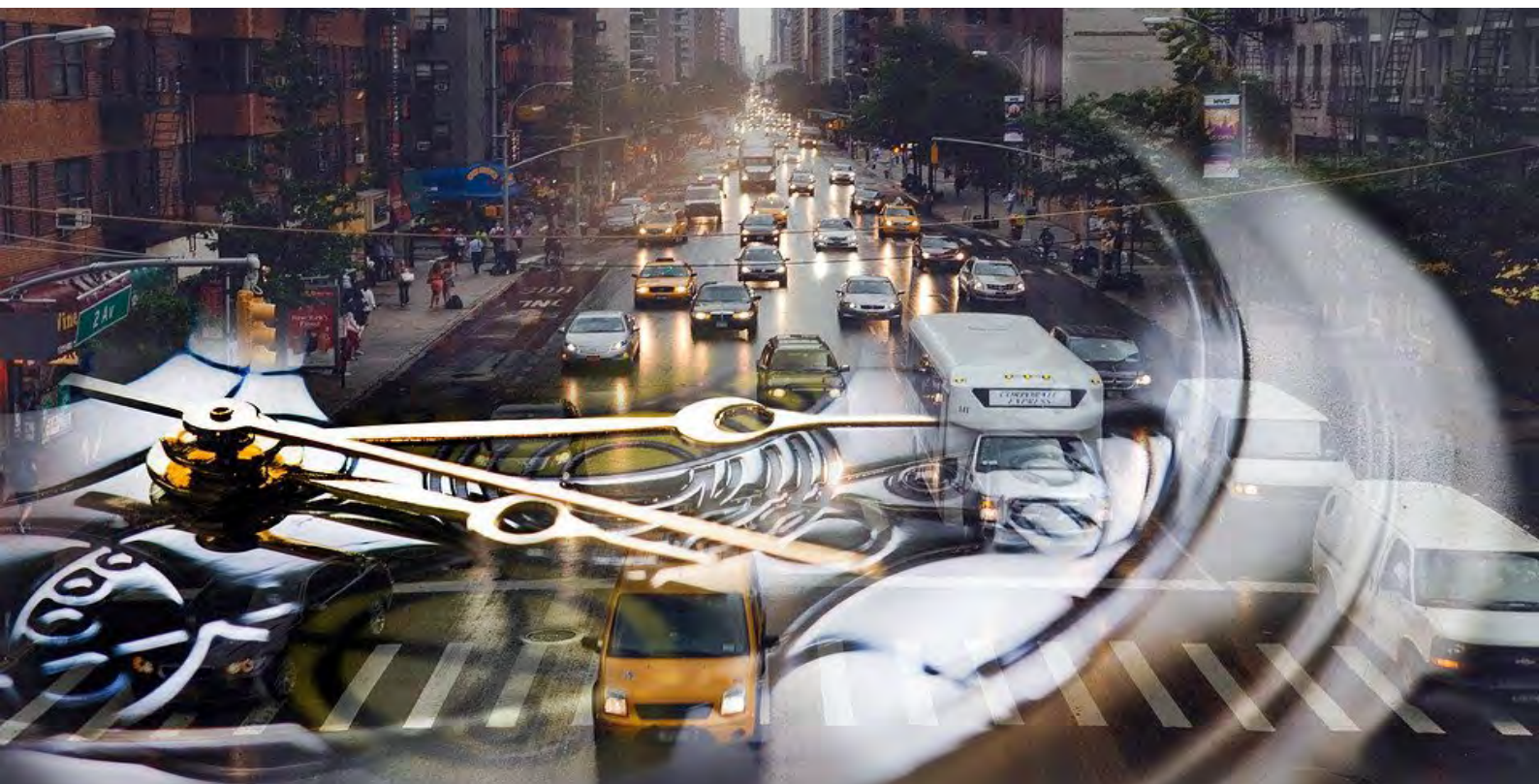
“隐私”与“个人信息” 别再傻傻分不清

孟洁（环球律师事务所）

薛颖（知名互联网企业隐私合规专家）

朱玲凤（知名互联网企业隐私合规专家）

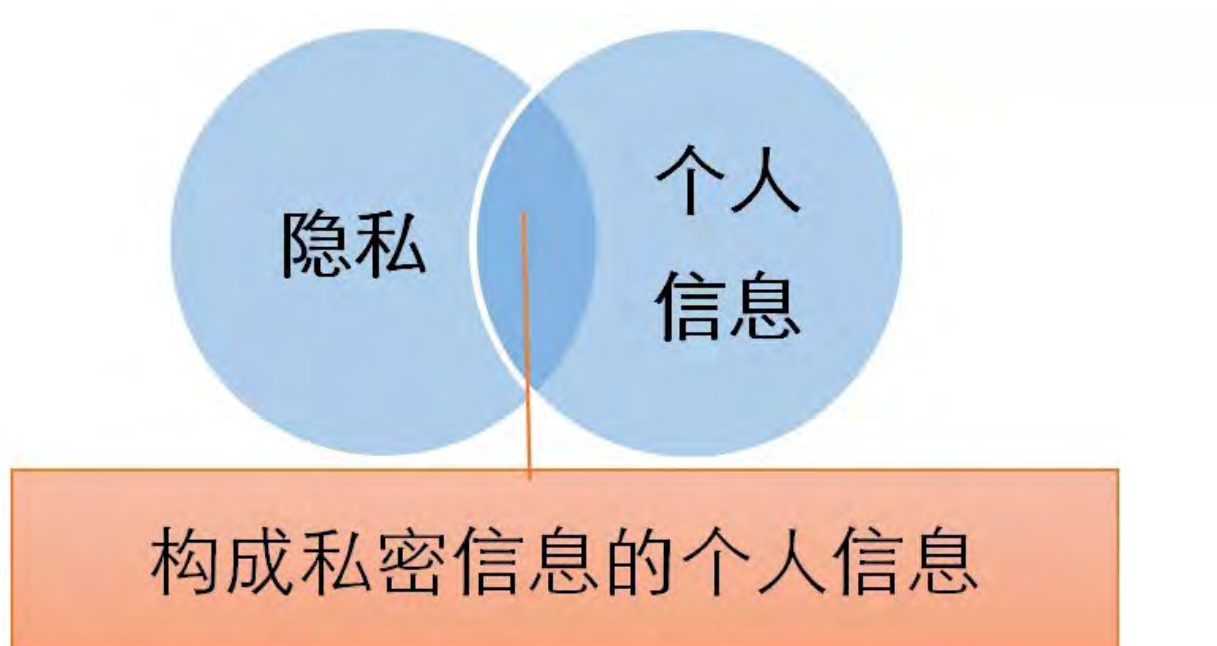
*本文为作者个人观点，不代表所在单位立场



【前言】

作为《民法典》中的“新料”，“隐私”和“个人信息”被一并列入人格权编以专章保护，两者经常被混同，那它们之间究竟是什么关系呢？

简单粗暴地说，在《民法典》下，这两者都被用于保护大数据时代的信息主体人格权益且但分别对应两个请求权基础，只是各自保护的对象有重叠部分——



一、隐私≠个人信息

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息，权利主体的核心目的在于“不愿为人知晓”和“生活安宁”，即隐私的核心是“私密性”，即信息主体不想让外界知悉这些空间、获得的信息，即使有些信息并不属于他的个人信息，甚至只是一种物理空间（私人活动所覆盖的范围）。由于主体行权的目的多在于防御第三人获知，因此是一种相对偏主观感觉的认知。

个人信息则是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的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等，**核心是“可识别性”**，即该等信息可直接或结合识别出特定自然人，主体行权目的多在于想要积极管理已授权第三人处理的个人信息。但是否属于是其个人信息，则是相对偏客观事实的认定。

因此，针对自然人的隐私或个人信息而言，“**私密性**”和“**可识别性**”是两种重要但不同的划分维度，存在一定程度上的重合（即主观上不愿让外界知悉的、客观上可识别其个人的信息），大体可分为下述情形——

情形	信息的二元属性	举例
1) 既是隐私，又是个人信息	既有私密性，也有可识别性	基因数据、性取向
2) 不是隐私，仅是个人信息	无私密性，但有可识别性	面部特征、手机号码
3) 仅是隐私，非个人信息	有私密性，无可识别性	将游戏人物作为暗恋对象
4) 既非隐私，也非个人信息	无私密性，无可识别性	匿名化的数据

值得注意的是，上表的前三种情形存在此消彼长、相互角力的有趣情况。特别的，随着大数据时代进行信息收集、追踪、匹配的能力越来越强，**个人信息的边界在不断扩展，而可被归入到隐私范畴的信息却越来越少**，即情形2) 扩张为主流样态、情形1) 和3) 的空间却越来越小[1]。这才导致老百姓常常有种错觉，认为个人没有“隐私”，甚至将个人信息与隐私混同。

二、模糊的边界：构成私密信息的个人信息

如前所说，作为隐私权和个人信息重叠保护对象的“私密信息”是《民法典》下一个重要的新生术语，也是最难界定的人格权客体之一。如果一项信息同时具备“能够识别自然人”和“主体不愿为他人知晓”两个要件，才是“构成私密信息的个人信息”。

但在个人信息处理和司法实践中，对某一信息属性的认定难点往往不在于“可识别性”，而在于难以判断“私密性”，即构成个人信息的同时是否还会进一步构成私密信息。然而，是否构成私密信息不仅是一项主观认定，而需要同时兼顾考虑三重视角：

- **信息主体个人的合理隐私期待**，即，作为信息主体个人的内心感觉、想法、诉求、期待、愿景。
- **普通人的一般合理认知**，即，作为一个普通人通常会作出的预期判断与根据正常人的社会经历和认知水平会作出的内心反应。
- **实际的信息收集和处理场景**，即，在特定情况下并结合当时的具体情境会做出的心理判断与暗示。

如果以上三者任何一因素发生变化，对于个人信息的“私密性”判断都可能出现不同结果。例如，极端来讲，即使“性取向”系敏感个人信息、公众亦一般认知为隐私，但是否绝对属于“隐私”，也要看主体自身的性格、认知、理解力与抗压性、主体所在环境的包容性与开放性、是否有主动意愿公开、是否为实现特定诉求、是否因此会遭受歧视性待遇等。例如在一些较为传统的社区环境，个人一般不愿意公开同性取向，而在开放程度大的城市，愿意公开同性伴侣关系的人越来越多，而一些公众人物公开表明自己的性取向，就更难以构成其隐私了。当发生隐私权与个人信息认定的争议时，法律应当同时考虑以上三点、不可偏废一端，才能保证其公平公正。

在北京互联网法院的“抖音”案中，判决从用户合理隐私期待的纬度将个人信息兼具的隐私属性划分为三个层次：一是符合社会一般合理认知下共识的私密信息；二是不具备私密性的一般信息；三是兼具防御性期待及积极利用期待的个人信息，是否侵权就需要结合信息内容、处理场景、处理方式等进行符合社会一般合理认知的判断^[2]。另一民事判决中从场景化角度来分析，指出社交应用的好友关系在一定范围内已公开，并非不愿为他人知晓的私密信息。当然，这些诉争标的兼具个人信息与隐私权争议的案件还比较零星、尚未形成普遍共识。虽然对于社交软件中的虚拟社交关系、电话通讯录等构成个人信息的分歧不大，但这些信息是否同时仍然具有“私密性”的属性，则在企业 and 用户产生很大分歧。因不同社交软件对社交关系的公开模式多有差异，因此用户的合理隐私期待也**应该场景化识别**，即不应脱离具体软件的适用场景概括出过于抽象的论断。

此外需要注意，并没有法律规定隐私必须是“被他人知晓后会导致个人主体遭受负面或不当评价”的信息。隐私指向的私密性如果遭到破坏，会导致主体无法实现其合理隐私期待、精神或客观上受到一些伤害，但却并不意味着一定会受到名誉毁损。**如果以他人如何评价该等信息来作为隐私的构成要件，将会极大缩减隐私权的适用范围，变相抬高了该权利的保护阈值。**

三、区分隐私权保护和个人信息保护的核心意义： 处理者可适用的正当性事由不同

区分隐私权保护和个人信息保护的核心意义，并不在于信息主体能获得的救济有多少差别。如果用户仅仅选择“隐私权”或“个人信息保护”两者之一作为其维权的请求权基础，并不意味着主张个人信息保护所获得的救济就必然较少、侵犯隐私权承担的赔偿责任必然较大，毕竟停止侵害、消除影响、赔礼道歉和赔偿损失等民事责任方式都分别适用这两项独立的人格权救济，但**隐私权的权利主张体现出信息主体更希望就该等信息的私密性获得司法认可**（当然，实践中证成私密性一般比证成可识别性更有难度）。但更为重要的是，**就可适用的正当性事由而言，处理隐私比处理个人信息的条件要严苛得多。**

1 处理隐私的正当性事由

处理隐私的正当性事由极其有限，仅限于——

- 基于法律规定；
- 基于权利人明确同意。

因此，**不能基于行政法规等**低位阶的法律渊源且不能在没有主体“明确同意”的情况下处理隐私。例如，公开患者病历资料只能基于患者同意，而不能基于其他的事由。

2 处理个人信息的正当性事由

相比之下，处理个人信息的正当性事由则宽泛得多：

- 法律、**行政法规**的规定；
- 在该自然人本人或者其监护人同意的范围内合理实施的行为；
- 合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；
- 为维护公共利益或者该自然人合法权益，合理实施的其他行为；
- 为公共利益实施新闻报道、舆论监督等行为而合理使用。
- 《个人信息保护法》进一步增加其他正当性事由，如为订立或者履行合同所必需、为履行法定职责或者法定义务所必需等。

因此，一旦一项司法判决认定某项信息不构成“隐私”、只能以“个人信息”来保护，则其实际影响意味着**收集该等信息的企业可选择的正当性事由更多、合法性空间拓宽**，甚至，即使都是基于“同意”来处理，获取有效同意的门槛实操起来也可能会有所降低（如告知/单独/明确/具体等同意要件的严苛度弱化、产品端合规形式相对宽松等，不会考虑该等同意是否真正满足了主体的合理隐私期待）。

四、不受隐私权保护不等于不受个人信息保护

近期大众针对个别司法判决产生的朴素观点认为某项信息“**不属于隐私就不受保护，企业可以肆意使用**”，其实是个巨大误解。虽然隐私权客体之一的私密信息和个人信息的边界因在一定程度上相互交织而带来了可解释空间，但《民法典》仍以专章形式给出了隐私权和个人信息两种并存的保护路径：

(1) 即使与自然人相关联的某一信息不属于隐私权保护的范畴，但如果具有“可识别性”，仍然可以作为个人信息保护

(2) 如果该等信息既具有隐私权属性，也构成个人信息，**则应当采用“隐私权保护优先+个人信息保护补充”的叠加保护方式**：优先适用处理隐私的正当性事由和获得隐私权侵权救济，同时也应该遵守个人信息保护的其他要求，包括不仅应当遵守《民法典》中关于个人信息保护的六字箴言“正当/合法/必要”、告知透明（第1035条）、确保安全（第111和1038条）和实现主体权利（第1037条）等规定，还应该遵守《网络安全法》等相关法律法规中对个人信息保护的规定。当然，侵害方因同一行为同时承担民事责任、行政责任和刑事责任的，财产应优先用于承担民事责任。

上述复杂的保护路径背后体现了大数据时代对传统的隐私权保护框架产生了冲击，而民法则不得不作出相应的回应。在大数据和网络化时代，几乎自然人的所有行为都可以被数字化表征和处理，无论是互联网还是物联网企业，都离不开数据（包括私密信息）来提高效率和产能，数据也成为了很多企业向个人用户提供服务的基础，所以产生了从用户让渡个人信息的绝对权转化为个人要求企业合理利用个人信息的诉求变化。

但即使如此，仍然需要企业处理个人信息时尊重主体的最低信任水平和满足其基本的隐私期待，以期达到一种平衡：对于可积极利用而不会对基本人身自由和尊严造成重要影响的可识别性信息予以“个人信息保护”以替代“隐私权保护”，以遵循一定规则下的可利用性来代替纯粹的防御性；对于其他构成隐私的个人信息仍然受到隐私权保护，隐私权仍然是人之为人的尊严和自由所不可分割的人格利益，不会因为大数据时代的到来而磨灭。

苹果CEO库克在2021年1月的一次演讲中提到“如果我们接受生活中的一切都可以被汇总和出售，并且认为这是正常的、不可避免的，那么我们失去的不仅仅是数据，而是失去了做人的自由”。综上所述，“隐私”和“个人信息”都是保护我们在大数据时代人身尊严和自由的法律武器，《民法典》也基于对于两种权益的不同诉求制定了相应的保护路径，信息主体则应该根据信息的不同属性搭配适用相应的请求权基础。

最后还要说明一下：把“隐私”和“个人信息”做上述精细的区分是基于我国《民法典》的规定，而在日常生活、企业数据合规治理、大众媒体、跨境交流等语境下时刻都进行上述区分则未必有必要或可行，比如你看库克这次演讲中通篇都在说的“隐私”其实大部分都是我国《民法典》说的“个人信息”，但也不妨碍在大家都理解这里以保护隐私之名来保护个人信息或反之亦然……你懂的。

注释：

[1] 在“庞先生诉趣拿公司”一案中，二审法院明确指出，“在当今的大数据时代，信息的收集和匹配成本越来越低，原来单个的、孤立的、可以公示的个人信息一旦被收集、提取和综合，就完全可以与特定的个人相匹配，从而形成某一特定个人的详细而准确的整体信息。这些整体信息一旦被泄露扩散，任何人都将没有自己的私人空间，个人的隐私将遭到巨大威胁，任何他人未经权利人的允许，都不得扩散和不当利用能够指向特定个人的整体信息。”

[2] 黄某诉微信读书案（2019）京0491民初16142号。



个人信息保护工作机构及负责人设置要求

环球律师事务所
孟洁 | 鲁裕鑫



【前言】

《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）第五十二条明确要求，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。在法律层面明确了企业需要设立个人信息保护负责人这一要求，本文将重点介绍我国相关立法及标准的规定，并结合欧盟的要求进行具体分析。

一、欧盟

业内实践中，多以“DPO”作为此类岗位负责人的统一称谓。这一表述最初引自欧盟《通用数据保护条例》（GDPR）——“Data Protection Officer”。但是，GDPR并未对其做出明确定义。笔者理解，DPO集“普法专员”“内部督查员”“客服专员”“政府公关专员”“信息安全专员”等多岗位于一身，并具有独立履行职能，有助于企业遵守法律法规，引导企业和员工履行GDPR项下的义务，监督企业内部数据合规制度的执行，配合监管机构进行监督与执法，是“问责机制的基石与纽带”。

根据GDPR第37条第1款规定，数据控制者和数据处理者应当在以下三种情况下设立DPO：1. 处理是公共机构或公共实体进行操作的，法庭履行其司法职能时除外；2. 数据控制者或数据处理者的核心处理活动天然性地需要大规模性地对数据主体进行常规和系统性的监控；或者3. 数据控制者或数据处理者的核心活动包含了第9条规定的对某种特殊类型数据的大规模处理和第10条规定的对定罪和违法相关的个人数据的处理。

GDPR规定的的数据保护官的职责主要包括：1. 告知组织机构及其员工在GDPR和其他相关数据保护法规下的各项义务；2. 监督组织机构是否遵守GDPR及其他相关数据保护法规的规定，是否符合组织机构内部与个人数据保护相关的政策，具体包括参与责任分配，对数据处理活动人员进行培训以及制定提高相关人员合规意识的政策；3. 就是否进行隐私影响评估及监督隐私影响评估执行情况提供意见；4. 与主管监管机构进行沟通并作为其所在组织机构的内部联络人。

同时，GDPR也提供了一些基本保证，以确保DPO能以独立的方式行事。例如，数据控制者和处理者必须确保在执行与数据保护相关的任务时，DPO不会受到公司任何干扰的指示，包括最高管理层人员。此外，不得因他们执行任务而以任何方式解雇或处罚他们。例如，DPO认为，组织的活动可能会导致数据主体处于高风险时，可以建议控制者或者处理者进行数据保护影响评估。如果公司不同意DPO的建议，不认为它有充分根据并决定不进行安全影响评估的，公司可以忽略这些建议，但是，不能因DPO提出建议而对其进行解雇或惩罚。

根据GDPR以及EDPB出具的相应解释条文，对于满足条件的企业，设立DPO属于一项必须履行的法律义务，尽管法规没有规定诸如“大规模系统监测”和“核心活动”等术语，但是，第29条工作组已就如何解释这些条款发布了指导原则。例如，社交媒体和搜索引擎公司作为数据控制者，其商业模式往往基于大量个人数据的处理、大规模定期和系统地监控数据主体，通过提供有针对性的广告服务和允许公司在其网站上订阅广告产生可观的收益。其中，效果类广告是一种根据人口统计数据 and 消费者历史购买记录或行为投放广告的方式，因此，需要系统地监控数据主体的在线习惯和行为。根据GDPR，这类企业被强制要求任命DPO。另外，医院和医疗保险公司的活动包括对特殊类别个人数据（包括遗传和生物特征数据）的大规模处理或披露同样需要加强保护，因此，GDPR也要求其指定数据保护官。如果不设立，属于违反GDPR的明确规定，将面临相应的法律责任。对于依法可以不设立DPO的企业，EDPB的解释条文中仍建议这部分企业设立DPO，并将“是否有专人负责数据保护以确保组织按照GDPR的规定处理数据”作为证明公司合规性的有力参考因素之一。

在决定设立DPO后，企业接下来考虑的问题应当是DPO所应当具备的基本素质，从而缩小目标范围，确保委任的人选能够切实有效的帮助公司规避合规风险、及时响应监管及个人信息主体的要求并妥善处理。

结合相关法律法规的要求，笔者认为，DPO至少应当具备以下几点基本素养：

- 掌握一定的专业知识并具有独立履行职责的能力，在处理数据保护方面有实践经验；
- 与数据控制者之间有被雇佣或被委托的关系；
- 具备较强的沟通与协调能力，能够妥善处理来自监管机构或个人信息主体的各项要求或投诉；
- 熟悉公司内部的业务模式以及数据流转情况，能够对公司的合规工作提出可落地、可执行的建议措施。

而对于DPO的人选，公司既可以选择由公司内某位员工担任，也可以聘任外部人员如律师等担任。但考虑到DPO需要配合企业落实上文中所述的义务及要求，笔者建议企业在聘任DPO的时候优先考虑自有员工；如果公司出于其他考量需要从外部聘任DPO的，应当与其签订书面的聘用协议，并在协议中对DPO应当履行的职责及工作进行明确约定，从而确保DPO能够有效地帮助企业业务正常发展的情况下满足法律监管的要求。

但需要提示公司注意，一旦公司任命了DPO，必须确保其在所有与个人数据保护相关的问题中及时、全面地参与。为了使DPO能够有效地执行其任务，公司必须为其提供必要的资源，包括财务资源、基础设施和设备，还包括为DPO提供足够的时间来履行其职能，并提供持续培训，使他们能够发展自己的专业知识并及时了解数据保护法律法规的所有发展。此外，DPO的成功设立，并不代表责任及义务的转移，数据控制者和数据处理者仍是责任承担的主体。在GDPR体系下，DPO本人不会因为履行职责而受到免职或惩罚，WP29更是明确地指出DPO履行勤勉义务的情况下，对企业数据不合规不负个人责任，而是由数据控制者承担确保数据合规的义务。但DPO仍可能会因自身的渎职、失职行为而受到处罚，各成员国的立法中，部分国家也对DPO自身职责履行行为不当的情形做出了处罚规定。

因此，公司及DPO本人均应当充分重视以下几个方面的合规义务。概言之，DPO本人应当严格按照法律法规履行职责，充分履行勤勉注意义务；公司应当充分支持DPO工作，并依照DPO的合规建议，在内部积极整改及落实。具体来说：

- 对现有法规进行解读、新法跟进以及定期组织法律法规内部培训；
- 协助制定及落实符合法律法规要求的内部制度及流程等文件；
- 负责开展及监督DPIA工作；
- 对日常数据处理操作进行监督与审计，并提出合规意见；
- 落实数据处理岗位相关员工的职责及义务说明；
- 在监管机关审查时，履行配合、响应义务；
- DPO直接向最高管理层报告，其履行的其他任务或职务不能与DPO的职务产生利益冲突。

DPO能否有效开展后续的合规工作，更多情况下取决于企业领导层的支持与配合。同理，企业负责人对个人信息保护内容的熟识程度与支持力度，也取决于DPO平时对政策动态、行业资讯的及时了解并主动分享，以及与企业负责人进行沟通交流。DPO与公司之间多是一种互相支持与促进的关系。企业任命DPO，并给予相应的资源支持，DPO则应为企业的业务发展保驾护航。定期组织全员培训，提高员工的数据保护意识，能够有效避免安全事件、用户投诉等问题发生。

企业设立DPO除了可以落实这一项法定义务外，还可以在DPO的协助下从上文所述的几个方面提升合规水平，成本与收益的对比一目了然。

二、中国

相较于欧盟以统一、集中且具体的方式对DPO的设立及职责等情况进行规定，我国目前没有“DPO”或“数据保护官”这一称谓。但是，可以从一些现行法律法规及国家标准中找到类似的表述。从实质看，这些职务尽管叫法不同，其设立的目的与意义都是类似的，以下可能统称为“数据保护岗位负责人”。

在《个人信息保护法》生效之前，我国已有部分法律法规和规范性文件对企业的网络安全保护/个人信息保护义务进行了规定，并且要求设置类似信息保护负责人的职位，例如2017年6月1日生效的《中华人民共和国网络安全法》（以下简称“《网络安全法》”）第二十一条明确要求网络运营者应当制定内部安全管理制度和操作规程，确定“网络安全负责人”；对于关键信息基础设施的运营者，第三十四条作出了进一步安全保护义务要求。再如2021年9月1日生效的《中华人民共和国数据安全法》（以下简称“《数据安全法》”）第四章“数据安全保护义务”中对于重要数据处理者，明确要应当设置“数据安全负责人”以落实数据安全保护责任。但无论是《网络安全法》还是《数据安全法》，均并未明确“网络安全负责人”或“数据安全负责人”的具体责任与义务，而只是从宏观的角度上给予指引。

笔者对目前各法律法规及标准中对类似职位的名称职位、职责以及未设立相应职位可能受到的处罚情况进行简要汇总与对比。

法规	职务名称	职责	未设立的法律后果
《网络安全法》	网络安全负责人	落实网络安全保护的相关工作。	由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款。 (如涉及关键信息基础设施的运营者) 由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款。
《数据安全法》	数据安全负责人	重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。	由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。



《关键信息基础设施安全保护条例》	关键信息基础设施网络安全管理机构负责人	领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。	由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款。
《银行业金融机构数据治理指引》	首席数据官（自愿）	主要负责人对数据质量承担最终责任。	/
《个人信息保护法》	个人信息保护负责人	对个人信息处理活动以及采取的保护措施等进行监督。 个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。	由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。
《儿童个人信息网络保护规定》	儿童个人信息保护负责人	负责儿童个人信息保护相关的工作，对内部员工处理儿童个人信息的行为采取审批、记录等限制措施。	参照《网络安全法》的规定，推定可能会受到十万元以下的罚款及警告、责令改正的处罚。

《信息安全技术 个人信息安全规范》（GB/T 35273-2020）（以下简称“《国标》”）	个人信息保护负责人	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。	
---	------------------	---	--

（一）设立与职责

从上表可以看出，关于数据保护岗位的设立和职责的规定，我国多是以“一般+特例”的方式进行规定，至于这几个岗位之间的关系，笔者主要从上表所列的职责范围以及各职位之间能否兼任这两个维度进行具体分析：

（1）职责范围

结合法律法规及项目工作经验，笔者对上表中各职位的职责范围进行比对，仅供公司在设立相应职位时参考。

首席数据官≥网络安全负责人=网络安全管理机构负责人>数据安全负责人>个人信息保护负责人>儿童个人信息保护负责人。

(2) 《个人信息保护法》中对于个人信息保护负责人的要求

首先，根据《个人信息保护法》的要求，应当在境内设立个人信息保护负责人的情况主要包括：

1. 处理个人信息达到国家网信部门规定数量（参考《国标》要求）的个人信息处理者；
2. 在境外处理境内自然人个人信息的个人信息处理者。

其次，根据《个人信息保护法》的要求，个人信息保护负责人的工作职责主要包括：

1. 根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取措施；
2. 防止未经授权的访问以及个人信息泄露、篡改、丢失；
3. 定期组织对处理个人信息遵守法律、行政法规的情况进行合规审计；
4. 对个人信息处理活动进行个人信息保护影响评估；
5. 对于信息泄露、篡改、丢失采取补救措施，并通知履行个人信息保护职责的部门和个人。

此外，《个人信息保护法》中也对个人信息保护负责人的设立要求与职责义务做出了明确规定。

《个人信息保护法》中对于个人信息保护负责人的要求		
设立标准	• 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；	第五十二条
	• 在境外处理境内自然人个人信息的个人信息处理者。	第五十三条
报备要求	• 公开个人信息保护负责人的联系方式，将个人信息保护负责人的姓名、联系方式等报送监管机构。	第五十二条
主要职责	• 对个人信息处理活动以及采取的保护措施等进行监督；	第五十二条
	• 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的，与监管机构沟通。	第六十四条
工作内容	• 根据个人信息的处理目的、处理方式、个人信息的种类以及对个人的影响、可能存在的安全风险等，采取措施；	第五十一条
	• 防止未经授权的访问以及个人信息泄露、篡改；	第五十一条
	• 定期组织对处理个人信息遵守法律、行政法规的情况进行合规审计；	第五十四条
	• 对个人信息处理活动进行个人信息保护影响评估；	第五十五条
	• 对于信息泄露、篡改、丢失采取补救措施，并通知履行个人信息保护职责的部门和个人。	第五十七条

(3) 兼任情况

《个人信息保护法》和《国标》中明确规定对于满足一定条件的企业，应当设立专职人员负责个人信息保护工作。除此之外，我国现阶段没有其他关于上述岗位必须由专职人员担任的规定。

- 在排除法律法规的禁止性规定后，从岗位本身的职责范围判断，笔者认为，“首席数据官”“网络安全负责人”及“网络安全管理机构负责人”（如果某企业同时还是关键信息基础设施运营者的情况下）三个职位基本可以由同一人兼任的，而“个人信息保护负责人”的职责范围相比较之下则更特定更具体，建议有个人信息保护方面实践经验与专业知识的人员担任则会更好，因为在一定程度上可能还有与消费者、监管机构、行业协会的沟通需求。基于企业运营合理性的考虑，在职位委任方面，笔者将针对企业规模与发展阶段的不同情况，给出如下参考性建议：
- 如果企业属于初创类型公司，所涉及的数据量级及业务体量等情况不具备设立个人信息保护负责人条件的，可以由网络安全负责人或者信息安全负责人或者法务负责人兼任。
- 如果企业处理的数据包括重要数据，建议公司按照《数据安全法》要求设置具体的数据安全负责人。如果企业同时还处理个人信息，且处理规模已经符合《个人信息保护法》和《国标》中规定的需要设立个人信息保护负责人的情况，可以由同一人担任数据安全负责人和个人信息保护负责人。但针对网络安全负责人（偏信息安全），仍建议与数据安全负责人/个人信息保护负责人（偏隐私安全）分离设置。当然，如果网络安全负责人同时也兼具个人信息保护知识与经验的，也可以由同一人担任两个角色，并且给予“数据保护官”的专门职务。待企业规模再大时，甚至还可以给该人配置专员，以共同支持网络安全与个人信息保护的全盘工作，或者由其他岗位的同事一起成立个人信息与隐私保护委员会。
- 如果企业涉及的个人信息处理活动频繁且信息量级较大，但企业规模又不足以设立专职的个人信息保护负责人的，建议可以在网络安全负责人下由一名员工专项负责个人信息保护工作，例如：互联网公司、广告公司、大数据企业等。
- 如果企业主要的经营活动基本不涉及个人信息处理相关的工作，更多涉及网络运营维护、网络安全技术等方面的事项，但偶尔也有可能接触到客户或员工的个人信息，可以由一人同时兼任网络安全负责人和个人信息保护负责人。例如：网络技术服务公司等。

针对儿童个人信息保护负责人，笔者认为，如果公司主营产品的直接或间接受众是儿童，且有条件设立儿童个人信息保护专员的，建议除设立个人信息保护负责人外，还应委任专人担任儿童个人信息保护负责人。反之，可以由个人信息保护负责人兼任，因为除了儿童群体特殊，有专门保护要求以外，其保护的主体均是个人信息与隐私安全。如果企业所售产品或者提供服务并非特别针对儿童，覆盖的是全年龄段的用户，则可以直接由个人信息保护负责人来兼任儿童个人信息保护负责人的角色。对于完全不从事收集、存储、使用、转移、披露儿童个人信息等活动的企业，可以不设立此职位。



（二）法律责任

通过上文表格可以看出，现阶段对于企业未设立数据保护岗位负责人有处罚的生效法律依据主要源于《网络安全法》《数据安全法》《儿童个人信息网络保护规定》。

根据《网络安全法》第五十九条，如公司未确定网络安全负责人，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款。关键信息基础设施的运营者未设置专门的安全管理负责人的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款。

而按照《数据安全法》第四十五条，如公司处理数据涉及重要数据，但未明确数据安全负责人，则将由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。

随着《个人信息保护法》的正式出台及实施，对于未设立个人信息保护负责人的企业，将会面临非常严重的处罚后果，对于企业而言，根据《个人信息保护法》第六十六条，个人信息处理者未履行规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。因此，建议企业可以参考《个人信息保护法》以及《国标》中的相关规定，及早设立个人信息保护负责人，以避免在发生数据泄露等事故时，经监管审查发现没有设立个人信息保护负责人，而被依据生效后的《个人信息保护法》进行处罚。

在责任承担的主体方面，鉴于个人信息保护负责人属于在企业内部主持数据安全与个人信息保护工作的人，不能排除其属于“直接负责的主管人员以及其他责任人员”，如因自身工作存在故意或过失，或从事违法行为，有可能需要承担相应的民事、行政甚至刑事责任。《网络安全法》第五十九条、《数据安全法》第四十五条和《个人信息保护法》第六十六条都明确了对于“直接负责的主管人员和其他责任人员”的法律责任。以《个人信息保护法》为例：违反规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

但从笔者对法条及目前执法案例、司法判例的理解，个人信息保护负责人在尽到了合理、谨慎、注意义务且自身不存在任何违法行为，如数据保护岗位负责人尽职尽责，已对所有发现的风险进行了披露并且反复要求企业进行整改，而企业仍然置若罔闻，不予理睬的，那么大多数情况下，个人信息保护负责人不应当再承担法律责任了，但企业自身仍是对外承担安全责任的主体。

（三）实务建议

结合上文对中欧数据保护岗位负责人应当承担的责任义务的分析与对比，下文将对我国企业数据保护岗位负责人如何开展工作及履行职责，提供一些参考性的建议。

对于企业而言，如果企业活动处理个人信息达到国家网信部门规定数量，或本身为境外公司处理境内自然人个人信息，需要按照《个人信息保护法》设立个人信息保护负责人。综合《个人信息保护法》和《国标》要求，个人信息保护负责人的主要作用体现在：

- 统筹监督公司内部个人信息安全工作；
- 制定个人信息保护工作计划、政策、章程并落实；
- 对个人信息保护工作进行评估、扫描风险、危机处理（包括回复数据主体请求）、提供建议，并进行定期审计；
- 实时跟进最新立法，在企业内部展开个人信息安全培训，提升企业整体数据合规意识；
- 与监管机构进行沟通，协调与政府关系。

企业内部数据岗位负责人需要从宏观的全局把握，到**具体实践（风险控制、操作指引和危机处理）**，以及**后端与数据主体和监管机关的沟通**，为企业提供全方位全流程的支持与服务，具体工作建议如下：

（1）基础工作的铺垫

在企业内部的合规工作，首先是让管理层明晰合规工作的重要性。数据保护岗位负责人可以将发生的数据相关案例处罚原因、处罚情况以及后续影响进行汇总并汇报给管理层，这样容易引起重视。其次，建立数据安全保护小组或虚拟委员会。依照目前国内的情况看，除了部分企业设有数据保护专职岗位以外，大多数企业是由信息安全或者法律合规部门来兼顾处理数据合规事务。但是，合规工作不仅仅涉及信息安全或法律问题，还需要考虑产品经营模式、消费者投诉、技术手段等多方面内容。建立数据安全保护小组或虚拟委员会，让不同部门的人更深入了解企业内部各方的工作，有助于协调统一地推进工作。最后，对所做的一切合规工作（如评估报告、内部培训等）都需要有留存记录（即留痕），证明企业为数据合规已经开展了实质性工作，也是日后监管机构来核查时的主要参考依据。

（2）组成机构的职责分配

一般情况下，法律合规部门、数据运营部门、各产品线、运维和IT部门与个人信息安全保护工作最密切相关，因此，可以由其中一个部门的负责人牵头（如果符合条件，亦可被委任为数据保护岗位负责人），从相关部门抽取核心人员（经签署专项保密协议后）共同组建企业个人信息保护工作机构，各司其职，分别负责《国标》要求的各项具体内容。具体说，包括以下几个方面：

由法律合规部负责制定、签发、实施、定期更新用于自检的合规清单（形式可以参考**附件三 App收集使用个人信息企业自评估核对清单**），以及隐私政策和相关规程；组织开展个人信息安全培训；制定应急预案和组织应急演练；对滥用个人信息的投诉、举报进行调查，严厉查处不合规现象和违纪员工，如非授权访问、篡改或删除个人信息，违规使用、滥用信息等；维护企业个人信息保护的联系途径，对个人信息主体提出的疑问或投诉进行解答与处理；对机构内部各部门的执行情况进行审计，包括对隐私政策的落实情况、对安全事件的处置、应急响应和安全能力审计等，如有需要，还应当与相关监管机构保持日常良好的沟通。

由法律合规部牵头，数据运营部门及其他必要部门配合组织开展个人信息保护影响评估，包括个人信息收集和使用的评估，并形成评估报告（每年至少一次）；建立、维护和更新个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；对用户发布的信息进行管理，对特殊信息进行报告。

由产品经理对用户隐私政策结合产品进行发布；对弹窗式等通知以及权限管理等问题进行产品设计；对个人信息主体要求访问、更正、删除、撤销同意等请求进行产品可实现性支持；预设个人信息泄露时的通知机制；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。

由运维部门对个人信息存储及每次流转进行保护影响评估，形成相应的评估报告；制定数据本地化存储的管理制度，梳理与第三方企业的安全保障责任和义务，对日志留存、数据分类、备份和加密等进行管理。

由IT部门负责对企业整体网络环境进行事先评估，制订相关信息安全、网络安全，以及信息、网络的应急管理制度，负责网络的运行管理：安全配置网络参数，严格控制网络用户访问权限，维护网络安全正常运行；监控网络关键设备、网络端口、网络物理线路，防范黑客入侵，及时向个人信息保护工作机构报告安全事件，对有安全隐患、缺陷和漏洞的网络进行及时修补，制定补救机制。

(3) 建设企业数据合规体系

建设完备的数据合规体系是一项大工程，建议国内数据保护岗位负责人重点从以下三个层面开展数据合规或治理工作：第一，梳理数据流转情况。需要清楚、全面地了解企业内部对数据收集、使用、共享、转让、公开披露、存储、删除等环节的现状以及所有配套机制的实施情况，比对相关法律法规及标准后，对不足部分进行改进；第二，完善内部制度规程。主要包括设置访问权限控制机制、建立个人信息保护影响评估制度以及采取技术保护手段等；第三，完善外部文件，包括用户协议、隐私政策以及与第三方签订的合同等。外部文件是外部评估企业合规水平的重要参考依据，最好结合之前对数据流转情况的梳理完成。第四，需要有对危机事件做出迅速反应、评估与决策，安排并分配处理信息安全事件相关人员，对事件采取措施并向监管机构进行报告，与投诉/举报人和媒体进行充分沟通的能力；第五，在合适时机将企业内部合规能力与成绩对外进行展示。

当前，很多企业的业务模式不仅仅局限于国内。因此，在完成上述工作后，数据保护岗位负责人还需要考虑如何在国内与国外不同的监管模式下创设符合公司实际情况的合规路径。数据保护岗位负责人首先需要考虑国内对于数据出境的要求。无论企业进行至少每年一次的自评估还是需要报请相关主管部门组织评估，组织进行安全评估已经成为数据出境的前置程序。数据保护岗位负责人需要对这些程序非常了解或者咨询专业机构的意见。其次，要兼顾目标国家的相关法律要求。如果企业拥有出海业务，数据保护岗位负责人需要知悉并结合各个目标国家的不同隐私保护规定，制定出与出海目标国家相配套的合规方案。具体建议，请参考环球数据合规团队撰写的《数据全球化与隐私保护指引》。最后，从节约成本与提高效率为出发点，根据企业实际情况，是考虑选择创设多法域的不同合规路径，还是采用“统一+特殊”的路径，这些都需要数据保护岗位负责人帮助企业完成选择并拟定有效措施。

需要特别提醒的是，如果企业属于《个人信息保护法》规定的提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当进一步成立主要由外部成员组成的独立机构，对个人信息处理活动进行监督，并定期发布社会责任报告，对于平台内违法违规处理个人信息的用户，应当进行及时评估采取必要措施，包括停止提供服务。根据《关键信息基础设施安全保护条例》，如果公司被认定构成关键信息基础设施运营者，则还应当对网络安全管理机构负责人进行安全背景审查。

【总结】

随着《个人信息保护法》的生效，企业设立个人信息保护负责人已经同GDPR一样成为了法定义务而不是建议性的规定，但无论是GDPR规定的DPO制度，还是我国的网络安全负责人/个人信息保护负责人制度，其角色定位的核心均是提前防治企业运营中可能遇到的安全风险。究其根本，是人们对个人信息保护的逐渐重视与意识的不断提升。数据资产将最终成为企业的核心竞争力，做好数据合规不仅仅对企业自身的业务运营有极大的帮助，在企业进行融资、并购、上市等过程中，已经成为了投资人衡量企业价值的核心要素。企业在保障数据合法合规处理的同时，最好还能够建立起自身的合规文化，将数据保护意识贯彻在日常工作中，并将其形成常态。而这一切工作的开端，大都需要数据保护岗位负责人的牵头、推动并争取到全公司上下各方面的支持与配合。

随着社会数字化和数据资源化的逐步加深，特别是我国有关数据立法的日益完善，个人信息保护负责人在企业中的角色与地位日趋凸显。虽然《个人信息保护法》等法律法规中对于数据保护岗位负责人/个人信息保护负责人的任职资格和独立性并未做明确要求，但是结合《国标》来看，我们仍建议企业在选择合适的数据保护岗位负责人/个人信息保护负责人时还是应当综合考量相关人员的数据处理工作经历和信息保护专业知识，并且无论是从企业内部任命或是从外部选聘，均应为数据保护岗位负责人/个人信息保护负责人提供必要的资源，保障其独立履行职责。



《个人信息保护法》 八步走 落地路径与实务解读

孟洁（环球律师事务所）

薛颖（知名互联网企业隐私合规专家）

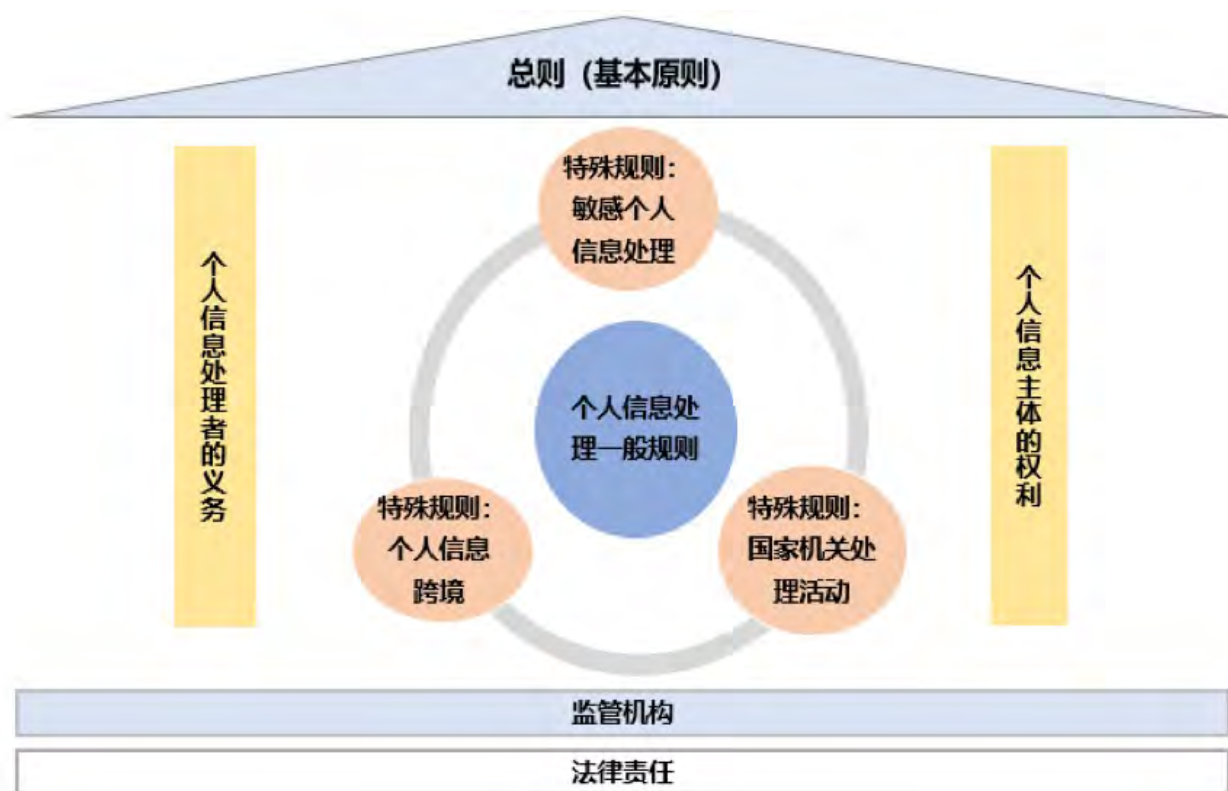
朱玲凤（知名互联网企业隐私合规专家）

* 本文为作者个人观点，不代表所在单位立场



【前言】

2021年8月20日颁布并将于2021年11月1日生效的《中华人民共和国个人信息保护法》（以下简称“《个保法》”）构建出了一套完整的个人信息保护法律架构：



本文旨在向企业提供实务中落地实施《个保法》的工作路径指引，并重点解读相应的条款。

第一步：识别业务活动中所处理的数据是不是《个保法》项下的“个人信息”。

第二步：识别所在企业是属于《个保法》项下的哪一类主体。主体身份不同，对应的义务和责任也不同。

第三步：判断企业处理个人信息的行为是否符合《个保法》的原则和一般规则，即是否遵守无场景差异的、普适性基本要求。

第四步：确保企业遵守《个保法》对于一般处理者的一般义务规定。本文所述的一般义务即无场景差异的义务要求。

第五步：如果企业属于用户数量巨大且复杂的基础性互联网平台（“守门人”），那么不但需要遵守一般处理者的通用义务与规则，还需满足与其自身地位相称的特殊增强性义务。

第六步：无论是一般处理者还是守门人处理者，除了遵守《个保法》下关于其自身的一般性义务规定以外，在某些特定场景或者高风险场景下，还需要履行增强性义务以达到合规。

第七步：确保企业能够实现数据主体对其个人信息处理活动所主张的权利。

第八步：识别企业可能承担的违法后果和举证责任。



一、识别所处理的数据

识别所处理的信息是否属于个人信息是判断《个保法》是否适用的前提要件。根据《个保法》第四条，个人信息是指是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。该定义与《信息安全技术 个人信息安全规范》（2020年版）（以下简称“《个人信息安全规范》”）、《中华人民共和国民法典》（以下简称“《民法典》”）中对个人信息的定义相近。但是其中不同之处是，《个保法》删除了《个人信息安全规范》规定的关联路径。

需要注意的是，《个保法》第七十二条规定，自然人因个人或者家庭事务处理个人信息不适用本法。此条与美国CCPA关于个人信息的定义有非常大的区别。在CCPA的语境下，个人信息既包括与个人相关的设备信息，也包括家庭信息。此外，《个保法》第七十二条还规定“法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定”，所以《个保法》也不适用对上述信息的处理。同时，《个保法》也不适用匿名化处理后的信息。根据《个保法》第七十三条的规定，“匿名化”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。

鉴于敏感个人信息属于个人信息类别中需要重点保护的类别，识别所处理的信息是否属于个人信息后，需要进一步了解有关于敏感个人信息的规定和识别所处理的数据是否属于敏感个人信息。根据《个保法》第二十八条规定，敏感个人信息是指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。

《个保法》第二十八条规定，只有在具有特定的目的和充分必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。除《个保法》将不满十四周岁未成年人的个人信息定义为敏感信息外，《儿童个人信息网络保护规定》将不满十四周岁的未成年人定义为儿童。因此，处理儿童的个人信息既要满足敏感个人信息的规定，也要满足有关儿童个人信息保护的特殊规定。

企业在识别所处理数据涉及敏感信息后，还需进一步判断数据所属敏感个人信息项下的具体类别，例如是否涉及人脸数据等。《个保法》第二十六条对人脸信息进行了专门规定，即在公共场所安装采集人脸图像或用以识别个人身份的设备，只能用于维护公共安全的目的，不得用于其他目的，除非取得个人的单独同意。在2021年7月末最高人民法院制定并公布了《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》（以下简称“《人脸识别规定》”），其中第二条第一款规定了“在宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所违反法律、行政法规的规定使用人脸识别技术进行人脸验证、辨识或者分析的”属于侵害自然人人格权益的行为。对此，企业在宾馆、商场、车站等出于维护公共安全以外的目的使用人脸识别技术收集人脸信息时，应当以显著方式告知收集、使用人脸信息目的、方式、范围。例如，在摄像头安装显著处张贴告知进行提示，“此处摄像头用于人脸识别，以便实现某某目的，我们承诺会保护您的人脸等信息安全，详情可咨询前台或扫描二维码”。另一方面，企业应当单独征得个人信息主体的明示同意，且确保明示同意是其在完全知情的基础上自主作出的。

总而言之，做好合规第一步便是要识别不同的数据类型，然后根据不同的数据类型，严格遵守相应义务。同时《个保法》对个人信息“处理”的概念进行了明确界定，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、删除等。因此，数据处理已经包含整个数据生命周期，所以在实践过程中要避免“数据的收集及处理”等错误表达。与《中华人民共和国数据安全法》（以下简称《数安法》）比较，《个保法》的规定更加详细，其把数据的删除也涵盖在数据处理的定义中。

二、识别处理者的身份

《个保法》对于个人信息处理者进行定义，指的是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。该个人信息处理者的概念可以与《欧盟通用数据保护法》（以下简称“GDPR”）中个人信息控制者的概念相对应。

《个保法》项下大致分为三类处理者，包括一般处理者、守门人处理者以及受托人处理者。

对于一般处理者，又可分为境内和境外的两个场景。

“境内场景”是指在中华人民共和国境内处理自然人个人信息的活动。《个保法》和GDPR对境内一般处理者的规制思路有很大的区别。在境内部分，GDPR遵循属人原则，即欧盟的实体无论处理的是欧盟境内还是境外的个人信息，都要遵守GDPR的规定。《个保法》则遵循属地原则，焦点不在于数据处理者的实体是否是按照中国法律设立，更多关注数据处理者是否在中国境内处理数据。比如有一家在新加坡设立的公司，其数据处理的行为发生在新加坡。根据GDPR的规定，无论其数据处理行为在新加坡还是斯德哥尔摩，均受到GDPR的规制。然而，对于《个保法》的属地逻辑而言，因其数据处理行为发生在境外，则上述数据处理行为不受到《个保法》规制。鉴于此，《个保法》第三条第一款中的“自然人”既包括中华人民共和国境内的自然人也可以包括其他国家的自然人。

与之对应的“境外场景”是指在中华人民共和国境外处理中国境内自然人个人信息的活动，包括以向境内自然人提供产品或者服务为目的；为分析、评估境内自然人的行为以及法律、行政法规规定的其他情形。《个保法》对于境外数据处理行为的规定与GDPR“Target 标准”规制思路相似。对于此条规定，首先需要明确的是，“以向境内自然人提供产品或服务为目的”，如上所述此条的“自然人”包括中国境内的任何自然人，而不仅限于中国公民。同时，“以向境内自然人提供产品或服务为目的”具体指是企业的主观意愿上是为了向境内的自然人提供服务。比如，某公司开发了一款App，其功能主要是为了与支付宝和微信支付相关联，那么可能会推断出该业务是以向中国境内自然人提供服务或产品为目的。其次，境外情景的第二类为“为分析、评估境内自然人的行为”。相比GDPR用于“监控和追踪”的规定，《个保法》更直指问题本质，也与GDPR配套指南中对此条的解释一致。对于数据的监控和追踪只是第一步，法律关注点在于是否进而对上述监控和追责进行了评估与分析的行为。

第二类处理者指“守门人”处理者，即大型互联网平台。被认定为大型互联网平台需要满足三个条件，即提供重要的互联网平台服务、用户数量巨大以及业务类型复杂。

第三类处理者指接受委托处理个人信息的受托人。受托人处理者需要采取必要措施保障所处理的个人信息的安全，同时，受托人处理者也有义务协助个人信息处理者履行法定义务。



三、遵循个人信息处理行为基本原则与一般规则

与《中华人民共和国网络安全法》（以下简称《网安法》）相比，《个保法》的原则体系更为细化和完整。

首先是“合法、正当、必要、诚信”原则。根据《个保法》第五条的规定，处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。该规定相比于《网安法》增加了“负面清单”，即不得通过误导、欺诈、胁迫等方式处理个人信息，这也是当前监管中遇到众多此类“不诚信”处理活动执法经验的体现。

《个保法》第六条规定了“最小必要”原则，即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。收集个人信息，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。对于App运营者而言，建议参考今年3月出台的《常见类型移动互联网应用程序必要个人信息范围规定》（以下简称《必要个人信息范围规定》）进行自查。企业在运营App过程中，应当根据上述规定，明确提供基本功能服务所必须收集的个人信息范围，并与业务部门及时沟通调整实际收集个人信息的范围，以确保符合《个保法》的要求。针对不在《必要个人信息范围规定》39类范围内的其他App以及其他形态的产品（例如网站、PC端等），在收集个人信息时，亦需进行严格评估，避免超出必要范围收集使用个人信息。

《个保法》第七条规定了“公开透明”原则，即处理个人信息应当遵循公开、透明的原则，公开个人信息处理规则，明示处理的目的、方式和范围。次条对产品端隐私政策和各种告知文案的内容提出了原则性要求。

第八条规定了“信息准确”原则，即处理个人信息应当遵循公开、透明的原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第九条规定了“主体责任”原则，即个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。这一原则与后续不同场景下的责任主体识别、举证责任等都一脉相承。

值得注意的是,《个保法》的基本原则不仅为“宣誓性”条款,其规定体现了下位立法、执法和司法的价值导向。与《反不正当竞争法》的“原则条款”类似,《个保法》的基本原则条款还可能会在后续实践中不断适用,以便有效弥补法律在面对纷繁复杂的个人信息处理活动中出现的滞后性、规范的不完全性等问题。

除了“基本原则”外,《个保法》规定的个人信息处理活动一般规则对于所有处理活动场景都普遍适用。一般规则中包含了一些明星条款,也对之前社会各界、执法机构和专业学者关切的问题做出了回应,其中最为核心的处理规则就是“具备合法性事由”+“有效告知”。

《个保法》规定了处理个人信息的七类合法性事由,与《网安法》以及《民法典》相应规定的区别详见下述表格。

合法性基础 (7项)	网安法	民法典	个保法
同意 (普通 + 单独同意)	√	√	√完善
订立或履行个人作为一方当事人的合同所必需; 按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需	×	×	√新增
合理范围内处理个人自行公开或其他已经合法公开的个人信息, 该人明确拒绝或处理会侵害其重大利益的除外	×	√	√
应对突发公共卫生事件或紧急情况下为保护自然人生命健康和财产安全所必需	×	√为公共利益或该自然人合法权益合理实施	√
为公共利益实施新闻报道、舆论监督在合理的范围内处理	×	√	√
履行法定职责或者法定义务	×	×	√新增
法律、行政法规规定的其他情形	×	×	√新增

无论是基于何种合法性事由,数据处理者都要履行告知义务。《个保法》对于告知义务的规定要求非常细致完备,企业要以显著并且清晰易懂的方式将详细信息告知信息主体。比如,《个保法》第三十条和第三十一条规定,处理未成年人个人信息时,既要告知处理敏感个人信息的必要性和对个人的影响,同时需告知未成年人个人信息的处理有专门的处理规则,例如《儿童个人信息保护声明》。在不同场景下,《个保法》还规定了各种细化的告知义务,详情请见下述表格:

告知义务	方式与内容	处理个人信息前以显著方式、清晰易懂的语言告知: 信息处理者的身份和联系方式; 个人信息的处理目的、处理方式、个人信息种类、保存期限; 个人行使权利的方式和程序; 法律法规规定的其他事项
	事项发生变更——变更事项	
	合并/分立——接收方的名称或姓名、联系方式	
	处理敏感信息——必要性及对个人的影响	
	向他人提供——接收方的名称或姓名、联系方式、处理目的、处理方式和个人信息的种类	
告知义务	数据出境——境外接收方的身份、联系方式、目的、方式、种类、行权方式	
	个保负责人——联系方式	
告知义务	告知义务	法律法规规定保密或无需告知; 紧急情况下为保护自然人的生命健康和财产安全无法及时告知

四、识别并遵守一般处理者的一般义务

首先，从顶层设计角度讲，当处理个人信息达到一定数量时，企业需要指定个人信息保护负责人（《个保法》第五十二条）。企业关注的第一个问题是《个保法》下的个人信息保护负责人与《数安法》以及《网安法》下的负责人能否为同一个负责人。第二个问题是，企业设立了数据保护负责人，是否还需要设立数据保护委员会或者专门的部门负责数据保护相关事宜。上述两个问题都没有固定的答案，需要根据企业的实际情况进行判断。同时，对于我国境外的数据处理者，须设立境内专门机构或指定代表（《个保法》第五十二条）。这条规定与GDPR项下当地代表DPO的规定比较类似。

其次，企业需要对于个人信息的全生命周期进行梳理，管理个人信息的流转过程。在此之后，企业应对外声明企业内部是如何实施针对个人信息处理行为的，比如通过发布《隐私政策》和《服务协议》等说明。在此过程中企业需要考虑其业务是否涉及境外部分，如涉及境外的数据处理业务，则企业需要考虑是否需要设计单独的、针对不同司法管辖区域的外部声明还是制定一份统一版本的声明进行集中管理。

第三部分是关于内部制度流程的设计。内部流程制度需要配合处罚措施一起考虑方能比较长效地落地。



第四部分须考虑与第三方的合作设计。根据与第三方合作的关系，需要签署不同类型的委托合同。特别值得注意的是，在采购网络安全产品和服务时，企业不仅要满足《个保法》的要求，也要考虑到《网络安全审查办法》以及《数安法》的相关规定。

第五部分是关于数据安全管控及保障落地的有关规定，特别是关于数据分类分级的规定。与之前《个保法（二审稿）》相比，《个保法》终审稿仅规定了个人信息分类的义务，删除了个人信息分级的义务。同时，《个保法》还规定了加密、去标识化等安全技术措施，明确了数据的保存期限应为实现处理目的所必要的最短时间。

第六部分为风险评估的有关规定（《个保法》第五十五条）。此外，企业内部也要尽到相应的合规审计、记录以及实施应急预案的义务（《个保法》第五十四条以及第五十七条）。《个保法》第五十一条还规定了企业要定期进行安全教育和培训。

此外，当一般处理者作出一些特定行为时，还需要履行的义务详情，请见下述表格：

- | |
|--|
| <ul style="list-style-type: none"> ■ 共同处理个人信息：约定各自权利和义务+对个人权益造成损害，依法承担连带责任。（第20条） ■ 委托处理： <ul style="list-style-type: none"> ——委托方：DPA约定+监督受托人处理活动（第21条） ——受托方：不得超出约定处理；原则上禁止转委托；委托合同不生效、无效、被撤销、终止，将个人信息返还或者删除，不得保留。（第21条） ■ 向第三方提供个人信息： <ul style="list-style-type: none"> ○ 共享——告知详细接收方情况+单独同意；签署DPA，约定处理范围（超出另行同意） ○ 转让/转移（合并、分立、解散、被宣告破产）（第22条） ■ 向公众公开个人信息： <ul style="list-style-type: none"> ○ 已公开：原则上可在合理的范围内处理，除非个人明确拒绝；（第27条） <ul style="list-style-type: none"> 特殊：对个人权益有重大影响的，获取个人单独同意。（第27条） ○ 拟公开：原则上禁止，除非获取单独同意。（第25条） |
| <ul style="list-style-type: none"> ○ 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。（第10条） |



五、识别并遵守守门人处理者的特殊义务

《个保法》第五十八条对提供基础性互联网平台服务、用户数量巨大以及业务类型复杂的个人信息处理者规定了特殊的义务。但是对于上述三个条件的具体指引，还需要等待有关部门做进一步的规定。

针对个人信息处理者中的这类特殊主体，往往掌握大量的用户数据，其合规与否关系到社会公共利益，因此《个保法》提出了四项新的义务要求。守门人处理者的第一项特殊义务是建立健全个人信息保护合规制度体系，从法律义务提出到具体义务的落地，企业需要建构一个层层细化的规定。凡涉及上述处理个人信息环节的部门及员工，均应严格遵守企业内部有关个人信息保护方面的制度流程，提高企业的内部合规水平，同时注意留存记录，以便未来从容应对监管。其次，成立由外部成员组成的独立机构，监督个人信息处理活动。考虑这类主体一般规模庞大，占据了非常大的市场份额，由外部机构，类似于独立董事或者独立审计、律师事务所，来监督个人信息的处理活动，可以更好地督促平台履行合规义务。在处理复杂的业务时，大型的互联网平台也需要外部专家的支持和帮助。

守门人第二个特殊义务是遵守公开、公平、公正原则，制定平台规则，如平台服务协议、交易规则等，明确平台内产品/服务提供者处理个人信息的规范和保护个人信息的义务。例如，网络交易平台内的经营者应当对收集的个人信息严格保密，除依法配合监管执法活动外，未经被收集者授权同意，不得向包括关联方在内的任何第三方提供。

如果发现平台内的经营者等有严重违法违规的情形，大型互联网平台应当停止向其提供服务。

同时，由于互联网平台承载了许多对内和对外的义务，因此其应当定期发布个人信息保护社会责任报告，接受社会监督。责任报告增加了企业的透明度，也增加了个人对企业的信任感。

反观，欧盟没有在2018年公布的GDPR中对守门人处理者进行相关规定，而是在今年另行制定《数字市场法（草案）》（Digital Markets Act），从市场竞争的角度去对超大型平台关于垄断和竞争秩序的问题提出一系列要求，从而进一步保护个人信息。首先，欧盟对守门人的概念进行了相对明确的界定，即公司有一个核心平台，且在欧盟多个国家拥有持久性、庞大用户基础。同时，欧盟也给出了三个推定标准^[1]，除非能证明不具备这三个守门人的门槛性条件，否则将被推定为守门人。我国如果未来把这条落地到实处，后续还是需要出一些可量化的指标，确认什么样的机构应该被纳入守门人的范围。

其次，从守门人义务的规定来看，《个保法》要求成立由外部成员组成独立的监督机构，这点类似于GDPR项下的DPO，因为DPO既可以由公司内部成员构成，也可以委任公司外部人员担任。DPO需要具有相对独立性，比如不能有利益冲突、不能因实施DPO的职责而降薪。但就实践而言，目前仍有不少裁决和判例显示DPO不具有相对的独立性，这也许就是为何《个保法》需要在超大平台的规则上，即使内部已经设立了个人信息保护负责人，还要求有一个外部成员组成的独立机构进行监督的缘由了。

另外就制定公平公开平台规则而言，欧盟《数字市场法（草案）》更多强调的是如何让平台上的相关方，无论是商户还是用户均享受到平台所带来的利益和公平公开的规则，同时强调对平台自身不能过度优待，这其实和国内立法设定的方向和原则是一致的，只是欧盟给出了更多更细致的条款。《个保法》中之所以没有在这个条款中展开细致的规定，而只是作出要求守门人处理者制定公开透明的平台规则，就笔者理解，可能是为了避免在个人信息保护立法里有太多竞争性的条款可能会与原有的立法目标产生一定的冲突。

作为个保法的“明星条款”，“守门人处理者”的相关规定目前还缺少在先立法的支撑，也没有丰富的案例和指引作为参考。因此，期待未来《个保法》细则的出台，特别是对“守门人处理者”的认定条件和标准的规定，将给予企业有针对性的合规参考。

六、识别并遵守特定场景的增强义务

《个保法》还对一些高风险、处理活动复杂、涉及重大权益处理活动的特定场景规定了增强义务。

（一）必须获取“单独同意”的五种场景

当且仅当处理数据的合法性事由是基于同意的时候，有五个场景是需要获得“单独同意”的。这五个场景都是《个保法》下的明星条款。区别于《个保法》项下一般同意规则，个人信息处理者需将以下五种场景下处理目的、行为等单独向个人告知并取得“单独同意”。单独同意仅针对单一事项，不得通过一揽子授权的方式取得数据主体授权同意。《个保法》第二十五条规定，将个人信息予以公开需要获得信息主体单独的同意。前述段落已有参引的《个保法》第二十六条规定，在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，如果用于其他目的就需要取得个人的“单独同意”。就公共场所安装图像采集和个人身份识别设备的行为，GDPR以及EDPB在《关于通过视频设备处理个人数据的指南》中分了两个层次进行规定。首先是图像类的数据，其次是包括可以识别到单独个人的生物识别数据。如果是存储生物识别类数据（脸、声音等），应当适用敏感个人数据收集使用的同意，即获得明确同意。但是欧盟也面临了在公共场合下获得明确同意的困境，因为个人无法清晰的获知是否进入可能产生信息采集的公共区域，这种情况下粘贴公共通知是无法被视为明确告知同意的。所以EDPB提出了一个建议，例如控制者希望使用视频监控的方式对大楼的访问进行管理，首先控制者需要给出人脸识别的替代方案，例如胸卡或者钥匙。其次，控制者需要采取有效的交互方式获得用户的明确同意，例如通过按下按钮触发人脸识别的方式等。

但是，就这两条“单独同意”的适用频率和行业普适性而言，还是比较低的。以下所提到的“单独同意”场景，则是绝大部分企业无法避开且会被经常适用到的场景。

首先，《个保法》第二十三条规定了个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。“向他人提供”的数据离岸行为有多种形式，包括共享、委托处理、转让、转移等。这个时候都需要获取信息主体的单独同意。

其次，《个保法》第三十九条规定了个人信息处理者向境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

另外，《个保法》第二十九条规定处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。当然，某些针对敏感个人信息的处理活动不是基于同意而是基于履行法定义务，例如某些业务场景下需要基于法律法规要求对用户进行强身份认证、履行实名认证义务，在这种情况下处理活动的合法性基础便不再是基于用户同意。

对比GDPR中同意的构成要件，《个保法》对同意的要求为：信息主体自愿作出的、知情的且明确作出的意思表示。但是没有提到关于“具体”的要求。GDPR中作为同意构成要件的“具体”，要求颗粒度更细，要求同意是基于某种特殊目的而作出的，必须跟一个或者多个特定目的的相关，且用户可以对于目的进行选择，防止企业给出一个宽泛的目的范围去获取用户的同意，但实际的处理目的超出用户的预期，造成用户数据滥用。用欧盟目前对于Cookie合规的要求来举例，根据欧盟相关规定，Cookie根据使用目的可以划分为必要类/分析类/营销类等等，每种不同使用目的类型的Cookie都需要获得用户单独的同意。因为GDPR对每一个同意都要求是具体且单独，所以从立法技术上来说不需要对不同的场景做出类似《个保法》单独同意的特殊要求。但综合实践来看，GDPR上述规定无疑给企业以及用户均增加了负担。我国《个保法》在立法过程中考虑到了这个问题，没有将具体且单独的同意要求加至一般同意的规定中，而是对可能对个人产生较大影响的场景才设置了单独同意的要求，即通过一个“即时、单独、充分”的告知，不可捆绑的被授权，且该等同意需要个人主体明示做出。《个保法》与GDPR上述关于“同意”的区别需要我们在实践落地过程中进行关注和区分。

（二）处理敏感个人信息

《个保法》对处理敏感个人信息的特殊要求总结来讲为三句话，即目的限定更严、告知事项更多、同意机制强化（当合法性基础适用“同意”事由时）。

《个保法》规定，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。《个保法》第三十条规定，处理敏感个人信息的，除必须告知的一般事项外，还应当向个人增强告知：处理敏感个人信息的必要性以及对个人权益的影响，除非依法可以不向个人告知。《个保法》第二十九条规定处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

（三）必须进行保护评估的场景

《个保法》对先前审议稿中第五十五条和五十六条的内容做了修改，把“安全评估”的表述替换成了“风险评估”，使得评估范围更加完整和饱满。因为对于个人信息的保护不仅是安全侧的义务，也需要结合对个人信息主体权利行使的保护。对于风险评估事项，企业需要考虑在某项行动前对高风险的事项进行评估。其次，对拟计划出境的个人信息进行评估。

在网络安全审查的适用与启动方面，《网络数据安全条例（征求意见稿）》和最新出台的《网络安全审查办法》作出相应规定：

《个保法》对“高风险场景”进行了兜底性的描述，即对个人权益有重大影响的个人信息处理活动。《个保法》列举了几项属于高风险场景的数据处理活动。但是，需要强调的是，高风险场景并不仅限于《个保法》列举的示例，还应包括其他符合定义的场景。所以，企业首先需要判断自己的数据处理活动是否落入高风险场景范围内。“高风险场景”的适用条件包括敏感个人信息；自动化决策；委托处理、公开；境外提供；兜底以及对个人权益有重大影响的个人信息处理活动。

在确定适用条件之后，我们需了解要具体评估什么内容。首先，要评估处理目的、处理方式是否属于数据处理的一般原则，即合法、正当、必要原则。其次，要评估数据处理活动对个人权益的影响及风险程度。这要根据不同的处理行为做出一个针对性的分级。第三，要评估所采取的安全保护措施是否合法、有效并与风险程度相适应。

最后，即使经过相关决定和平衡后，风险已经被限制在对个人主体影响很小的范围内，企业还需要对整个的风险评估的过程进行报告和记录，并且该记录至少保存三年，这与企业违反法律规定时涉及的举证义务相关，而三年又与诉讼时效有联系。

GDPR有关于DPIA的规定，从适用范围上来讲，比《个保法》适用范围窄。且虽然规定企业有记录义务，却没有像《个保法》一样要求至少三年的保存期限。但GDPR相关规定的参考价值核心在于帮助我们理解个人信息保护影响评估的本质。就笔者个人观点，DPIA强调的是评估过程，属于程序性要求，而非要求达到一个固定标准的实体性要求。就企业而言，它给企业提供了一种合规路径和实现方式，通过DPIA去排查某行为是否符合合规要求，来确定产品或业务是否符合个人信息保护的要求，也是GDPR给予企业证明自身合规性的方法。

（四）自动化决策的场景（明星条款）

我们从两方面去解读《个保法》对自动化决策场景的相关规定。首先，自动化决策不一定直接关联对个人信息的展示或者对个人信息进行触达。企业在进行数据分析和自动化决策后，可能需要进一步开展对个人数据做个性化的推送或者展示，这个行为会对个人信息主体的权益造成影响。“保证处理的透明度和结果公正、公平”与“不得对个人在交易价格等交易条件上实行不合理的差别待遇”两项规定关注点在于处理者对个人信息进行自动化决策后，可能对个人信息主体的权益造成影响的场景。自动化决策的过程要符合对外公示的要求，企业要告知数据主体对其个人信息进行了处理，并保证所处理的结果公平公正，不会对信息主体造成歧视。《国务院反垄断委员会关于平台经济领域的反垄断指南》的相关规定中，也提到了针对“大数据杀熟”问题。部分互联网企业利用大数据分析对不同群体进行差别定价，实行“价格歧视”，对其他数据处理者的商业活动产生影响，从而导致不公平竞争的乱象出现，扰乱了市场秩序。而《个保法》遏制商家对大数据的滥用，主要是为建立健全大数据安全规范使用，提倡算法透明、公平，保护消费者的个人权益。

《个保法》还规定，利用个人信息进行自动化决策而进行信息推送、商业营销的，应同时提供不针对个人特征的选项，或者提供拒绝的方式。但是，仅为通知性的推送不属于该条规定的范围内。《电商法》以及《网络交易监督管理规定》中也对“提供不针对个人特征的选项”进行了规定。相比较而言，《个保法》对此并没有提出很多额外的特殊要求。对于“提供拒绝方式”的这项要求，《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》（以下简称“工信部164号文”）等也对类似的义务做出了规定。

GDPR项下的自动化决策有两种方式，一种是完全基于自动化技术且无人工干预的自动化决策，另外一种是基于用户画像的自动化决策。对于第一种基于自动化技术的决策，比如可以在没有人工干预的情况下，判断哪些人能够面试，哪些人能够简历过筛，哪些人能够享受社会福利。这种自动化决策的防御重点在于人工智能需要为人类服务，而不是因为一些技术而影响人本应该享有的福利，这也是为何起初欧盟禁止自动化决策的原因。

欧盟对于基于用户画像的自动化决策尺度就放松了，与我国的自动化决策保护的立法思路基本一致，强调公平和透明。比如对大数据杀熟的限制，此外是决策需要透明，如果个人对这个处理过程有疑虑，可以要求处理者予以说明。

我们可以从最近意大利数据保护机构对两个外卖软件作出的处罚决定中看出自动化决策对于算法公平性和可适用范围的要求。在这个案例中，意大利执法机关认为，首先，外卖软件可能会对骑手进行特征分析，进而给骑手分配配送订单，但是并未提供关于处理逻辑以及这种处理对骑手的重要性和后果，不满足透明性的要求。其次，在利用自动化决策以及特征分析进行订单分配时没有保障骑手的数据主体权利，至少未获得人为干预和监督的权利，未满足公平和保障用户权利的要求。目前，自动化决策与画像权已经成为了规制算法的主要条款，我们也期待在《个保法》落地过程中，反对自动化决策是否能成为算法规制的核心条款。



（五）数据跨境场景

《个保法》对数据跨境场景的相关规定，需要结合其他法条一起理解，例如《关键信息基础设施安全保护条例》《数安法》以及《网络安全审查办法》等。企业首先需要了解其本身所属的性质以及拟出境的数据是否涉及数据本地化要求。《个保法》第四十条规定关键信息基础设施运营者和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，应当境内存储其处理的数据。对于“规定数量”的具体规定，还有待相关法规进一步给出具体的细化规定。企业还要判断拟出境的个人信息是否构成重要数据。如果构成重要数据，即使一般的网络运营者，也需要遵守重要数据境内存储、业务特需单独审批的要求。另外，根据《个保法》第四十一条规定，境外司法或者执法机构要求提供存储于境内的个人信息的，非经主管机关批准，不得提供。《数安法》有类似规定。

只有在不涉及数据本地化要求的情况下，企业才进一步考虑个人信息出境需要满足哪些具体条件。首先，《个保法》第三十九条规定，向境外提供个人信息的，应当向个人告知并取得个人的单独同意。提前告知并获取同意的义务可以被视为数据出境行为的前置条件。其次，《个保法》第三十八条对确实需要向境外提供个人信息的情况，规定了相应的条件：企业通过国家网信部门组织的安全评估；或者，接受专业机构进行的个人信息保护认证；或者，与境外接收方签订根据国家网信部门制定的标准合同（类似于GDPR下的SCC条款），约定双方的权利义务；以及，提供了符合法律规定的兜底条件以待日后补充。

即使《个保法》明确了个人信息出境的法定要求，但在出境前，企业还需要内部提前实施对拟出境个人信息的自评估，确认其个人信息出境行为具有合法性、正当性和必要性。同时，企业也需要对个人信息接收方的安全保护能力，包括安全措施和法律环境等进行评估。无论是采用网信部门组织的评估还是专业机构认证的模式，网络运营者提供数据接收方相关信息的义务无法避开，包括提供数据接收方对出境后处理个人信息的活动不低于《个保法》保护水平的证明等。另外，企业还有义务确定以及了解接收方是否会将拟出境的个人信息进一步转移，或者存在损毁、乱用、篡改的可能性。虽然《个保法》没有对自评估的具体内容进行规定，但强调了企业需进行履行评估义务的必要性。

最后，在某些特殊情况下，企业可能被考虑列入个人信息一定程度自由流通的范畴，而免受流通限制。如《个保法》第三十八条新增了“中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。”同时，接收方处理中华人民共和国公民个人信息，不得危害国家安全、公共利益。如果接收方确有上述危害国家安全、公共利益的行为，国家网信部门可将其列入限制、禁止提供清单或者采取反制裁的范围。

我们可以从最近意大利数据保护机构对两个外卖软件作出的处罚决定中GDPR项下的跨境传输与《个保法》的跨境传输机制在核心内容上基本保持一致，核心条款是确保数据传输到境外之后，能得到和在境内一样的同等保护水平。除此之外，《个保法》还加上个人信息处理者应当采取必要措施保障同等个人信息保护标准的条款，其实可以视为对于EDPB在Schrems II案件后更新SCC和补充措施指南的回应。跨境传输规定的核心在于达到同等个人信息保护水平，因此《个保法》规定，无论企业选择哪种跨境方式，都需要提供必要的保障措施确保数据安全跨境到第三国家，被传输的数据都能达到跟在国内一样同等的保护水平。GDPR与《个保法》较大的区别在于告知同意的规则，GDPR将同意列为跨境传输的例外条件，如果个人数据主体被明确告知其数据传输无法得到充分保护且可能存在风险，仍明确表示同意这种预期的数据转移，那么企业也可以以此作为数据跨境转移的合法性基础。而在《个保法》中，企业除了满足前述提及的四选一的适用条件以及必要保障措施外，还需要获得信息主体的单独同意，这与境外大多数国家的跨境合法性基础规定不同，需要企业在实践过程中进行重点关注。

七、确保实现个人信息主体权利

个人信息主体拥有的权利一定程序上也对应了企业应当履行的义务。《个保法》第四十四条规定，个人拥有知情权、决定权、限制或拒绝他人对其个人信息进行处理等权利，上述权利对应了企业告知等义务。《个保法》第四十五条规定了个人有权查阅、复制个人信息。《个保法》第四十六条规定了个人享有更正权，即核实后更正和补充的权利。《个保法》第四十八条对自动化决策进行了规定，即个人有权要求企业进行说明实施自动化决策的情况（上文已作介绍）。同时，《个保法》第十六条和第四十五条还分别规定了个人享有撤回同意权和可携带权。可携带权不仅是给予个人信息主体自己查阅复制的权利，个人还可以请求将其个人信息转移至指定的个人信息处理者。同时，符合国家网信部门规定的个人信息处理者还需要提供转移的路径。对于可携带权需要重点考虑的是如何去指定个人信息处理者以及网信部门的规定条件。

《个保法》第四十七条还规定了五种企业应及时删除个人信息的情形：（一）处理目的已实现、无法实现或者为实现处理目的不再必要；（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；（三）个人撤回同意；（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；（五）法律、行政法规规定的其他情形。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

《个保法》第四十九条还对近亲属的相关权利做了相关规定，即自然人死亡的，近亲属为了自身的合法、正当利益，可对死者的相关个人信息行使查阅、复制、更正、删除等权利（除非死者另有安排）。例如，近亲属可以查阅死者生前的银行账户等。《民法典》第九百九十四条也规定了死者的隐私受到侵犯时，其配偶、子女、父母或近亲属有权依法请求行为人承担民事责任。

此外,《人脸识别规定》第十五条亦规定“自然人死亡后,信息处理者违反法律、行政法规的规定或者双方的约定处理人脸信息,死者的近亲属依据民法典第九百九十四条请求信息处理者承担民事责任的,适用本规定”,也为死者近亲属如何保护其自身权益提供了配套规定。即使有上述规定,个保法还特别提到“死者生前另有安排的除外”,所以个人信息主体在生前设立遗嘱时,也可以将个人信息,像房产、车辆、存款、股票、知识产权等一并列入遗嘱。GDPR项下的用户数据权利与《个保法》的规定十分类似,连权利项的规定都是相似的。GDPR分别规定了数据主体行权、访问权、更正权、限制处理权、数据可携带权、反对权、反对自动化决策与画像权以及权利的例外。

这里着重讨论一下**数据可携带权**的内容。《个保法》对数据可携带权的规定与GDPR项下对数据可携带权的规定有所区别。具体来讲,该权利在《个保法》的规定下应为“有限的可携带权。”首先,从结构上来讲,《个保法》对携带权的规定只是比复制和查阅权利多加了一款,而非单独一条。从内容上,《个保法》规定只有在符合网信部门的规定下,才可以实施数据可携带权。为什么《个保法》对数据可携带权的规定仅仅“迈出了一小步”呢?这可能是考虑到GDPR本身对于数据可携带权的规定从2018年产生到现在的实施困境。GDPR对权利的客体做了很明确的范围限定,即针对用户本人的数据。例如,在两个人聊天的过程中,个人只能对自己说的话行使可携带权。数据可携带权是针对数据主体自己提供的数据以及在自动化采集过程中的数据,也就是传统所说的Raw Data,即没有经过处理的数据。信息主体不可以要求企业把经过其智力创造和衍生加工之后的模型数据作为用户行使可携带权的内容。同时,GDPR仅要求提供数据的形式是电子形式的,所以主体不可以要求企业把电子形式的数据以纸质版分享给用户。同时,GDPR中规定了要求履行可携带权的数据需要“结构化、普遍使用和机器可读”的格式,这产生的问题是什么叫做“普遍使用的”。EDPB解释到,“普遍使用”不是要求企业将数据转化成某一种格式使用,而是强调须具有“通用性”。但是现在对此没有明确的标准,即使在诉讼过程中,法院也只是强调了“通用性”和“互操作性”,没有具体解释应该怎么做。由此产生的实施困难是,除了少数大型互联网企业例如谷歌、微软和苹果可以给用户提供一个平台以结构化的方式提供数据,小平台根本没有办法实现该点要求,小平台没有良好的内部数据结构,无法快速地找到用户的数据,并以结构化的方式提供给客户或者第三方。《个保法》对于数据可携带权的规定初衷在于不希望大型平台通过锁定用户的方式影响竞争,但同时考虑到了这项权利如何落地实施存在极大的挑战,所以才对可携带权做了一定的限定,增加了符合国家网信部门规定的个人信息处理者还需要提供转移路径的规定。

“数据可携权”一直到终审稿才进入《个保法》,一经颁布就成为明星条款。虽然该条款是用户“权利”树条款中离实际落地最远的一个,但《个保法》下的“个人主体权利”体系却因此更为完善,在这一方面也得以在全球个人信息保护立法中保持了领先地位。

《个保法》下复杂全面的“个人权利”条款大大弥补了此前我国个人信息保护领域各层级规范性文件 and 执法中的薄弱环节,体现了《个保法》从既往的重视监管“数据处理者”走向兼顾“赋权个人”,立法角度更为全面,也意味着企业的数据合规工作会有更多来自个人信息主体层面的推动力。

八、识别违法后果和承担举证责任

与GDPR的最高处以上一年度营业额百分之四罚款的规定比较,《个保法》将罚款力度增加到上一年度营业额的百分之五。《个保法》对违法后果的规定看似十分严格,但是《个保法》的处罚规则并不是“一揽子”条款。实际上,对于违法行为以及对应的违法后果做了阶梯性的规定。

与《网安法》类似,《个保法》对违法后果的规定采用了“双罚制”的结构。第一,针对违法处理个人信息的数据处理者,除了罚款,还能责令暂停或终止提供服务。第二,对于情节严重的违法行为,除了罚款,还可以一并要求责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。针对直接负责的主管人员和其他直接负责人员,除了罚款以外,还可禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。值得注意的是,《个保法》并没有严格界定什么情况属于“情节严重”,但结合GDPR相关处罚案例来说,数据泄露、受影响的信息主体数量可能成为较大的考虑因素。同时,该条还使用了“拒不改正”这样的表达,因此笔者认为无论在何种情况下,展现出积极的改正态度始终是优解。

随着数据保护合规体系的构建,整体数据监管态势趋于严格。近年来,对于部分重要数据密集且智能化、网联化发展较快的行业,如金融行业和汽车行业,数据安全不仅仅涉及保护企业资产不被篡改、损毁、破坏和个人信息安全,还可能会影响社会安全、国家网络安全,或个人权益造成重大影响。由此,在2021年,这些行业先行发力,数据安全与合规治理已经变成这部分行业的重要命题。

《个保法》第六十七条规定违法行为依照规定记入信用档案。对于侵害个人信息权益的处理活动,适用过错推定原则,即个人信息处理者不能证明自己没有过错的,其应当承担损害赔偿等侵权责任。赔偿额度根据个人受到的损失或者侵害人获取的利益来决定,法院也可能会有此进行调整。

值得注意的是,《最高人民法院关于适用<中华人民共和国民事诉讼法>的解释》第二百八十三条规定,环境保护法、消费者权益保护法等法律规定的机关和有关组织对污染环境、侵害众多消费者合法权益等损害社会公共利益的行为,根据民事诉讼法第五十五条规定提起公益诉讼。《个保法》第七十条规定,对于受到侵害的对象是多人情况,人民检察院、法律规定的消费者组织与国家网信部门确定的组织可以依法向人民法院提起诉讼。“国家网信部门确定的组织”具体包括哪些组织,还需要法规进一步进行解释和说明。《个保法》第七十一条还规定,违反本法规定,构成违反治安管理行为的,依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。

由此能看出,《个保法》对违法后果的规定体现了“多维”以及“阶梯形”的特点。

【总结】

《个保法》在高度关注下诞生，构建中国个人信息保护相关法律规定的顶层设计，完成了里程碑的一步。《个保法》在众多条款中吸收了之前国内个人信息保护的相关实践，给出了相应细致的解决路径，同时针对大数据杀熟、超级平台等给出了现实的回应，《个保法》值得数据合规领域人士细细研读。正如GDPR生效后，EDPB制定了大量的指南解释法律规定以及为企业提供实践指引，我们相信《个保法》未来也会有大量的配套规范性文件，为落地实践提供明确的方案以及解决多个前瞻性条款的具体适用。《个保法》的诞生不是数据合规行业的成熟定型，更应该说将引起新的繁荣发展，证明数据合规行业进入了稳步前进的阶段。

注释：

[1] 守门人推定标准：守门人可基于客户数量、累积活动能力、市场估值等综合标准进行推定，具体应考量如下三个累积条件：

第一，影响内部市场的规模：企业在过去三个财政年度在欧洲经济区（EEA）实现的年营业额等于或超过65亿欧元，或者在上一财政年度其平均市值或等值公平市价至少达650亿欧元，并在至少三个成员国提供核心平台服务；

第二，控制着企业用户通向终端用户的重要门户：如果公司运营的核心服务平台在上一财政年度在欧盟建立或位于欧盟的月活跃终端用户超过4500万，并且在欧盟建立的年活跃商业用户超过1万；

第三，享有或在不久的将来预期享有稳固而持久的地位：企业在过去三个财政年度中的每个年度都符合其他两个标准。

如果上述三个条件均得到满足，则推定该企业为守门人，除非企业提出确凿论据来证明相反的情况。

《重要数据识别指南》新版草案出台， 兼议十二项企业合规义务

环球律师事务所
孟洁 | 王程 | 张淑怡

【前言】

博观而约取，厚积而薄发。在数字化竞争的大背景下，数据已经成为了国家博弈间的重要战略资源，网络安全防护工作也成为了国家安全壁垒的重点要求。2021年9月1日生效的《数据安全法》首先提出了建立国家安全观以及数据安全制度体系，要求国家数据安全工作协调机制统筹协调制定国家重要数据目录，加强对重要数据的保护。随后于2021年11月14日《网络数据安全条例》（以下简称《网络数安条例（征求意见稿）》）公开向社会征求意见，不仅明确了重要数据的定义，还提出了一系列重要数据安全监管制度，因此，“什么是重要数据”以及“如何识别重要数据”便成为了影响当前国家数据安全工作的重大议题。

有鉴于此，国家信息安全标准化委员会于2022年1月13日公布了于最新调整后的《信息安全技术 重要数据识别指南（征求意见稿）》（以下简称《指南》）。《指南》划分了重要数据的定义范围，重要数据是指“以电子方式存在的，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、公共利益的数据”。这既说明了重要数据的存在形式，也明确了以造成不利后果为判断重要数据的唯一标准。并且，《指南》指明识别重要数据的基本原则、明确重要数据的识别因素等，不仅为各行业、地区、部门制定本行业、本地区、本部门的重要数据具体目录提供参考，也为企业识别其自身掌握的重要数据提供实践指引，从而进一步为国家重要数据安全保护工作提供支撑。

一、《指南》修改亮点

相比于2021年9月23日发布的第一版《信息安全技术 重要数据识别指南》（征求意见稿）（以下简称《2021指南》），《指南》是从整体上对《2021指南》进行了重大修订，具体变化体现在如下几点：

1. 改变了体系思路

相较于《2021指南》以及再早之前版本中大篇幅对重要数据采取不穷尽列举的方式，《指南》仅对识别重要数据的基本原则和重要数据的识别因素进行了说明，给企业和各主管机构留有更多权衡和商榷的余地。

《指南》明确指出，从原先对各类别数据具体范围的框定到目前只确定原则性的做法，《指南》所确定的基本原则包括：聚焦安全影响、突出保护重点、衔接既有规定、综合考虑风险、定量定性结合、以及动态识别复评这六大原则。

2. 删除了关键信息基础设施、国家秘密和个人信息的定义

虽然《指南》中仍然有提到关键信息基础设施、国家秘密和个人信息这些术语，但是在术语和定义一节中，《指南》删除了此前版本中针对这些术语的定义，一来是将文件重点放在“重要数据”本身，避免了众多文件对同一概念的反复定义、重点不明等问题。二来，能够比较明确地说明，重要数据不包括国家秘密和个人信息。被删除的定义可以直接参考《中华人民共和国保守国家秘密法》《个人信息保护法》等上位法的相关规定。但是基于海量个人信息所形成的统计类数据（aggregate data）、衍生数据（derived data）是有可能属于重要数据的。

3. 取消了对重要数据的特征进行说明

此前版本中，对重要数据的“特征”说明是文件的一大亮点。《2021指南》从与经济运行相关、与人口与健康相关、与自然资源与环境相关、与科学技术相关、与安全保护相关、与应用服务相关、与政务活动相关、以及其他这八个领域入手，分别介绍了重要数据在该领域下不同角度、不同类别的特征，同时对于各大关键领域下的典型重要数据进行了重点举例说明。如与自然资源与环境相关，涉及地理信息的地图数据、导航数据、特殊测绘数据、重点目标地理信息、未公开的重点目标地理信息等均有可能属于重要数据，并对每类数据进行了解释和说明。

经本次修改，《指南》删除了特定领域的划分和详细的举例说明，改而将所有领域打通，将所有领域对重点数据的识别维度均放在认定因素上，从本质上介绍重要数据的识别因素。在总原则引领下，重要数据识别判断因素主要包括：（1）反映国家战略储备、应急动员能力；（2）支撑关键基础设施运行或重点领域工业生产、运行的数据，关键系统组件、设备供应链数据；（3）反映关键信息基础设施网络安全保护情况，可被利用实施对关键信息基础设施的网络攻击；（4）关系出口管制物项；（5）可能被其他国家或组织利用发起对我国的军事打击；（6）反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可能被恐怖分子、犯罪分子利用实施破坏；（7）可能被利用实施对关键设备、系统组件供应链的破坏，以发起高级持续性威胁等网络攻击；（8）反映群体健康生理状况、族群特征、遗传信息等的基础数据；（9）达到国家有关部门规定的规模或者精度的国家自然资源、环境基础数据；（10）关系科技实力、影响国际竞争力；（11）关系敏感物项生产交易以及重要装备配备、使用，可能被外国政府对我实施制裁；（12）在向政府机关、军工企业及其他敏感重要机构提供服务过程中产生的不宜公开的信息；（13）未公开的政务数据、工作秘密、情报数据和执法司法数据；（14）国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；以及（15）其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。具备以上因素之一的，可能被认定为重要数据。

结合上述识别因素，《指南》对如下相关场景包含的重要数据进行举例：战略物资产能、储备量；反映关键信息基础设施网络安全方案、系统配置信息、核心软硬件设计信息、系统拓扑、应急预案等情况的数据；描述出口管制物项的设计原理、工艺流程、制作方法等的信息以及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告；反映重点安保单位、重要生产企业、国家重要资产（如铁路、输油管道）的施工图、内部结构、安防等情况的数据，以及未公开的专用公路、未公开的机场等的信息；未公开的水情信息、水文观测数据、气象观测数据、环保监测数据；以及描述与国防、国家安全相关的知识产权的数据等等。

同时，《指南》撰写负责人左晓栋院长介绍，在修订《指南》的过程中，标准编制组进一步调研了全球其他国家在网络安全、数据安全领域制定类似标准的情况，选择以美国正在使用的《Guideline for Identifying an Information System as a National Security System》（《国家安全系统识别指南》（NIST 800-59））为参照制定本次《指南》。2003年8月，美国国家标准和技术研究院（NIST）与美国国防部联合制定并颁布了NIST 800-59，提出了判断国家安全系统的方法。NIST 800-59同样从识别的大方向入手，讨论了识别国家安全系统的基础、识别国家安全系统的方法，并提供了国家安全系统识别列表，通过解答问题的方式协助判断某一系统是否符合国家安全系统的定义。

但值得注意的是，从立项之初乃至2020年5月，《指南》的重点编制依据均为美国NIST发布的《将各类信息与信息系统映射到安全类的指南》（SP 800-60）。SP 800-60不仅对信息进行了分类，还分别从信息保密性、完整性、可用性角度为信息标明影响级，分别为低、中、高。这与《2021指南》以及更早期标准的编制思路是一致的——拟以文件形式发布重要数据清单，尽可能做到定性与定量相结合的方式识别重要数据，并重点参考了SP 800-60级别为“中”和“高”的信息。此次《指南》的重大修订（甚至改变了编制依据），体现了我国现阶段引导识别重要数据的整体思路的转变，从定性定量描述转化为了对重点原则的把握。这表明，从一定程度上我国逐渐不再框定、限制重要数据的范围，而是改为从数据自身性质出发，给予主管机构更多裁量认定的空间和灵活性，也符合现阶段社会发展的趋势。

总体来说，虽然此次重大修订后的《指南》难以如此前的版本以“手把手”方式来教企业如何核对自身所涉信息是否为重要数据，但是《指南》为企业的自我评估提供了更加灵活的指引思路和识别路径。这种比较开放式的识别方法，为认定重要数据解开了思维约束，但也带来了一定挑战和不确定性风险。下文我们将结合目前的法律动态和监管趋势，从《指南》的修订点入手，把握重要原则，熟悉识别因素的重要规则，深入分析企业在处理重要数据时应注意的合规义务。

4. 引入了数据分级和数据流动的关联

《指南》提出，在识别重要数据时应遵循的基本原则中，应当突出保护重点。通过对数据分级，可明确安全保护重点，使一般数据充分流动，重要数据在满足安全保护要求的前提下有序流动，释放数据价值。相较于此前版本，《指南》引入了“数据分级”这一制度，与去年九月开始施行的《数据安全法》中国家提出应建立数据分类分级保护制度这一要求前后呼应，顺应政策走向。与此同时，《指南》强调一般数据“充分流动”，相较于《2021指南》中对于一般数据“自由流动”的态度更加突显出了我国鼓励数据流动、开发数据资产价值的趋势要求。

二、处理重要数据企业的合规提示

1. 梳理数据资产，识别重要数据，形成重要数据目录

我国《数据安全法》《网络安全法》《网络数安条例（征求意见稿）》等法律法规均明确提出了重要数据的概念，企业首先需要做的便是对于企业所持有的数据资产进行梳理，参考《指南》所列举的重要数据的识别因素进行判断，明确企业收集的数据的类型，识别数据资产清单中各类数据的用途、面临的主要安全威胁，判断数据安全性（保密性、完整性、可用性等）遭破坏后可能对国家安全、公共利益造成的影响，形成企业的重要数据目录。

同时，《数据安全法》第二十一条明确各地区、各部门制定本地区、本部门的重要数据目录。因此，对于在特定领域的企业，则也可以同步参考本领域内行业主管发布的重要数据识别清单。例如，《汽车数据安全管理办法（试行）》明确在汽车领域下的重要数据清单：

- 军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；
- 车辆流量、物流等反映经济运行情况的数据；
- 汽车充电网的运行数据；
- 包含人脸信息、车牌信息等的车外视频、图像数据；
- 涉及个人信息主体超过10万人的个人信息；
- 国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

工业和信息化部通过《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》从危害所造成影响程度为着眼点，对构成重要数据的范围进行了说明。当数据泄露、损毁、丢失所造成的危害和影响程度符合下列条件之一的为重要数据：

- 对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；
- 对工业、电信行业发展、生产、运行和经济利益等造成影响；
- 造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；
- 引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；
- 恢复数据或消除负面影响所需付出的代价大；
- 经行业监管部门评估确定的其他重要数据。

在识别完企业内部的重要数据后，根据《网络数安条例（征求意见稿）》第二十二条，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，备案内容包括：

- 数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；
- 处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身；
- 国家网信部门和主管、监管部门规定的其他备案内容。

需要注意的是，一旦处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。

此外，当企业处于运营状态时，其所拥有的数据资产是处于流动状态的，而非仅定格在制作数据资产表的那一刻。因此，企业也需要定期对数据资产梳理表进行复盘与更新，以保持数据状态是最新和完整的，并且符合生产运营情况。

2. 明确数据安全负责人和管理机构，完善内部制度体系

根据《数据安全法》第二十七条，处理重要数据的企业应明确数据安全负责人和管理机构，落实数据安全保护责任。根据《网络数安条例（征求意见稿）》第二十八条，对于年度数据安全管理机构，应在数据安全负责人的领导下，履行以下职责：

- 研究提出数据安全相关重大决策建议；
- 制定实施数据安全保护计划和数据安全事件应急预案；
- 开展数据安全风险监测，及时处置数据安全风险和事件；
- 定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；
- 受理、处置数据安全投诉、举报；
- 按照要求及时向网信部门和主管、监管部门报告数据安全情况。

对于数据安全负责人，应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。

同时，企业应以数据为中心，从制度、规范、流程等角度制定数据安全全生命周期的数据安全制度，包括《数据安全组织架构和安全职责》《重要数据采集规范》《重要数据使用规范》《重要数据安全审计》等。

3. 对于重要数据采取分类分级、加密保护

在第一步识别出重要数据的基础上，对于数据库内的重要数据进行打标，并将其根据企业内部的分类分级制度，从数据处理的全流程角度采取更细致化的保护措施，包括针对数据的访问、分发/复制、传输、存储、文件标签、屏幕显示、销毁、备份等环节均加强保障数据安全。同时，根据《网络数安条例（征求意见稿）》第九条，使用不同类型的加密技术对不同程度的重要数据进行保护。

4. 开展网络安全等级保护，使用可信网络产品和服务

根据《网络数安条例（征求意见稿）》第九条，企业应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护要求。同时，企业在采购网络产品和服务时，应当优先采购可信的网络产品和服务，定期检测并维护信息系统安全。

5. 发生重要数据安全事件时的报告

根据《网络数安条例（征求意见稿）》第十一条，当发生重要数据泄露、毁损、丢失等数据安全事件时，企业应当在发生安全事件的八小时内向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等。同时，在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。防患于未然，企业应当提前制定相关的应急预案以及报告流程，以在发生重要数据安全事件时及时尽到报告义务。

6. 共享、交易、委托处理重要数据时审批以及评估要求

当企业共享、交易、委托第三方处理重要数据时，首先，根据《网络数安条例（征求意见稿）》第三十三条规定，应征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。其次，根据《网络数安条例（征求意见稿）》第十一条，企业共享、交易、委托处理重要数据时，一方面，应当开展安全评估，评估的角度包括：提供数据以及数据接收方处理数据的目录、方式、范围等是否合法、正当、必要；重要数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；数据接收方的诚信状况、守法情况、承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全；在数据处理过程中的管理和技术措施等是否能够防范数据泄露、毁损等风险；与数据接收方订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务等内容。评估认为可能危害国家安全、经济发展和公共利益，企业不应共享、交易、委托第三方处理重要数据。

另一方面，应当与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督。

同时，留存共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

若企业受第三方委托、接收第三方共享或交易数据时，应当履行约定的义务，不得超出约定的目的、范围、处理方式处理重要数据。

7. 对企业整体处理活动定期开展风险评估并向监管报告

根据《数据安全法》第三十条，企业应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

在开展评估时，根据《网络数安条例（征求意见稿）》第三十二条，企业可以自行或者委托第三方数据安全服务机构每年开展一次数据安全评估，风险评估报告至少保存三年。同时，企业须在每年1月31日前将上一年度数据安全评估报告报设区的市级网信部门，年度数据安全评估报告的内容包括：

- 处理重要数据的情况；
- 发现的数据安全风险及处置措施；
- 数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性
- 落实国家数据安全法律、行政法规和标准情况；
- 发生的数据安全事件及其处置情况；
- 共享、交易、委托处理、向境外提供重要数据的安全评估情况；
- 数据安全相关的投诉及处理情况；
- 国家网信部门和主管、监管部门明确的其他数据安全情况。

8. 发生合并、重组、分立、解散、破产时的报告义务

根据《网络数安条例（征求意见稿）》第十四条，企业发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据的，应当向设区的市级主管部门报告。

若企业发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。

9. 在重要数据出境前开展评估

（1）出境前的评估与批准

根据《网络数安条例（征求意见稿）》第三十七条的规定，企业应当在出境重要数据前通过国家网信部门组织的数据出境安全评估。在出境时，企业不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供重要数据。同时，企业应采取合同等有效措施监督数据接收方按照双方约定的目的、范围、方式使用数据，履行数据安全保护义务，保证数据安全，接受和处理数据出境所涉及的用户投诉，存留相关日志记录和数据出境审批记录三年以上。

数据出境对个人、组织合法权益或者公共利益造成损害的，企业应当依法承担责任，并配合国家网信部门会同国务院有关部门的核验工作以及责令停止数据出境的行为，采取补救措施。若属于外国司法或者执法机构要求提供数据的情形，则必须经中华人民共和国主管机关批准后方可提供。

(2) 出境后的年度报告

企业若向境外提供重要数据，根据《网络数安条例（征求意见稿）》第四十条，应当在每年1月31日前编制数据出境安全报告，向设区的市级网信部门报告上一年度数据出境情况，内容包括全部数据接收方名称、联系方式；出境数据的类型、数量及目的；数据在境外的存放地点、存储期限、使用范围和方式；涉及向境外提供数据的用户投诉及处理情况；发生的数据安全事件及其处置情况；数据出境后再转移的情况；国家网信部门明确向境外提供数据需要报告的其他事项等内容。

类似的，《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》第二十四条同样强调重要数据出境应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。

10. 若企业有上市计划，则应审慎评估重要数据相关风险

《网络安全审查办法》除关注掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查外，还要求企业重点防控重要数据被窃取、泄露、毁损以及非法利用、非法出境的风险；上市存在重要数据被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险。因此，若企业持有重要数据，则在赴国外上市时需要额外评估重要数据的安全风险以及对国家网络安全的影响，配合国家的网络安全审查。此外，考虑到企业在赴国外上市还会涉及数据出境的情况，因此需要额外关注《数据出境安全评估办法（征求意见稿）》要求所有数据处理者在向境外提供数据前须事先开展数据出境风险自评估。如果出境数据中包括在境内运营过程中收集和产生的重要数据的，则运营者还应通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

同时，根据《网络数安条例（征求意见稿）》第三十二条，企业应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年1月31日前将上一年度数据安全评估报告报设区的市级网信部门。企业应保存该等风险评估报告至少三年。

11. 制定培训计划，定期开展培训

根据《网络数安条例（征求意见稿）》第三十条的规定，企业应当制定数据安全培训计划，每年组织开展全员数据安全教育培训，负责处理重要数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

12. 遵循企业本行业对于重要数据的额外要求

《数据安全法》及其配套规则从普适的角度对于处理重要数据企业的合规义务进行了要求，各行业、各地区同样被赋权针对重要数据出具本行业、本地区的要求，因此，企业同样需要关注本行业、本地区的额外规定。

例如，《汽车数据安全若干规定（试行）》针对汽车数据处理活动所涉及的重要数据进行了规定，额外要求包括：

- 汽车重要数据原则在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估；
- 每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送年度汽车数据安全情况，内容包括：汽车数据安全负责人、用户权益事务联系人的姓名和联系方式、处理汽车数据的种类、规模、目的和必要性、汽车数据的安全防护和管理措施，包括保存地点、期限等内容；
- 向境外提供汽车重要数据的，补充报告接收者的基本情况、出境汽车数据的种类、规模、目的和必要性、汽车数据在境外的保存地点、期限、范围和方式、涉及向境外提供汽车数据的用户投诉和处理情况等内容。

【总结】

悬衡而知平，随着《指南》的修订和完善，我们相信在识别重要数据方面最终将会在顺应世界数据资源竞争趋势的同时，形成具有中国特色的可操性的指南。与此同时，我们建议企业首先应当梳理数据资产，识别并形成重要数据目录，并落实数据安全负责人和管理机构、完善内部制度体系、定期开展培训；其次，企业应当在落实网络等级保护要求的同时，对重要数据进行分类分级和加密保护；再次，当企业发生重要数据安全事件、在处理重要数据、涉及重要数据出境，以及赴国外上市等场景时，应当依法履行不同场景下开展自评估、向监管机构报告、向有关机构申报批准等合规流程；最后，企业还需要时刻关注所处行业和领域的特殊规定及行业标准，以便能够有针对性地及早做好准备。如此以来，企业才能在监管新趋势、新要求下不慌不乱，抓住机遇，迎接挑战。

征信信息已成为保护重点 暨同步解读《征信业务管理办法》

环球律师事务所
张昕 | 孟洁 | 鲁裕鑫



【前言】

随着《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）在2021年8月20日出台并将于2021年11月1日正式生效实施（落地实践推荐，请参阅《〈个人信息保护法〉八步走落地路径与实务解读》），中国人民银行（以下简称“央行”）于2021年9月30日发布了《征信业务管理办法》（以下简称“《办法》”），对于信用信息的范围、采集、整理、保存、加工、对外提供、使用、安全及跨境流动等进行了系统性规定，重点强调了信用信息的安全保护与合规使用，保护信息主体的合法权益。

《办法》对于传统征信行业及在过去几年飞速发展的大数据金融风控行业有着深远的影响。我国征信业正进入快速发展的数字征信时代，征信新业态不断涌现，但由于缺乏明确的征信业务规则，导致征信边界不清，信息主体权益保护措施不到位等问题不断出现。[1]相较于2021年1月11日发布的《征信业务管理办法（征求意见稿）》（以下简称“《征求意见稿》”），《办法》紧扣最新出台的《个人信息保护法》，进一步明确了征信机构和信息提供者的责任义务和信息主体的权利，完善了征信业务中企业/个人信息的处理规则，并对合规整改期限提出的具体要求。

为有效解决上述困境，《办法》不仅对于信用信息和征信业务作出了清晰的界定，还通过明确信用信息全生命周期的要求来更好地保护个人信息主体及企业的合法权益。

一、数字征信时代：数字经济下的必然，征信监管的挑战

（一）互联网大数据征信的发展

在过去短短的近十年中，征信行业发生了飞速的发展，大数据分析能力的进步与普惠金融需求的扩大，催生了一大批类征信金融科技服务企业，提供包括风控、身份验证、反欺诈等在内的一系列产品。

除了技术进步带来的突破性提升以外，大数据征信的发展其实也是市场需求使然。根据央行数据显示，截止2019年底，征信系统收录自然人信息约10.2亿条，收录企业及其他组织信息约2834.1万户。这个数字并未覆盖数字经济下广泛的活跃群体，比如大学生、小微企业主等未曾和传统金融机构发生借贷关系的自然人。而数字征信则利用互联网的优势，涵盖了更多不同场景下采集和积累的用于判断企业和个人信用状况的各类信息，如个人支付、消费相关数据、银行持卡人数据、交通信息、通信信息、互联网金融借贷黑名单信息等等。虽然这些信息相对于传统征信所采集的信息而言与个人信用关联度较弱，但往往金融科技企业通过算法模型的不断创新，由大数据征信产品对传统征信无法覆盖到的大量“白户”进行一定程度的个人信用评分和信用评级，弥补了市场需求中的空白。

除此之外，由于传统央行征信数据应用于金融机构借贷等场景较为有限，互联网业态下类征信产品的广泛应用可以克服前者的局限。除了互联网金融产品外，互联网类征信产品更是应用在如住宿、租车免押金、签证申请等各类场景。《个人信息保护法》与《办法》的出台也正是契合了当前互联网金融各类业务形态蓬勃发展的社会场景，便于运营者及时履行合规义务。

（二）征信行业的监管历史与动态

如前面所述，数字征信的蓬勃发展带来了征信业务边界不清晰和个人信息主体权益保护不到位的问题。针对此，央行及其他国家机关是否有推动征信体系的建设与发展的探索与举措呢？关于征信行业边界及资质要求不清晰的问题，央行已着手建立了国家性的基础数据库，并稳健地推动征信机构的市场化。中国人民银行征信中心（即金融信用信息基础数据库）于2006年正式成立。2013年3月15日施行的《征信业管理条例》（以下简称“《条例》”）中明确了金融信用信息基础数据库的法律地位。同时，《条例》中明确了个人征信机构采取“审批制”，企业征信机构采取“备案制”的监管框架。截至目前，通过人行备案的企业征信机构约为130多家，然而截至目前已经获得牌照的个人征信机构仅为“百行征信有限公司”和“朴道征信有限公司”两家。整体来看，央行对于个人征信机构牌照的发放非常谨慎。

针对个人金融数据的保护，尤其是信用信息的保护问题，近几年来监管机构也积极响应，个人信息保护要求呈现不断提高的整体趋势，行业特定法规、政策和标准也不断出台。截至目前，有关征信行业发展及信用信息保护的主要法规及政策性文件梳理如下：

发布时间	文件名称	发布机关
2005-08-18	《个人信用信息基础数据库管理暂行办法》	中国人民银行
2009-01-24	《征信数据交换格式 信用评级违约率数据采集格式》（JR/T 0042-2009）	中国人民银行、全国金融标准化技术委员会
2010-01-23	《融资性担保公司接入征信系统管理暂行规定》	中国人民银行、中国银行业监督管理委员会
2011-01-07	《关于小额贷款公司接入人民银行征信系统及相关管理工作的通知》	中国人民银行
2012-07-06	《个人信用信息基础数据库数据报送管理规程（暂行）》	中国人民银行
2013-01-21	《征信业管理条例》	国务院
2013-11-15	《征信机构管理办法》	中国人民银行
2014-11-02	《金融信用信息基础数据库用户管理规范》	中国人民银行
2014-11-17	《征信机构信息安全规范》	中国人民银行
2016-09-20	《企业征信机构备案管理办法》	中国人民银行
2016-12-23	《国务院办公厅关于加强个人诚信体系建设的指导意见》	国务院
2017-08-02	《关于加强征信系统查询用户信息管理的通知》	中国人民银行
2018-05-04	《中国人民银行关于进一步加强征信信息安全管理的通知（附：金融信用信息基础数据库接入机构征信合规与信息安全年度考核评级管理办法）	中国人民银行
2018-08-07	《关于加强互联网借贷业务征信合规管理的通知》	中国人民银行重庆营业管理部

特别是在2020年12月25日国务院政策例行吹风会上，中国人民银行副行长陈雨露充分肯定了非借贷类替代数据在征信系统建设中的作用，他表示“人民银行牵头的国家金融信用信息基础数据库，是全球最大的征信系统，同时由市场化的征信机构自主采集企业和个人的征信信息，就是非信贷的征信信息，目前也已经成为我国征信体系的重要组成部分。”^[1]

与此同时，监管机构对于个人征信业务开展的规范化提出了更严格的要求。2020年下半年，人行等多个金融监管部门约谈各大互联网金融平台，提出整改要求。中国人民银行于2020年12月30日对相关个人征信机构开出罚单，没收该征信机构因擅自从事个人征信业务活动获益的1917.55万元，并处罚62万元。在这样征信市场规范化要求日益完善的趋势下，《办法》也应运而生。

二、《征信业务管理办法》要点解读

（一）“征信业务”和“信用信息”的定义

征信业务边界不清晰一直是征信业市场主体的合规难点。什么样的业务算是征信业务呢？相较于《征求意见稿》，《办法》中增加了对征信业务的定义，即“对企业 and 个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。”此外，《办法》在《条例》的基础上，进一步对“信用信息”作出了下述定义。

第三条 本办法所称征信业务，是指对企业 and 个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。

本办法所称信用信息，是指依法采集，为金融等活动提供服务，用于识别判断企业 and 个人信用状况的基本信息、借贷信息、其他相关信息，以及基于前述信息形成的分析评价信息。

《办法》所指的征信业务下所覆盖的信息种类非常广泛，既包括用于识别判断企业 and 个人信用状况的基本信息、借贷信息和需要结合具体业务场景和实际情况进行判断的其他相关信息，还包括“基于前述信息形成的分析评价信息”，一般指金融科技公司基于用户的基本信息与其他信息通过模型计算出的个人信用分，因其属于综合自有或结合第三方个人信用状况信息形成的对信用的评价，也将纳入征信信息的范围。建议相关企业在履行合规义务时，暂且采取较宽范围的判断机制，待相关标准及执法细则进一步明确时再参照调整。

由于替代类数据在征信行业中的作用日显重要，单从数据类型本身出发可能较难判断相应的处理行为是否构成征信业务。根据《办法》第三条的定义，更多是从数据处理活动的目的来判断，如数据处理目的（1）“为金融等活动提供服务”，并且（2）“用于识别判断企业 and 个人信用状况”，尤其是涉及第（2）点时，则很可能与该类数据相关的处理活动都构成征信业务。

值得注意的是，《办法》并未对上述两个目的给予进一步解释与明确。从广义理解，市场上大部分征信类服务都将被包括在内，而从事识别、分析、计算得出个人信用状况、为金融等活动提供服务的相关处理行为的企业，也需获得相应的资质与牌照。此外，《办法》要求个人征信机构应当向中国人民银行报告与其合作的信息提供者。

第十四条 个人征信机构应当将与其合作，进行个人信用信息采集、整理、加工和分析的信息提供者，向中国人民银行报告。

个人征信机构应当规范与信息提供者的合作协议内容。信息提供者应当就个人信用信息处理事项接受个人征信机构的风险评估和中国人民银行的情况核实。

《办法》第五条规定金融机构不得与未取得合法征信业务资质的市场机构开展商业合作获取征信服务，结合上述第十四条，可以体现出对驻贷平台“断直连”的总体要求。大数据公司只有在与持牌征信机构合作的情况下，由持牌征信机构向中国人民银行报告后，方可为金融经济活动提供个人信用信息。然而，具体的合作模式，以及众多大数据公司与数量有限的持牌征信机构合作，是否最终演变成为通过持牌征信机构走一个“通道”，持牌征信机构是否能够真正实现大数据公司所提供的数据服务的有效监督和审查，尚待更深入的探讨，这也有待于监管机构进一步阐释与探索。

参考《办法》第九条和第十条，大数据公司自身，首先应确保其信息来源、信息质量、信息安全、并得到信息主体的授权等。同时需明确与持牌征信机构合作时各自在获得用户同意、信息采集、加工处理、信息更正、异议处理、信息安全等方面的权利义务和责任。大公司在对用户数据进行分析后向征信机构进而向金融机构提供的基础信息、分析数据和判断结果等均需要征得用户的同意。

另值得注意的是，如前所述，对企业和个人信用状况形成的分析评价信息也被定义为“信用信息”，如果将此类产品或者信息（画像、评分、评级）对外实质提供，则也适用本《办法》。在征求意见稿的基础上，《办法》新增的“‘实质’提供”要件，进一步强化和扩大了《办法》的适用范围。因此，大数据公司即使自己未使用“信用信息服务”“信用服务”“信用评分”“信用评级”“信用修复”等名义，但只要对外实质提供以上产品，就应当适用《办法》。

第五十条 以“信用信息服务”“信用服务”“信用评分”“信用评级”“信用修复”等名义对外实质提供征信服务的，适用本办法。

整体来看，企业开展个人征信业务必须事先获得中国人民银行发布的许可牌照。当涉及个人信息处理时，应比照金标委去年发布的《个人金融信息保护技术规范》（JR/T0171-2020）的要求。可以看出，目前监管机关的规制范围不仅仅局限于持牌机构，还涉及金融信息处理的非持牌机构（如从事企业征信业务）也应当予以重视，从事信用评级业务的，还应当依法办理信用评级机构备案。

（二）个人及企业信用信息的跨境传输

作为金融市场一项重要“基础设施”板块，央行近年来不断部署征信行业的对外开放，这对于建立稳定且与全球金融接轨的金融市场而言至关重要。2016年5月，央行与商务部发布联合公告，明确外商投资设立企业征信机构实行国民待遇。根据该公告，设立个人征信业务的外商投资机构应当符合《条例》第六条和《征信机构管理办法》的规定，并需要取得中国人民银行的前置许可。该项工作的开展卓有成效，自2016年以来，已有华夏邓白氏办理企业征信机构、益博睿征信（北京）有限公司和科孚（上海）商务信息服务有限公司三家外资征信机构通过了备案，在中国境内开展企业征信服务。

《办法》在上述对外开放工作的基础上，就跨境征信业务场景提出了数据保护方面的详细要求，主要可总结为三个维度：

1. 本地化存储及备案的要求

《办法》第三十九条明确在中国境内开展征信业务及其相关活动的，采集的企业信用信息和个人信用信息都应当存储在境内，这也呼应了《网络安全法》《数据安全法》和《个人信息保护法》对于关键信息基础设施运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储的法律要求。同时《办法》第四十一条进一步对征信机构与境外征信机构合作的场景作出规定，即需要在合作双方协议签署后、业务开展前由征集机构履行向中国人民银行报告的义务。

第四十一条 征信机构与境外征信机构合作的，应当在合作协议签署后、业务开展前将合作协议报告中国人民银行。

2. 跨境传输个人信息

《办法》第四十条规定，如征信机构向境外提供个人信息，需要符合法律法规的要求。在《个人信息保护法》的框架下，数据跨境传输需要遵守一系列的合规要求，包括数据跨境安全评估（包括个人信息的数量、范围、敏感度、接收方保护水平等）、个人信息主体单独同意、采取“四选一”的保护措施等等。《中国人民银行关于银行金融机构做好个人金融信息保护工作的通知》等法律法规对于某些特定数据类型的跨境传输还作出了限制，甚至禁止出境。这些都是征信机构在进行信用信息跨境传输前应重点考量的因素，同时需要结合具体的业务场景判断适用的法规及合规的出境流程。这对企业自身合规体系的准确性与完备性提出了较高的要求，建议企业尽早采取相应的合规措施。

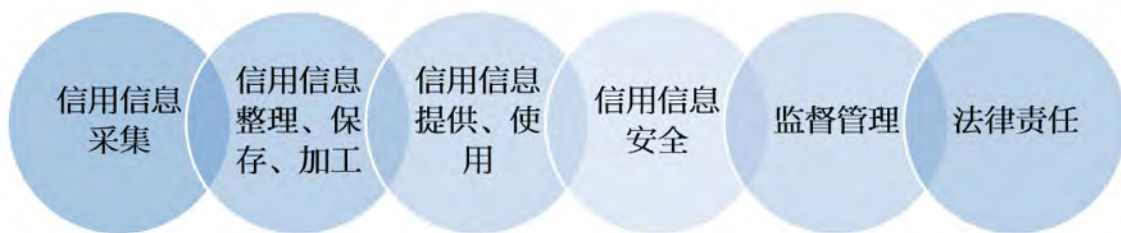
3. 跨境传输企业信用信息

除对个人信息有跨境传输的限制外，《办法》第三十六条还对跨境传输的企业征信信息提出了如下要求：“向境外信息使用者提供企业信用信息查询产品和服务，应当对信息使用者的身份、信用信息用途进行必要的审查，确保该信息用于贸易、投融资等合理用途，且不得危害国家安全”。

以上从一定角度也代表了我国对于数据出境的严格管制标准，建议涉及跨境业务的企业尽早搭建完备且合规的数据出境体系。

三、新规下的征信行业数据保护合规要点提示

《办法》共八章，第一章“总则”和第八章“附则”对于新规的整体适用性、征信行业的原则性要求等作出了整体的规制与明确。其余章节沿袭了目前中国个人信息保护的框架与思路，结合数据生命周期与征信行业的具体业态，对于信用信息的采集，整理、保存、加工、对外提供、使用、信息安全等作出了较为全面的合规要求。整体上与《民法典》《网络安全法》《个人信息保护法》和GB/T35273-2020《信息安全技术 个人信息安全规范》等法律法规和国家标准的规制要求一脉相承。以下，我们将逐一梳理和阐释：



（一）信用信息的采集

《办法》第二章对于个人信用信息和企业信用信息的采集环节作出了明确规定，整体应当采取合法、正当的方式，遵循最小、必要的原则，不得过度采集信用信息。因此，征信机构在采集个人或企业信用信息时应仔细衡量该类信息是否与信用状况的分析与评价有较为直接的关联，是否为实现上述目的所必须，尽量减少不必要的信息采集，同时应结合《条例》第十四条的禁止和限制要求。

1. 征信机构直接采集个人和企业信用信息

《办法》第十二条要求征信机构在直接采集个人信用信息时，应明确告知个人信息主体采集的目的，并在个人信息主体同意后方可采集。《办法》第十五条要求征信机构在直接采集企业信用信息时，应当基于合法的目的，不得侵犯商业秘密，虽然删除了《征求意见稿》中需要取得企业同意的要求，但实际上留给企业通过合同的方式自行约定。

2. 征信机构间接采集信用信息：信息合法性审核及合同约定

当征信机构通过信息提供者间接采集信用信息时，需要制定相关制度，对信息提供者的信息来源、信息质量、信息安全、信息主体授权等进行审核[3]，即根据《办法》第十三条规定，信息提供者是否向信息主体履行其信息将提供给征信机构的告知义务并获取个人主体同意。除此之外，在征信机构与信息提供者所签署的合同中，双方应对信息采集、加工处理、信息更正、异议处理、信息安全等方面明确各自的责任和义务[4]。这两方面的要求整体与一般个人信息保护工作中，通过第三方间接收集个人信息的合规逻辑思路一致。

以上对于征信机构的合规性要求非常高，不仅要自身做到合规以满足监管要求，同时还要对与其合作的信息提供者进行实质性审查和充分的背景调查（类似于传统的供应商尽职调查）以满足自身合规要求，这将最大程度地避免因信息提供者的违规而给征信机构自身带来损害和负面影响。

3. 向中国人民银行报告

个人征信业务机构另外一项需要特别注意的义务是，经营个人征信业务，应当制定个人信用信息的方案，并向中国人民银行报告采集的信用信息类型、信息来源、采集方式、个人信息主体合法权益保护制度等事项及其变化。鉴于目前个人征信机构“审批制”的框架，有意申请个人征信机构牌照的企业应重点关注此项合规义务。

《办法》中将《征求意见稿》的“报备”要求修改为“报告”，一字之差体现出主管机关从“报告备案”到“报告审批”的监管态度转变。

第十一条 征信机构经营个人征信业务，应当制定采集个人信用信息的方案，并就采集的数据项、信息来源、采集方式、信息主体合法权益保护制度等事项及其变化向中国人民银行报告。

（二）信用信息的整理、保存与加工

1. 建立错误更正机制

《办法》第十六至十八条要求征信机构不得篡改原始信息，应当遵循客观性原则，并且采取措施提高征信系统信息的准确性，保障信息质量。如在信息使用的过程中发现错误的，应当及时响应。如该错误的信息由个人信息提供者处采集，则征信机构应及时联系并通知信息提供者更改。如错误信息主要由于内部错误引起，应及时更正并优化信用信息内部处理流程。

2. 存储技术安全及时间要求

《办法》第二十条延续了《条例》对于个人不良信息的保存期限的规定，应当存储至不良行为或事件终止之日起5年，到期后征信机构应当进行删除。如征信机构将其作为样本数据的，应进行匿名化处理。

虽然《办法》删除了《征求意见稿》中对于个人身份标识信息具体的存储策略，即将其与其他信息分开保存，并实行物理隔离，但在个人信息保护要求日益严格的监管情况下，仍建议征信机构应尽力落实该条的要求。

（三）信用信息的提供与使用

《办法》第二十一条首先对信用信息提供、使用作出原则性要求，即遵循公平性原则，不得设置不合理的商业条件限制不同的信息使用者使用，不得利用优势地位提供歧视性或者排他性的产品和服务。而对具体场景的合规要求详细如下：

1. 对信息使用者建立动态审查机制

《办法》第二十二条和第二十三条要求征信机构对于信息使用者进行审查，审查的内容应包括信息使用者的身份、业务资质、使用目的等。同时，征信机构应该采取技术手段，对信息使用者接入征信系统的网络和系统安全、合规性管理措施进行评估与检测，还应当重点对查询行为进行监测，以保障信息使用者查询个人信息时获取了信息主体的同意，且查询手段合法合规。如有违规行为，应停止提供服务。

这同样对征信机构的合规性提出了更高要求。除了要对其信息提供者做到审查之外，对其信息使用者同样需要做到审查（类似于传统的 KYC 义务），尽可能识别信息使用者的真实身份而免遭欺诈，或者避免因提供的信息被滥用或者被用于非法用途，从而给企业或个人信息主体带来负面影响和损失。

2. 提供个人信息主体的查询、异议、投诉的渠道

遵从《个人信息保护法》的框架，即数据处理者应响应个人信息主体请求，提供个人信息副本，《办法》第二十五条规定，个人信息主体有权每年两次免费获取本人的信用报告，征信机构可以通过互联网查询、营业场所查询等多种方式为个人信息主体提供信用报告查询服务。

综合考虑信用信息的特殊性和《个人信息保护法》中规定的信息主体有权请求更正、补充其个人信息，《办法》第二十六条规定，信息主体认为信息存在错误、遗漏的，有权向征信机构或者信息提供者提出异议；认为侵害自身合法权益的，可以向所在地中国人民银行分支机构投诉；进一步明确了信息主体的权利和行权机制。



3. 具体征信服务的细化合规要求

《办法》第二十一条对征信机构对外提供征信产品和服务提出了原则性规定，要求遵循公平性原则，不得设置不合理的商业条件限制不同的信息使用者使用，不得利用优势地位提供歧视性或者排他性的产品和服务。《办法》第二十八至三十条具体列举了征信机构提供的产品，并分别提出了细化的合规要求，特别建议公司注意对用户画像、自动化决策等行为的适用规则：

序号	产品与服务	合规要求
1.	信用信息查询产品和服务	1. 客观展示查询的信用信息内容，并对内容及专业名词进行解释说明； 2. 信息主体有权要求征信机构在信用报告中添加异议标注和声明。
2.	画像、评分、评级等信用评价类产品和服务	1. 建立评价标准，不将与信用无关要素作为评价标准； 2. 正式对外提供信用评价类产品和服务前，应当履行必要的内部测试和评估验证程序，使评价规则可解释、信息来源可追溯； 3. 提供经济主体或者债务融资工具信用评级产品和服务的，应当按照《信用评级业管理暂行办法》（中国人民银行发展改革委财政部证监会令〔2019〕第5号发布）等相关规定开展业务。
3.	信用反欺诈产品和服务	1. 建立反欺诈信用信息的认定标准。

应当向中国人民银行或其省会城市中心支行以上分支机构报告^[5]包括信用报告的模版及内容、信用评价类产品和服务的评价方法、模型、主要维度要素等事项。

以上2、3两项，提供此类产品和服务的企业应尤其注意：在适用本《办法》的上述两项要求时，如果针对个人主体，还必须事先取得个人征信牌照；换言之，需在取得牌照的前提下，满足以上要求。

4. 明确禁止的征信服务/产品与行为

由于信用信息在金融市场及商业活动中有举足轻重的基石作用，信用评价对于个人信息主体的权益可能产生巨大的影响，故《办法》第四章还通过相关条款明令禁止了可能对信息主体权益造成损耗或影响信用评估客观公正性的行为。比如，第二十七条明确征信机构不得以删除不良信息或者以不采集不良信息为由，向信息主体收取费用。除此之外，第三十二条禁止提供包括对信用评价结果进行承诺、对征信产品和服务进行虚假宣传等在内的征信服务和产品。

（四）信用信息安全

征信机构同时应当搭建完善的内控体系，通过采取必要的技术手段及安全管理制度，确保信用信息的安全。除了上文提到的，信用信息跨境传输的保护要求外，征信机构还可着手从以下角度入手，建立一个完善有效的内部信用信息保护体系：

1. 日常运营维护的管理

《办法》第三十五条要求征信机构采取技术与管理双重手段确保征信系统的运行设施设备、安全控制设施设备及互联网应用程序的安全。并且，需要维护征信系统的日常运维管理，保障系统物理安全、通信网络安全、区域边界安全、计算环境安全、管理中心安全。

人员管理

首先，《办法》第三十六条要求征信机构在相关人员的录用、离岗、考核、安全教育、培训和外部人员访问管理等方面做好人员安全管理工作。借鉴搭建企业内部个人信息保护体系的经验与思路，征信机构可通过《员工保密协议》《关键岗位人员保密协议》《离职保密协议》等文件对于员工的安全保密义务作出明确约束，同时积极组织员工进行安全培训与考核，确保制度流程的贯彻与实施。

其次，征信机构应建立《信用信息访问流程与制度》和《外部人员信息访问流程》，对于能够访问信用信息员工的权限和范围作出规定，并准确记录员工查询信用信息的时间、方式、内容、途径等细节。

建立应急处置制度

由于信用信息的高度重要性，征信机构应提前建立内部的《数据安全事件响应策略》，明确处理相应事件的流程，采取必要措施、相关人员的责任义务等。在发生危机事件时，立即采取减损措施，并向中国人民银行及其省会（首府）城市中心支行以上分支机构报告。

额外保护措施

在《征求意见稿》的基础上，《办法》提高了对企业征信机构信用信息安全的监管门槛，从保存或处理50万户以上企业信用信息修改为100万户以上。

个人征信机构、或保存或者处理100万户以上企业的企业征信机构，应满足额外的信用信息保护要求，包括核心业务信息系统网络安全保护等级具备三级或者三级以上安全保护能力；设立信息安全负责人和个人信息保护负责人；设立负责信息安全和个人信息保护工作的专职部门、制定相关制度流程并组织定期检查执行情况等。

（五）监督管理

《办法》的第六章提出了对于征信机构的双重监督模式。除了中国人民银行及其省会（首府）城市中心支行以上分支机构可对征信机构的征信内控制度建设、征信业务合规经营情况、征信系统安全情况等进行检查外，征信机构应向社会公开一系列事项，包括采集的信用信息类别、信用报告的基本格式内容，异议处理流程等，接受社会监督。双重监督模式的建立也大幅提高了征信机构工作的透明度。

针对个人征信机构，《办法》在《征求意见稿》的基础上新增了合规审计要求。个人征信机构应当每年对自身个人征信业务遵守《个人信息保护法》《条例》的情况进行合规审计，并将合规审计报告及时报告中国人民银行。

此外，《办法》还进一步明确信息提供者和信息使用者的监管机构。违反《条例》规定，侵犯信息主体合法权益的，由**中国人民银行及其省会（首府）城市中心支行以上分支机构**依法对其检查和处理。

(六) 法律责任

《办法》在第七章单独规定了违规行为的罚则，并且增加了对直接负责的主管人员的处罚机制。

征信机构违法情形	罚则	
	对单位	对主管人员
擅自从事个人征信业务	由中国人民银行按照《征信业管理条例》第三十六条进行处罚。	
擅自从事企业征信业务	由中国人民银行省会（首府）城市中心支行以上分支机构按照《征信业管理条例》第三十七条进行处罚。	
与未取得合法征信业务资质的市场机构开展商业合作获取征信服务	由中国人民银行及其分支机构责令改正，对单位处3万元以下罚款；	对直接负责的主管人员处1000元以下罚款。
违反《办法》第八条、第十六条、第二十条、第二十七条、第三十二条规定	由中国人民银行及其省会（首府）城市中心支行以上分支机构按照《征信业管理条例》第三十八条进行处罚。	
违反《办法》第十四条、第二十一条、第三十一条、第三十四条、第三十九条、第四十二条规定	由中国人民银行及其省会（首府）城市中心支行以上分支机构责令改正，没收违法所得，对单位处3万元以下罚款；	对直接负责的主管人员处1000元以下罚款。

【总结】

从整体来看，《办法》响应了数字征信时代的潮流，同时也是征信行业规范化发展重要的一步，尤其是对于替代性数据的认可，有助于传统征信行业在数字经济下进行转型，向社会提供更全面准确的信用评估产品和服务。在个人信息保护方面，《办法》整体延续了当前一般行业对个人信息保护的基本要求，要求征信机构重视对征信信息全生命周期范围内的合规保护，落实《个人信息保护法》的合规，并且明确要求企业内部应当制定相应的内部制度，可以看出监管机关监管的重点不再囿限于企业对外展示的内容，而已经逐渐转向了搭建企业内部制度、合规措施、流程等方面。

《办法》在附则中也对从事征信业务机构的合规整改明确提出了具体时间要求，即在《办法》施行（2022年1月1日）前未取得个人征信业务经营许可或者未进行企业征信机构备案但实质从事征信业务的机构，应当自《办法》施行之日起18个月内完成合规整改，否则将承担法律责任。因此，特别提醒相关企业注意尽早开展合规工作。

注释：

[1]国务院政策例行吹风会，<http://www.gov.cn/xinwen/2020zccfh/49/index.htm>。

互联网信息服务管理办法大修 信息安全监管释放趋严信号

环球律师事务所
孟洁 | 董杰睿



【前言】

为了促进互联网信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，国家互联网信息办公室、工业和信息化部、公安部共同起草了《互联网信息服务管理办法（修订草案征求意见稿）》（以下简称“《管理办法（征求意见稿）》”），并于2021年1月8日向社会公开征求意见。

追溯我国对互联网信息服务管理的立法沿革，早在2000年9月25日，我国便首次针对互联网信息服务活动制定了相应的管理办法，即《互联网信息服务管理办法（2000）》（以下简称《管理办法（2000）》）。2011年1月8日，国务院发布了对《管理办法（2000）》的修订（以下简称《管理办法（2011）》），该次修订内容变化不大，仅针对第20条中引用的法规名称作了文字调整，即将《治安管理处罚条例》修改为《治安管理处罚法》。此次《管理办法（征求意见稿）》是对十年前国务院颁布的《管理办法（2011）》的重大修订，也是在2012年向社会征求意见后又一次的公开意见征求，不乏体现了监管机构对与日俱新的互联网信息服务样态，提出更加细化与严格的监管态度。条文数量也比老版本几乎增加了近一倍，由27条增加至54条，内容删改幅度较大。

本文将以分析《管理办法（征求意见稿）》相关条文为基础，提出以下几大主要变化，并通过梳理《管理办法（征求意见稿）》中对企业提出的各项具体义务，形成正副面的合规清单，为企业开展互联网信息服务业务提供合规启示与帮助。



一、确定适用对象

《管理办法（征求意见稿）》第二条，在《管理办法（2011）》的基础上，进一步明确了适用对象的范围，规定主要适用于两类主体：第一类，凡是在中华人民共和国境内的任何组织或者个人，只要向中国境内的用户提供互联网信息服务，无论利用了境内或是境外的网络资源，均属于《管理办法（征求意见稿）》的适用对象。包括**①互联网信息服务提供者、②互联网网络接入服务提供者、③域名注册和解析等互联网服务提供者**，均落入适用对象的范围；第二类，对互联网信息服务进行监督管理的机构。

本文主要针对第一类适用对象展开分析。其中第一类中的**①互联网信息服务提供者**，根据《管理办法（征求意见稿）》的解释，是指为网络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。这些在互联网上常见的信息提供或者服务类型，都属于向用户提供互联网信息服务，并没有特别难理解。而第一类中的**②互联网网络接入服务提供者**，主要包括提供互联网数据中心业务、内容分发网络业务、互联网接入业务等，具体业务形态包括但不限于网络代理、主机托管、空间租用等，因此很多IDC服务商也属于该类互联网信息服务提供者因而适用本办法[1]。由于第一类的**③域名注册和解析等互联网服务提供者**从字面意义上并不难理解，因此不再展开介绍。可见《管理办法（征求意见稿）》的适用对象，几乎涵盖了绝大部分提供互联网服务的境内企业，对相关企业的影晌与意义也非常重大。

二、明确主管部门及其职责

《管理办法（征求意见稿）》第五条、三十条至三十五条详细描述了**国家网信部门、国务院电信主管部门、国务院公安部门以及国务院其他有关部门**的职责范围。据此，上述部门将依次主管互联网信息内容监督、互联网信息服务行业管理、互联网信息安全监管等方面，及时采取执法措施，监测、防范、处置危害国家网络空间安全、侵害公民合法权益的违法犯罪活动，营造清朗的网络空间。

其中，第三十五条还明确规定了上述有关主管部门可以对与涉嫌违法行为有关的电子设备、存储介质、物品、设施、场所采取查封、扣押强制措施，可以查询与涉嫌违法行为有关的银行账户。显然，这赋予了主管部门采取行政强制措施的权力，显示了国家加大执法力度的趋势。

三、细化法律责任

近年来，因违反《管理办法（2011）》而受到处罚的案例不胜枚举。例如，2019年3月，上海某信息科技公司运营的某财经新闻类网站及App在未获得互联网新闻信息服务资质的情况下，违规登载新闻信息，且内容导向存在偏差，扰乱网络信息传播秩序。上海市网信办约谈了该企业的负责人，并责令其全面整改，最终对其作出了行政处罚的决定。

2020年1月，杭州某网络科技有限公司未经许可在其开办的本地头条网站和App中开展互联网新闻信息服务活动，经查后杭州市网信办责令该公司停止相关服务活动，并作出了行政处罚的决定。

《管理办法（征求意见稿）》对互联网信息服务者更是提出了各项新要求（具体参见下文“四、公司合规义务清单”的梳理），希望构建一个更为细致全面的互联网信息服务管理体系。国家网信部门、国务院电信主管部门、国务院公安部门以及国务院其他有关部门联动管理，互联网信息服务业务的设立、运行到监督的每一步，互联网信息服务提供者都需注意符合合规清单所列的相关义务，否则将会承担相应的法律责任。并且，对违规行为的企业可以处以最高100万的行政处罚，对部分违规行为的罚款幅度也由违法所得的3倍以上5倍以下提升到违法所得的5倍以上10倍以下。同时，不仅违规企业会受到处罚，对其直接负责的主管人员和其他直接责任人员也可能受到最高10万元的行政处罚。

此外，国家将设立互联网信息服务信用档案并公布。被有关主管部门吊销许可或取消备案的违规企业，三年内不得重新申请相关许可或备案；被主管部门责令注销账号、关停网站的违规企业，相关互联网服务提供者三年内不得为其重新提供同类服务。这一规定不仅使违规企业需在短时间内承受行政罚款带来的经济负担，还使企业未来三年在互联网信息服务领域的发展受到严重限制，所带来的负面影响极其之大。

相较于此前，《管理办法（征求意见稿）》针对互联网服务提供者的每项义务均规定了相应的法律责任，扩大了互联网服务提供者承担法律责任的范围。同时，《管理办法（征求意见稿）》加大了对违法行为的惩罚力度。由此可见，《管理办法（征求意见稿）》公开后，企业在从事互联网信息服务时，应更加严格地遵守并履行我们以下所列的公司合规义务清单，以避免违规所带来的不利影响和经营风险。

四、公司合规义务清单梳理

“合规清单”具体内容，请见文末附件一。

《网络交易监督管理办法》 压实平台主体责任，企业未来该如何应对？

环球律师事务所
孟洁 | 董杰睿



一、法规出台背景

在3·15之际，国家市场监管总局出台了《网络交易监督管理办法》（以下简称“《管理办法》”），以进一步规范网络交易市场秩序，维护各方主体合法权益，促进网络交易持续健康发展。早在2018年9月，国家市场监管总局网监司便成立起草小组，启动了《管理办法》的制定工作，在经历多次内部研讨会的充分谈论与修改后，形成了此次正式发布的《管理办法》，并将于2021年5月1日正式生效实施。

《管理办法》在原工商总局令第60号《网络交易管理办法》的基础上进行了修订，沿袭了《中华人民共和国电子商务法》（以下简称“《电子商务法》”）的中心主旨，针对经营者市场主体登记、平台责任和义务、各类法定公示义务等问题进行规定，细化补充了《电子商务法》的规定，成为了贯穿落实《电子商务法》的重要部门规章。此外，《管理办法》结合了疫情期间网络交易业态新动向，聚焦“网络社交”、“网络直播”等热点领域，深入研究其他服务提供者的功能角色、新业态新模式下各方参与者责任义务等重点问题。相较《电子商务法》而言，《管理办法》与时俱进地呈现了一套更符合行业发展趋势和业态监管需要的监管规则。

总体而言，《管理办法》在适用性方面更好地与现实情况接轨，对如何解决“过度收集个人信息”、“网购把关不严”、“平台二选一”等热点问题作出了——的指导与回应，并规定了较为严格的处罚措施。故，企业应当严格遵守并履行《管理办法》的规定，以避免违规所带来的不利影响与经营风险。鉴于此，我们将从《管理办法》的适用范围、规定亮点入手，进一步梳理和解读企业在不同场景下的具体合规义务，以更好地帮助企业应对合规风险，助力其在电子经济中进一步创新发展。

二、适用范围

《管理办法》适用于“在中华人民共和国境内，通过互联网等信息网络销售商品或者提供服务的经营活动”。同时，《管理办法》总体上明确了网络交易经营活动的三类主体：

①网络交易经营者，包括网络交易平台经营者、平台内经营者、自建网站经营者和通过其他网络服务开展网络交易活动的网络交易经营者；

②网络服务提供者，指网络社交、网络直播等服务提供者；以及

③其他服务提供者，即为网络交易经营者提供宣传推广、支付结算、物流快递、网络接入、服务器托管、虚拟主机、云服务、网站网页设计制作等服务的经营者。

（二）强化网络交易平台报送信息义务

此前，《电子商务法》第二十八条虽然规定了电子商务平台向市场监督管理部门报送平台内经营者身份信息的义务，但没有提供具体的落地指导，如报送频率、报送信息范围等。而本次《管理办法》则通过第二十二条、第二十五条的内容，分别提出了网络交易平台应当遵守的联系报送义务：

（1）按照国家市场监督管理总局及其授权的省级市场监督管理部门的要求，提供特定时段、特定品类、特定区域的商品或者服务的价格、销量、销售额等数据信息；以及

（2）于每年1月和7月向住所地省级市场监管部门报送平台内经营者身份信息，具体包括：①已办理市场主体登记的平台内经营者的名称（姓名）、统一社会信用代码（注册号）、实际经营地址、联系方式、网店名称及网址链接等信息；以及②未办理市场主体登记的平台内经营者的姓名、身份证件号码、实际经营地址、联系方式、网店名称及网址链接、属于依法无需办理市场主体登记的具体情形的自我声明等信息。其中，对超过年交易10万元额度的个人网店进行特别标示。

（三）强化网络消费者个人保护

当前，数据和流量成为网络市场竞争的关键要素。在网络交易过程中，网络交易经营者往往很容易掌握有大量消费者个人信息，平台乃至较大规模的普通经营者都能通过滥用个人信息不当获利。

但是，《电子商务法》仅概括性地规定了电子商务经营者收集、使用其用户的个人信息的一般性条款，停留在保障用户个人信息的浅层；而《管理办法》通过设置专门的个人信息保护条款，在原基础上新增了多项具体落地要求，具体包括：

（1）不得采用一次概括授权、默认授权、与其他授权捆绑、停止安装使用等方式，强迫或者变相强迫消费者同意收集、使用与经营活动无直接关系的信息；

（2）收集、使用个人生物特征、医疗健康、金融账户、个人行踪等敏感信息的，应当逐项取得消费者同意；以及

（3）网络交易经营者及其工作人员应当对收集的个人信息严格保密，除依法配合监管执法活动外，未经被收集者授权同意，不得向包括关联方在内的任何第三方提供

（四）细化评价删除的处理规定

《管理办法》第十五条规定，消费者评价中包含法律、行政法规、规章禁止发布或者传输的信息的，网络交易经营者可以依法予以技术处理。这一条可视为是对《电子商务法》第三十九条的例外规定，即电子商务平台经营者不得删除消费者对其平台内销售的商品或者提供的服务的评价。

在征求意见阶段，曾有相关专家对此前不得删除评论的规定提出异议，认为其没有考虑到恶意差评以及侮辱有害信息的删除需要。但经过起草小组的进一步调研，发现在实践中平台经营者难以判断用户评论是否恶意或不良；且据统计，平台内经营者因评价不实等原因申请平台经营者予以删除的，最终实际删除的比例不足5%。

因此，《管理办法》在延续了《电子商务法》中“不得删除用户评论”的原则性规定的同时，审慎地进行了细化，规定了平台对消费者评价中包含的法律、行政法规、规章禁止发布或者传输的信息网络交易经营者可以依法予以技术处理的例外情况。这既是通过信用制度对网络交易经营者的一种约束，也体现了对违法信息的打击力度。

（五）严厉惩处平台“二选一”行为

近年来，部分网络交易平台利用平台内经营者对其高度经营依赖性等方面形成的相对优势地位，对平台内经营者和其他平台的合作进行不合理限制的情况（即平台“二选一”问题）不断出现，引发了社会普遍关注。例如，在“双十一”、“618”等电商购物节，商家经常会接到电商平台的通知，要求其仅可在自己的平台内促销商品，这严重限制了平台内经营者自主经营权，也损害了广大消费者的利益。

对此，《管理办法》严格管制网络交易平台不合理限制或附加不合理条件干涉商家自主经营的情形，通过第三十二条的规定，禁止网络交易平台经营者对平台内经营者在平台内的交易、交易价格以及与其他经营者的交易等进行不合理限制或者附加不合理条件，干涉平台内经营者的自主经营。具体而言，包括禁止采取搜索降权、下架商品、限制经营、屏蔽店铺、提高服务收费等方式，限制平台内经营者自主选择在多个平台开展经营活动，或者利用不正当手段限制其仅在特定平台开展经营活动，以及限制平台内经营者自主选择快递物流等交易辅助服务提供者等行为。

此前，市场监管总局网监司负责人回答记者问时提到了，目前实践中平台实施的限制行为隐蔽性强，给监管执法增加了难度。而《管理办法》则是考虑到了这一点，在规制平台“二选一”时，聚焦于平台要求商家“二选一”时常见的具体措施，如搜索降权、下架商品、限制经营等，有的放矢地规制了平台“二选一”的不合理行为。

同时，此前发布的《管理办法》征求意见稿规定了监管部门可对平台限制商家自由经营的行为处以最高三万元的罚款，而正式出台的《管理办法》惩罚力度远高于此。《管理办法》第五十条规定了，网络交易平台经营者违反第三十二条的，将依照《电子商务法》第八十二条的规定进行处罚。《电子商务法》第八十二条的惩罚力度较大，监管部门可对违法平台处以最高二百万元的罚款。不难看出有关监管部门加大规制平台“二选一”行为的趋势，以及解决该问题的决心之坚定。

四、平台/电商合规义务清单梳理

通过分析《管理办法》对网络交易经营者提出的一些新要求，我们不难看出，《管理办法》希望构建一个更为细致全面的网络交易监管体系，从各类网络交易经营者主体入手，着重规定了网络交易平台经营者的义务，同时明确了违法责任与相关的监管机构。作为《电子商务法》的配套实施细则的《管理办法》中的条文规定更加细致，也更具有落地指导性。企业在日常开展业务时，应当同步注意符合以下合规要求，以避免承担违规所带来的法律责任。下文为根据《管理办法》的内容初步梳理的合规清单，以供企业及经营者参考：“合规清单”具体内容，请见文末附件二。



境外上市中的网络安全审查

环球律师事务所
孟洁 | 李来祥 | 殷坤 | 李楠



环球律师事务所
GLOBAL LAW OFFICE

【前言】

2021年12月24日，中国证券监督管理委员会发布《关于就〈国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）〉公开征求意见的通知》[1]，强调境内企业境外发行上市的，应当严格遵守国家法律法规和有关规定，建立健全保密制度，采取必要措施落实保密义务，不得泄露国家秘密，不得损害国家安全和公共利益。境内企业境外发行上市涉及向境外提供个人信息和重要数据的，应当符合国家法律法规和有关规定。经国务院有关主管部门依法审查认定，境外发行上市威胁或危害国家安全的，不得境外发行上市。

2022年1月4日，国家互联网信息办公室等十三部门发布《网络安全审查办法》。相较于2021年7月10日发布的《网络安全审查办法（修订草案征求意见稿）》，《网络安全审查办法》2022年修订版整体调整幅度不大，判断企业是否需要主动申报网络安全审查的实质标准仍为：是否掌握了100万用户个人信息并赴国外上市、是否影响或者可能影响国家安全。我们结合《网络安全审查办法》终审稿，特更新本文（本文初版发表于2021年12月29日）。

一、我国网络安全审查制度的演进

我国网络安全审查制度可追溯至2015年颁布的《中华人民共和国国家安全法》（简称“《国家安全法》”）。其中第五十九条明确，国家建立国家安全审查和监管的制度和机制，**对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。**

全国人大常委会于2016年通过的《中华人民共和国网络安全法》（简称“《网络安全法》”）第三十五条明确，**关键信息基础设施运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。**

2020年4月13日，国家互联网信息办公室（简称“网信办”）与其他11个国务院直属部门共同发布了《网络安全审查办法》，要求关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查，并明确废止了2017年5月2日发布的《网络产品和服务安全审查办法（试行）》（现已失效）。此前《网络产品和服务安全审查办法（试行）》将须进行网络安全审查的对象**仅限于关系国家安全的网络和信息系统的采购的重要网络产品和服务。**

2021年7月2日，网络安全审查办公室发布公告，对某互联网出行平台启动网络安全审查。随后，网信办会同其他六部委联合进驻该平台，开展网络安全审查，以确定其是否符合《国家安全法》《网络安全法》及《网络安全审查办法》。在审查过程中，为配合审查工作，防范风险扩大，该平台被要求暂停新用户注册。同一时期，网信办还启动了对其他三个互联网平台的网络安全审查。

2021年7月10日，网信办发布了《网络安全审查办法（修订草案征求意见稿）》，并向社会公开征求意见（简称“《审查办法修订征求意见稿》”）。《审查办法修订征求意见稿》扩大了网络安全审查的范围，将所有在中国大陆境内收集、产生数据，可能影响国家安全的数据处理者纳入了审查范围，由此明确网络安全审查将同时涵盖网络安全与数据处理活动安全两方面内容。此外，《审查办法修订征求意见稿》第六条规定，掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。进一步明确，对于数据处理者开展数据处理活动，影响或可能影响国家安全的，也应进行网络安全审查。审查内容主要包括两类，一类是针对核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险，另一类则是针对国外上市后关键信息基础设施、核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险。



2021年9月1日生效并实施的《中华人民共和国数据安全法》（简称“《数据安全法》”）承袭了《审查办法修订意见稿》对网络安全审查适用范围进行扩展的思路。《数据安全法》第二十四条规定，“对影响或者可能影响国家安全的**数据处理活动**进行国家安全审查。”因此，网络安全审查对象以生效法律规定得以确认，其不仅针对《网络安全法》下的关键信息基础设施运营者，而是包括关键信息基础设施运营者在内的开展数据处理活动的所有数据处理者。

2021年11月14日，网信办公布《网络数据安全条例（征求意见稿）》（简称“《数安条例意见稿》”），对《网络安全法》《数据安全法》《中华人民共和国个人信息保护法》（简称“《个人信息保护法》”）中关于数据安全的规定提出了细化要求。其中令人关注的条款是第十三条规定的网络安全审查义务。在如下情况下，数据处理者应当申报网络安全审查：

- （1）**汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的；**
- （2）**处理一百万人以上个人信息的数据处理者赴国外上市的；**
- （3）**数据处理者赴香港上市，影响或者可能影响国家安全的；**
- （4）**其他影响或者可能影响国家安全的数据处理活动。**

2022年1月4日，网信办在内的十三部委联合修订了《网络安全审查办法》（简称“《审查办法2022修订》”），该办法自2022年2月15日起施行，并废止了2020年4月13日公布的《网络安全审查办法》。

我们将网络安全审查制度的演进过程制作为如下图示，供读者参阅：



二、对境外上市企业启动网络安全审查的条件

针对境外上市是否涉及网络安全审查,《数安条例意见稿》对此前《审查办法修订意见稿》规定的**审查启动条件**进行了调整和补充,而《审查办法2022修订》基本沿用了《审查办法修订意见稿》的规定,具体比较如下:

《审查办法修订意见稿》	《数安条例意见稿》	《审查办法2022修订》
第二条: 关键信息基础设施运营者采购网络产品和服务,数据处理者(以下称运营者)开展数据处理活动,影响或可能影响国家安全的,应当按照本办法进行网络安全审查。 第六条: 掌握超过100万用户个人信息的运营者赴国外上市,必须向网络安全审查办公室申报网络安全审查。	第十三条: 数据处理者开展以下活动,应当按照国家有关规定,申报网络安全审查: (一) 汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立,影响或者可能影响国家安全的; (二) 处理一百万人以上个人信息的数据处理者赴国外上市的; (三) 数据处理者赴香港上市,影响或者可能影响国家安全的; (四) 其他影响或者可能影响国家安全的数据处理活动。	第二条: 关键信息基础设施运营者采购网络产品和服务, 网络平台运营者开展数据处理活动, 影响或者可能影响国家安全的,应当按照本办法进行网络安全审查。 第五条: 关键信息基础设施运营者采购网络产品和服务的,应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的,应当向网络安全审查办公室申报网络安全审查。 关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。 第七条: 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,必须向网络安全审查办公室申报网络安全审查。

根据《审查办法2022修订》，企业境外上市过程中的网络安全审查启动条件要点如下：

1. 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，必须向网络安全审查办公室申报网络安全审查。

《审查办法2022修订》新增了“网络平台运营者”这一概念，但并未对其进行明确定义，可参考《数安条例意见稿》对于“互联网平台运营者”的定义，“互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者”。假如《数安条例意见稿》最终出台时对现有条款不再调整，那么其所规制的数据处理者范围较《审查办法2022修订》中规定的网络平台运营者实则更大。但从申报条件来说，依然要重点关注“掌握”和“超过100万用户个人信息”这两个标准，对于传统企业，例如钢铁、食品等，在数字经济时代也迈向了数字化平台转型步伐，是否需要申报网络安全审查，依然取决于是否“掌握”及“超过100万用户个人信息”。

2. 《审查办法2022修订》未提及赴香港上市是否承担网络安全审查申报义务，未提及《数安条例意见稿》中赴香港上市的相关要求。

虽然从效力位阶上看，《数安条例意见稿》将由国务院发布，生效后属于行政法规，而《审查办法2022修订》生效后仅为部门规章，但是，从发布时间来看，《审查办法2022修订》现已发布，《数安条例意见稿》的意见反馈截止时间为2021年12月13日，二者均由网信办会同相关部门研究起草。因此，就香港上市是否需要申报网络安全审查的问题，我们认为后续《数安条例意见稿》较大概率会保持和《审查办法2022修订》的统一。根据《审查办法2022修订》，拟香港上市企业（即便掌握超过100万用户个人信息的网络平台运营者）通常并无网络安全审查主动申报义务，但企业仍应排查其是否落入《审查办法2022修订》第二条需要进行网络安全审查的范畴。

3. 《审查办法2022修订》第二条规定，关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。

结合《审查办法2022修订》第十条，评估国家安全风险时，重点考虑如下因素：

（1）如拟上市企业目前未被认定为关键信息基础设施运营者的（简称“非关键信息基础设施运营者”），则应评估：

（i）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及是否因政治、外交、贸易等因素导致供应链可能中断的风险；

（ii）产品和服务提供者遵守中国法律、行政法规、部门规章的情况；（iii）核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险、被国外政府影响、控制、恶意利用的风险等；（iv）其他可能危害网络安全和数据安全的因素等。据此，建议企业赴香港上市前，对网络安全和数据合规情况进行综合评估，并对企业处理数据是否存在影响国家安全的可能性提前进行自评估或者委托专业机构协助评估，综合考虑网络安全的可靠性、所在行业、数据量级、数据敏感程度、是否存在数据出境等情况，尤其重视上市过程中也须同等履行数据安全义务，防止因上市活动可能引发的安全风险。

（2）如拟上市企业已经被主管部门认定为关键信息基础设施运营者的，除上方第（1）点所述内容外，还应评估：

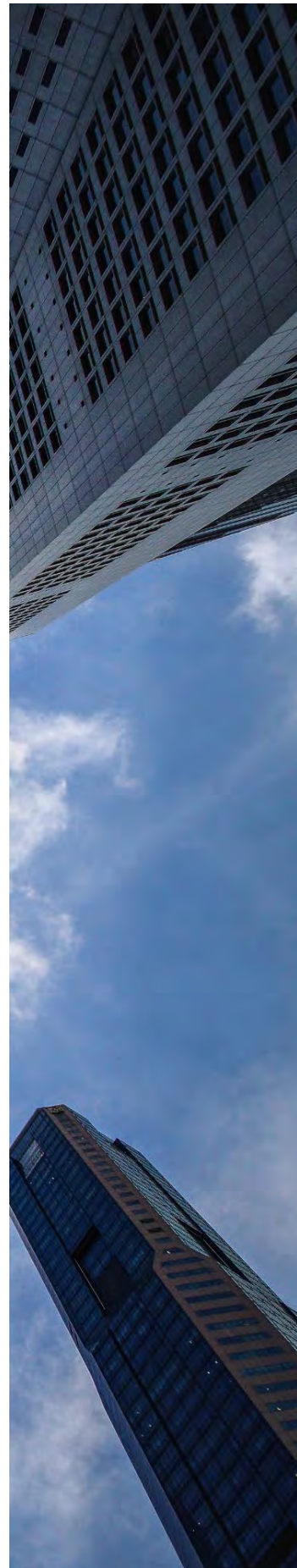
（i）企业所采购的产品和服务在使用后是否会产生关键信息基础设施被非法控制、遭受干扰或者破坏的风险；

（ii）产品和服务供应一旦中断，是否会对关键信息基础设施业务的连续性造成危害；

（iii）上市是否存在关键信息基础设施被国外政府影响、控制、恶意利用的风险，以及网络信息安全风险；

（iv）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

针对“关键信息基础设施运营者”的认定，国务院于2021年7月30日发布的《关键信息基础设施安全保护条例》仅给出原则性指引：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。该条例第九条、第十条进一步规定，由行业主管部门制定具体的认定规则，并对关键信息基础设施进行认定并通知运营者。



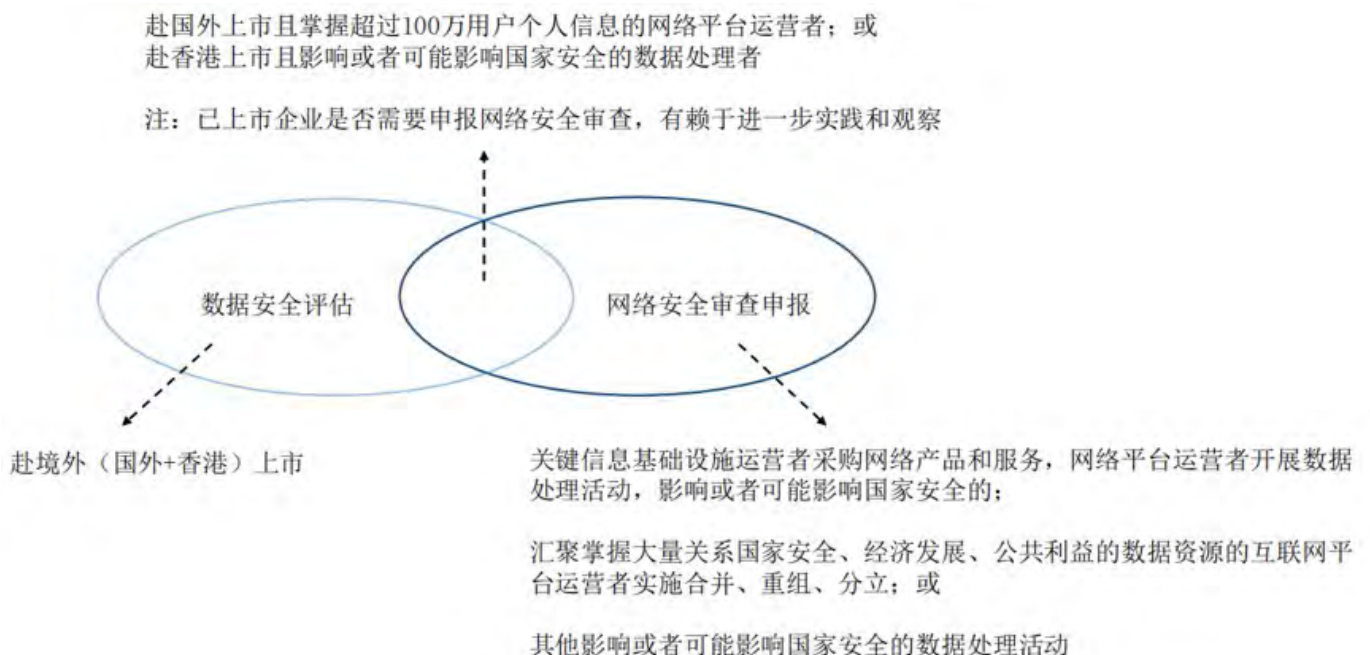
4. 网络安全审查可以由网络安全审查办公室依职权发起。

网络安全审查办公室有权对其认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动开展网络安全审查，网络安全审查办公室将委托中国网络安全审查技术与认证中心承担具体工作，由中国网络安全审查技术与认证中心在网络安全审查办公室的指导下，承担接受申报材料 and 进行形式审查等工作。网络安全审查办公室、网络安全审查工作机制成员单位和/或中央网络安全和信息化委员会依照《审查办法2022修订》的规定进行审查。

5. 数据安全评估义务。

《数安条例意见稿》除了第十三条规定的网络安全审查外，第三十二条还要求，赴境外上市的数据处理者，应当自行或委托第三方每年开展一次数据安全评估，并在每年1月31日将上一年度数据安全评估报告报送设区的市级网信部门。此处《数安条例意见稿》使用“境外”的表达，意味着无论赴国外上市还是赴香港上市，均需要进行数据安全评估。值得注意的是，《审查办法2022修订》增加了第二十二第二款，提出“国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。”这意味着，网络安全审查并不完全等同于数据安全审查。

我们将不同上市场景发行人的网络安全审查义务图示如下：

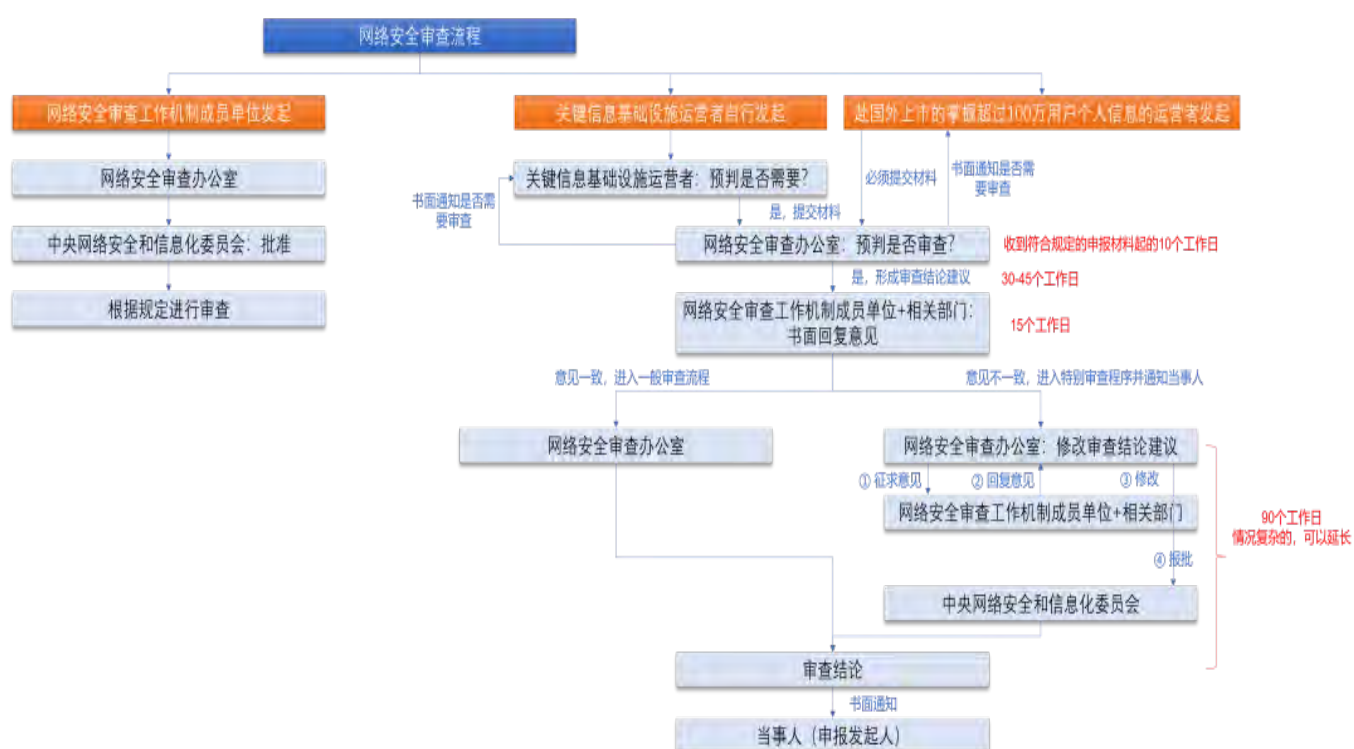


三、网络安全审查流程和时间

网络平台运营者赴国外上市的网络安全审查（如需）的流程如下：

- 网络平台运营者应当在向国外证券监管机构提出上市申请之前，申报网络安全审查。
- 网络安全审查办公室应当自收到符合《审查办法2022修订》第八条规定的审查申报材料起10个工作日内，确定是否需要审查并书面通知当事人。
- 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起30个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长15个工作日。
- 网络安全审查工作机制成员单位和相关部门应当自收到审查结论建议之日起15个工作日内书面回复意见。
- 网络安全审查工作机制成员单位、相关部门意见一致的，网络安全审查办公室以书面形式将审查结论通知当事人；意见不一致的，按照特别审查程序处理。
- 特别审查程序一般应当在90个工作日内完成，情况复杂的可以延长。

具体流程图示如下：



企业申报网络安全审查可能有以下三种情况：一是无需审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。

四、法律后果

对于违反《审查办法2022修订》的行为，《审查办法2022修订》仅规定依照《网络安全法》《数据安全法》的规定处理。相关的法律后果包括：

- 关键信息基础设施运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款（《网络安全法》第六十五条）。
- 关键信息基础设施运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款（《网络安全法》第六十六条）。
- 违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任（《数据安全法》第四十五条第二款）。
- 如应履行而未申报网络安全审查的，《数安条例意见稿》规定的处罚后果是：由有关主管部门对企业处以责令改正、给予警告、罚款、责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处罚款。

《审查办法2022修订》第十六条第二款进一步明确，为防范风险，当事人应当在审查期间按照审查要求采取预防和消减风险的措施。结合2021年7月网络安全审查办公室发起的审查情况来看，预防和消减风险的措施可能包括配合审查进行产品下架、停止新用户注册等。

《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》进一步规定，如企业属于该规定列举的不得境外发行上市的情形（包括经审查境外发行上市威胁或危害国家安全的）进行境外发行上市的，国务院证券监督管理机构、国务院有关主管部门对境内企业给予警告，并处以一百万元以上一千万元以下的罚款，情节严重的，责令暂停相关业务或者停业整顿、吊销相关业务资质许可或者吊销营业执照。对境内企业的控股股东、实际控制人、董事、监事、高级管理人员给予警告，单处或者并处五十万元以上五百万元以下的罚款。

此外，《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》还规定证券公司、律师事务所未严格履行职责、督促企业遵守相关规定的，给予警告，并处以五十万元以上五百万元以下的罚款。对有关责任人员给予警告，并处以二十万元以上二百万元以下的罚款。因此，上市中介机构在就网络安全审查相关问题发表意见时，亦应慎重对待。

五、近期港股上市案例中的相关披露

（一）网易云音乐

《网易云音乐（HK.09899）于2021年12月2日在香港联交所上市，其招股说明书中与网络安全审查有关的披露如下[1]：

“概要” 章节

于2021年7月10日，网信办就《审查办法修订意见稿》公开征求意见，规定关基运营者采购网络产品和服务，数据处理者（连同关基运营者统称“运营者”）开展数据处理活动，影响或可能影响国家安全的，应当进行网络安全审查。根据《审查办法修订意见稿》，掌握超过一百万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。然而，《审查办法修订意见稿》并无就“国外上市”提供进一步解释或诠释。截至最后实际可行日期，《审查办法修订意见稿》尚未正式施行。根据现有中国网络安全法律，关基运营者拟采购网络产品和服务，可能影响国家安全的，应当进行网络安全审查。如我们的中国法律顾问告知，在《审查办法修订意见稿》下，“关基运营者”的实际范畴及现有监管机制尚未明确，而中国政府机关对诠释及执行该等法律可能具广泛的自由裁量权。截至本文件日期，我们并无涉及网信办就网络安全审查作出的任何调查，而我们亦无就此方面接获任何询问、通知、警告或制裁。

2021年11月14日，网信办就《数安条例意见稿》公开征求意见。根据《数安条例意见稿》，数据处理者如进行以下活动：（1）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的；（2）处理一百万人以上个人信息的数据处理者赴国外上市的；（3）数据处理者赴香港上市，影响或者可能影响国家安全的；（4）其他影响或者可能影响国家安全的的数据处理活动，应当按照国家有关规定，申报网络安全审查。然而，《数安条例意见稿》并无就“影响或可能影响国家安全”提供进一步解释或诠释。如我们的中国法律顾问所告知，中国政府机关对于“影响或可能影响国家安全”的诠释可能具有广泛的自由裁量权。

假设《审查办法修订意见稿》及《数安条例意见稿》未来以目前的形式生效，视乎《审查办法修订意见稿》及《数安条例意见稿》的进一步实施详情、指引及澄清，我们及中国法律顾问认为将不会对我们截至本文件日期在任何重大方面遵守法律法规或上市构成重大不利影响，原因是（i）如“业务 - 数据安全”所披露，我们已实施措施，以确保安全存储和传送数据，以及防止任何未经授权取得或使用数据；（ii）截至本文件日期，我们并无遭受任何政府机关处以有关违反数据安全法律法规的重大罚款或行政处罚；（iii）截至本文件日期，我们概无将对业务运营有重大不利影响的数据或个人信息重大泄漏或对数据保护和隐私法律法规的违反；（iv）我们已在采取措施准备遵守《数安条例意见稿》的规定；及（v）我们将继续关注中国数据安全法规的发展。倘《审查办法修订意见稿》及《数安条例意见稿》生效，我们将向相关监管机构寻求指引，以确保我们采取的措施属适当。然而，本公司中国法律顾问不排除未来颁布的新规则或法规将对本集团造成额外合规要求的可能性。

“风险因素” 章节

全国人大常委会于2021年6月10日发布《数据安全法》，规范中国的数据处理活动和安全监管，该法已于2021年9月1日生效。根据《数据安全法》，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。于2021年7月10日，网信办就《审查办法修订意见稿》公开征求意见，该草案规定运营者开展数据处理活动，影响或可能影响国家安全的，应当进行网络安全审查。根据《审查办法修订意见稿》，掌握超过1百万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。此外，于2021年11月14日，网信办就《数安条例意见稿》公开征求意见，当中要求数据处理者于其日常营运遵守若干规定，并进一步列明若干情况下数据处理者应申报网络安全审查，包括数据处理者赴香港上市，影响或者可能影响国家安全的。然而，《审查办法修订意见稿》及《数安条例意见稿》均未就“国外上市”或“影响或可能影响国家安全”提供任何进一步解释或诠释。截至最后实际可行日期，《审查办法修订意见稿》及《数安条例意见稿》均未正式通过。我们无法保证我们在日后的融资活动中会否受

根据上述披露，网易云音乐未进行网络安全审查，其主张的理由如下：一方面，现行有效的《网络安全法》中对于“关键信息基础设施运营者”认定不明；另一方面，因《审查办法修订意见稿》与《数安条例意见稿》暂未生效，即使其按照现行版本生效，鉴于其对“国外上市”与“影响或可能影响国家安全”的定义不明晰，具体影响暂未可知。



（二）商汤科技

商汤科技（HK.00020）于2021年12月30日在香港联交所上市[2]，其招股说明书[3]中与网络安全审查有关的披露如下：

“概要” 章节	于最近中国政府机构已颁布（其中包括）《个人信息保护法》及《数据安全法》，以确保网络安全、数据及个人信息保护，表明随着相关监督管理力度不断加大，规管该等领域的相关法律及法规亦在不断完善。具体而言，网信办已提出《审查办法修订意见稿》及《数安条例意见稿》，征求公众意见，当中对潜在网络安全审查范围提出指引……我们及我们的中国法律顾问认为，假设管理条例草案及修订草案以其当前形式生效，其不会对我们的业务经营、全球发售或上市产生重大不利影响，理由如下 （i）如“业务—数据隐私及个人信息保护”所披露，我们已经实施全面措施以确保持续遵守相关法律法规；（ii）截至本招股章程日期，我们并未就数据及网络安全受到任何政府机构实施重大罚款、强制整改或其他处罚；（iii）截至本招股章程日期，不存在任何由主管政府部门或第三方针对本集团提起的未决的或可能提起将对我们的业务营运产生重大不利影响的数据或个人信息泄露、违反数据保护和隐私法律法规的重大事件、或者调查或其他法律程序；及（iv）我们将继续密切关注数据安全方面的法律法规及监管发展，并遵守最新的监管规定。本公司中国法律顾问不排除未来颁布的新规则或法规将对本集团造成额外合规要求的可能性。
“风险因素” 章节	于2021年7月10日，网信办颁布《审查办法修订意见稿》，进一步重申和扩大了网络安全审查的适用范围。根据办法草案，拟采购网络产品和服务的关基运营者及数据处理者（统称“运营者”）从事影响或可能影响国家安全的数据处理活动的，应当接受网络安全审查。办法草案进一步规定，倘若运营者掌握100万以上用户的个人信息并拟“国外”上市，则其必须进行网络安全审查。 然而，办法草案并未对“国外”上市规定进一步解释或阐释。诚如我们的中国法律顾问所告知，办法草案中掌握有100万以上个人用户信息的运营者赴国外上市申请网络安全审查的要求在当前形式下不适用于我们，主要乃由于（i）截至本招股章程日期，本集团尚未从适用中国政府当局收到任何通知或决定，将其确定为关基运营者，（ii）办法草案下的“数据处理者”的确切范围尚不明确，（iii）本集团正在申请于香港上市，而香港不属于“国外”的范围。于2021年11月14日，网信办发布了《数安条例意见稿》，重申了数据处理者应当申请网络安全审查的情形，其中包括（i）处理一百万人以上个人信息的数据处理者申请赴“国外”上市的；及（ii）数据处理者赴香港上市，影响或者可能影响国家安全的。然而，对于如何确定什么构成“影响国家安全”，其并无提供进一步的说明或解释，我们是否会根据该办法草案就全球发售接受网络安全审查仍存在不确定性。截至最后实际可行日期，上述两项办法草案尚未获正式通过。截至本招股章程日期，我们尚未收到适用政府当局有关国家安全的任何调查、通知、警告或制裁。本集团亦确认，截至本招股章程日期，我们并无涉及网信办基于国家安全或其他任何理由进行的有关网络安全审查的调查，且并未就此收到任何询问、通知、警告或制裁。此外，执行条款和预期采纳或生效日期可能会发生很大的不确定性变化。在现阶段，我们无法预测该等办法草案的影响（如有），且我们将密切监测和评价规则制定过程中的任何进展。因此，尚不确定拟议草案是否适用于我们的业务、全球发售，或者未来的监管变化是否会对我们这样的公司施加额外限制。鉴于上述不确定性，截至本招股章程日期，我们尚未申请有关网络安全审查。

基于商汤科技于招股说明书中的披露，其暂未根据《审查办法修订意见稿》或《数安条例意见稿》向监管部门申请网络安全审查。其主张的理由如下：商汤科技未被认定为关键信息基础设施运营者；商汤科技赴港上市不属于国外上市；现阶段《审查办法修订意见稿》与《数安条例意见稿》仍未生效，即使其按照现行版本生效，“数据处理者”、“国家安全”的定义未明确，因此商汤科技认为其被要求进行网络安全审查的可能性较低。

虽然上述两家公司于香港上市时，《审查办法2022修订》尚未颁布，但鉴于《审查办法2022修订》未对《审查办法修订意见稿》中需进行网络安全审查主体的判断标准作出实质性更改，因此以上两个案例仍具有一定的参考意义。

六、可借鉴的应对思路

基于《审查办法2022修订》的规定，结合过往案例中发行人于招股说明书中的披露，在香港联交所上市的发行人在招股书中的披露可以采纳以下思路：

- 发行人应判断其是否属于网络平台运营者，或是否已经被监管部门确认并通知为“关键信息基础设施运营者”（在可行的情况下，建议征求行业主管部门的意见）；如是，则发行人应评估其采购网络产品和服务的行为或者开展数据处理活动的行为是否影响或者可能影响到国家安全；如认为是，则需要及时申报网络安全审查。
- 在《审查办法2022修订》2022年2月15日实施后，如发行人属于掌握超过100万用户个人信息的网络平台运营者赴国外上市的，则必须申报网络安全审查。但是掌握个人信息数量并非赴香港上市企业申报网络安全审查的标准，因此赴香港上市是否需要进行网络安全审查的判断重点应落在“影响或者可能影响国家安全”，企业赴香港上市判断是否“影响或者可能影响国家安全”，可以参考本文第二节有关“非关键信息基础设施运营者”考虑的评估因素。
- 如果发行人不属于影响或者可能影响国家安全的非关键信息基础设施运营者或网络平台运营者，一旦因其处理数据的活动或行为影响或者可能影响国家安全，则仍然需要申报网络安全审查。建议相关企业参考本文有关“非关键信息基础设施运营者”考虑的评估因素。

虽然《审查办法2022修订》刚刚发布，我们依然期待《数安条例意见稿》终审稿可以早日出台，两者构成完整规则以指导实践。企业是否需要主动申报网络安全审查，建议可从运营者的主体性质、处理个人信息的人数，以及处理行为本身的影响等维度出发，对影响或者可能影响国家安全进行判断与风险评估。值得一提的是，上文两个港股上市案例中，无论是否申报网络安全审查，发行人均采取了数据安全及合规的相关措施，包括：保障数据的安全存储和传输、防止任何未经授权的数据获取和使用、加强网络与数据安全的内控制度、发挥管理层与董事会的监督管理职责等，以表明发行人对现有数据处理行为合法合规的做法。

【总结】

随着网络安全审查制度体系的逐步落地与完善，企业上市前的数据合规实施工作、评估及审计落实情况，以及确认是否需要依法申报网络安全审查已然成为拟赴境外上市企业所需面临的新课题。一方面，拟境外上市的企业需在上市前搭建较为完整的数据合规体系^[3]，以应对上市过程中保荐人、中介机构的询问以及监管部门的审核。另一方面，经自评，有可能触发网络安全审查申报的企业，应当在上市材料递交前履行网络安全审查申报义务，以符合监管要求。目前网络安全审查的案例有限，网络安全审查的具体实践仍有待观察和总结。

注释：

[1] https://www1.hkexnews.hk/listedco/listconews/sehk/2021/1123/2021112300033_c.pdf。为了便于阅读，招股书中的表述与本文其他部分的表述做了统一处理。

[2] https://www1.hkexnews.hk/listedco/listconews/sehk/2021/1220/2021122000006_c.pdf

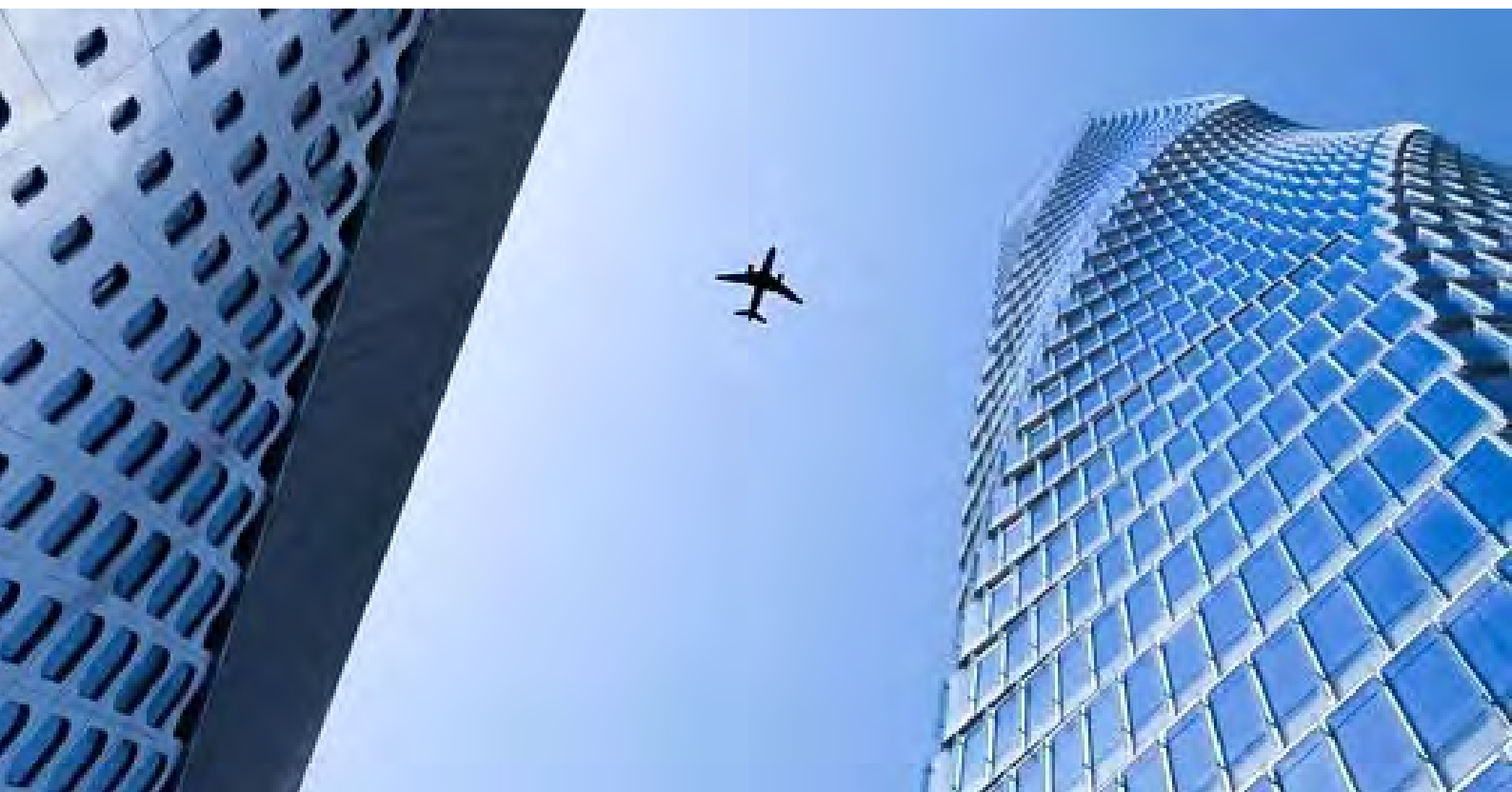
[3] https://www1.hkexnews.hk/listedco/listconews/sehk/2021/1207/2021120700018_c.pdf

[4] 具体可详见《面对网络安全审查，中概股企业需做何准备？——下篇：企业数据合规建议》



面对网络安全审查 中概股企业需做何准备？

环球律师事务所
孟洁 | 郁雷 | 张真真



【前言】

随着《网络安全审查办法》的正式发布，体现了监管机构近年来不断加密、加快的监管趋势和执法依据位阶上升、监管尺度不断细化。对于能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、云计算、大数据、国防科工、大型装备、化工、食品药品、新闻等敏感行业（以下简称“敏感行业”）及处理和掌握大量用户数据的平台类企业，特别是拟赴或已在国外上市的企业，在网络安全、数据安全及用户个人信息保护方面的责任义务不断加码的大背景下，应持续关注相关监管法律法规和政策的变化，不断优化和夯实企业数据合规工作，提升自身有关核心数据、重要数据、用户个人信息保护义务的合规水准，严格审查在采购关键产品（比如核心网络设备、重要通信产品等）、服务（比如云服务、大数据分析服务等）过程中的供应链风险问题，并从组织层面和系统层面双向提高防止数据泄露、窃取或毁损等安全事件的数据保障措施：例如在电信大数据领域中，对终端设备实施安全鉴别机制；对采集程序的接入实施强身份认证，例如Kerberos，LDAP等。同时还应当保证上传程序自身的安全机制，建议使用SFTP、基于Kerberos认证的Flume、Kafka等；设置组织内部统一的网络安全与数据安全策略；对相关软件配置安全基线、设置访问控制权限；限制对核心网设备执行端口镜像类操作；对冗余传输数据要求及时切断；以及需要加强在数据传输过程中的审计日志管理等。相关防范措施，我们还将在下文中具体阐释，以期帮助企业开展合规工作并预防发生风险。

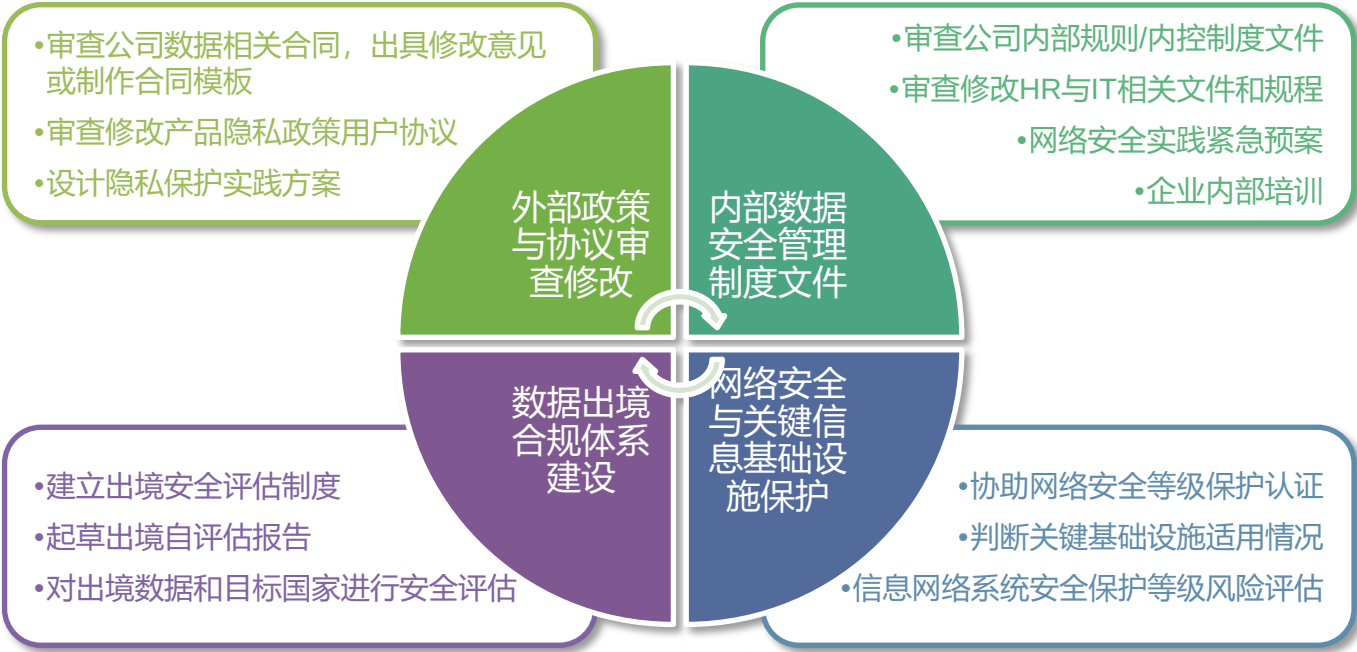
一、企业内部数据合规体系建构

随着我国数据合规相关法律法规的逐渐完善以及监管的不断加强，企业所面临的数据合规风险日益提高。在近期部分中概股企业赴美上市所引发的企业网络安全审查，以及《网络安全审查办法》最近出台的背景下，企业内部数据合规建设的重要性和紧迫性已经不言而喻，特别是在企业拟赴国内外上市、重组、投融资时更应当注重构建企业内部数据合规体系，从而为数据资产提供全生命周期的安全保护。在上市或完成重组或投融资后，还应当持续关注我国以及上市所在国关于数据以及个人信息的立法动态，及时完善企业的数据合规策略，并在企业进行数据共享、转让、公开披露、数据出境，发生重大安全事件或者企业业务模式、信息系统、运行环境发生重大变更时及时进行个人信息安全影响评估。

因此，我们建议企业应当将数据合规的主要治理重心放在以下五个部分：

- **设计和审查外部政策与协议：**包括涉及隐私保护实践方案，审查企业数据处理方面的相关协议、产品隐私政策及和用户服务协议等。
- **建立及完善企业内部数据安全及规划管理制度：**例如在设立总体内部规则、内控制度的同时，有针对性地修订HR及IT部门的制度文件及规程。此外，企业还应当设计网络安全事件应急预案，并定期开展企业内部培训与演练。
- **建立数据出境合规体系：**在出境前开展数据出境评估并落实安全保障制度与措施。当涉及数据出境时，企业应对出境数据的合法性、正当性、必要性和对目标国家的政治及法律环境进行安全评估，出具出境自评估报告。
- **完善网络安全与关键信息基础设施保护：**要求企业完成网络安全等级保护认证，核心数据以及重要数据的识别并配合开展分级分类保护的风险评估与控制措施，同时应结合相关法律法规判断关键信息基础设施的适用情况，并遵守关键信息基础设施运营者的增强法律责任和义务。
- **在完善合规制度的同时，**企业内部数据安全的组织架构也需要同时配套落实，以保证合规体系的完整、有效运行，可以按照决策层、管理层、执行层、员工和合作伙伴、监督层的组织架构设计。在具体执行过程中，组织也可赋予已有安全团队、法律合规部门与其它相关部门关于数据安全的工作职能，或者向第三方专业团队寻求帮助，协助企业开展机构设计、工作辅导与评估审计。特别是在面对网络安全审查时，需要企业内部各部门间相互配合、迅速响应，依据法律规定、监管要求和内部合规体系要求，配合监管完成审查与整改工作，必要时需要与监管部门进行提前沟通，以了解企业执行尺度与政策方向的匹配性，以便动态地调整符合国家法律法规、政策要求的合规基线。

当然，企业内部合规体系和组织架构也绝非一劳永逸的，而是需要不断动态调整的，特别是随着企业上市过程、投融资进展审查是否通畅而不断落实和完善，发现存在不合规之处，还需要及时整改与优化。同时需要组织人员进行培训，将梳理出来的问题通过内部落实整改与法律法规的跟踪变化进行比对并进一步复盘以查漏补缺、更新完善，最后构成一个有效的合规闭环。



二、针对网络安全、数据安全和个人信息保护审查的重点关注

《网络安全审查办法》的审查范围不再局限于《网络安全法》规定的关键信息基础设施运营者采购网络产品和服务，同时将数据处理者纳入网络安全审查的范围。换言之，即使企业不落入或者不确定是否落入关键信息基础设施运营者范围，若开展数据处理活动且达到影响或可能影响国家安全的标准，也需要履行主动申报网络安全审查的义务。因此，《网络安全审查办法》明确，网络安全审查的启动有下述情形：

➤ 主动申报审查：

- (1) 关键信息基础设施运营者采购网络产品和服务，应预判该产品和服务投入使用后可能带来的国家安全风险；
- (2) 网络平台运营者开展数据处理活动，影响或者可能影响国家安全的；
- (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。

➤ 依职权审查：

- (1) 网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照《网络安全审查办法》进行审查；
- (2) 网络安全审查办公室通过接受举报等形式加强事前事中事后监督，如审查办公室认为被举报的某产品或者服务或者某数据处理活动已经或者可能。

《数据安全法》在第二十四条规定，国家建立数据安全审查制度，对影响或者可能影响国家安全的的数据处理活动进行国家安全审查。但考虑到企业履行网络安全和数据安全义务以及审查要求上仍有差异，本部分将分别进行论述。此外，对于监管机构近年来不断升级的个人信息保护，也将同步给出合规建议。

(一) 网络安全审查合规建议

首先，良好的业务连续性管理是网络安全及数据合规工作的基石。根据《网络安全法》第22条、第23条，企业应确保业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用；同时为其产品、服务持续提供安全维护。

其次，企业应当确定网络安全等级保护工作责任人，建立网络安全等级保护工作责任制，落实责任追究制度。根据《网络安全法》第34条以及《网络安全等级保护条例（征求意见稿）》第20、21条，企业应当按照国家法律法规的规定和相关国家标准的要求，设置专门的网络安全管理机构 and 网络安全管理负责人，对网络安全管理负责人和关键岗位的人员进行安全背景审查，签署特殊保密协议，落实持证上岗制度。

第三，密码及通信安全管理也将成为网络安全审查的重要部分，建议企业根据《网络安全等级保护条例（征求意见稿）》第4条的规定，在网络建设过程中，同步规划、同步建设、同步运行密码保护措施。如果企业网络定级为第三级以上，应当使用国家密码管理部门认可的密码技术、产品和服务，并且履行密码安全管理职责，加强密码安全制度建设，完善密码安全管理措施，规范密码使用行为。在进口密码产品以及含有密码技术的设备或者出口商用密码产品时，依据2020年8月的《商用密码管理条例（修订草案征求意见稿）》，对涉及国家安全、公共利益的商用密码列入受进口许可要求约束的商用密码清单（“进口清单”）。在该情况下，商用密码产品（及相关服务）可能仍需遵守进出口管制要求、检测认证要求（在有限情况下）和国家安全审查要求。并且，因列入进口和出口清单的商用密码项目属于“两用物项和技术”，还必须向商务部提出申请，以获得许可。企业及企业员工只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外生产的密码产品。此外，企业及企业员工不得销售境外的密码产品。

第四，《网络安全审查办法》第十条提出了“审查重点评估相关对象或者情形的以下国家安全风险因素：

- （一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险；
- （二）产品和服务供应中断对关键信息基础设施业务连续性的危害；
- （三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；
- （四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；
- （五）核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；
- （六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；
- （七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素”。

因此，企业应当重点关注网络产品和服务的供应链安全审查工作，落实对上游供应商的事前评估、事中和事后审计的全生命周期审查。具体而言，明确供应商在收集、保存、使用、共享、转让、公开披露等数据处理活动中须遵循的规则，根据国家网络安全相关法律法规以及企业内部合规要求制定评估项，对供应商的数据与网络安全合规情况进行逐项评估，排查隐患，提前预防并有效防范数据泄露、窃取、损毁、非法篡改。此外，企业也应依据《网络产品安全漏洞管理规定》针对相关的网络产品、服务、系统采取相应的漏洞修补或防范措施。

第五，我国证监会曾在某企业发行可转债项目中询问：“发行人开展现有业务、本次募投项目是否需要进行网络安全等级保护测评”。根据《网络安全等级保护条例（征求意见稿）》第33条的规定，企业建设、运营、维护和使用网络，向社会公众提供需取得行政许可经营活动的，相关主管部门应当将网络安全等级保护制度落实情况纳入审计、审核范围。根据拟定的不同等级，企业应当遵守的责任和义务也有所不同。

第六，从风险控制和审计管理要求出发，企业应由安全审计员对系统各个组成部分进行审计和管理，包括根据安全审计策略对各类网络安全信息进行分类记录，并对记录分类存储、管理、查询和分析，并根据分析结果及时处理；网络日志需保存六个月以上，企业须对各类安全报警和日志信息进行关联分析，生成统一审计报告，提取出安全事件或隐藏攻击的规律，形成报警和预判。在进行云计算平台安全设计时，还应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计。

第七，依据《网络安全法》第22条及第34条、《关键信息基础设施安全保护条例》第15条及第18条，企业应当制定网络安全事件应急预案并定期进行演练；当企业发现提供的产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

（二）数据安全合规建议

根据此次公布的《网络安全审查办法》第十条的兜底规定，网络安全审查主要考量的风险包括一切可能危害关键信息基础设施安全、国家数据安全的因素。因此，结合《网络安全审查办法》和《数据安全法》，企业在进行合规落地时应尽到的义务包括：

首先，明确企业自身所控制和受规制的数据范围和类型，确保数据收集的合法、正当和必要性；其次，企业内部应当设立数据安全管理和分级分类保护制度，采取必要技术和措施保障数据安全；再次，需要按照要求对数据活动定期进行安全评估，并向有关主管部门报送风险评估报告。并且，企业需加强风险监测，在发现数据安全缺陷、漏洞等风险时，应当立即采取处置措施，若发生数据安全事件，应及时告知用户并向有关主管部门报告。当公安机关、国家安全机关因依法维护国家安全或者侦查犯罪需要调取数据时，企业应当在核验相关身份和证明后配合执法。并且，根据《数据安全法》第三十六条规定，当境外执法、司法机构依据其职权对企业进行调查，要求企业提供相关数据时，企业不能径直接按照境外执法机构的要求提供，应当先向主管机关报批方可提供。

需要特别注意的是，针对《数据安全法》中提到的“从事数据交易中介服务的机构”，在进行交易、提供服务时，还应当同时要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。这类企业在业务中往往会涉及大量数据信息，甚至可能会涉及关乎国家数据安全的信息，需要密切关注相关配套法规动态，落实合规举措，特别是赴国外上市时更需要审慎评估和自查。

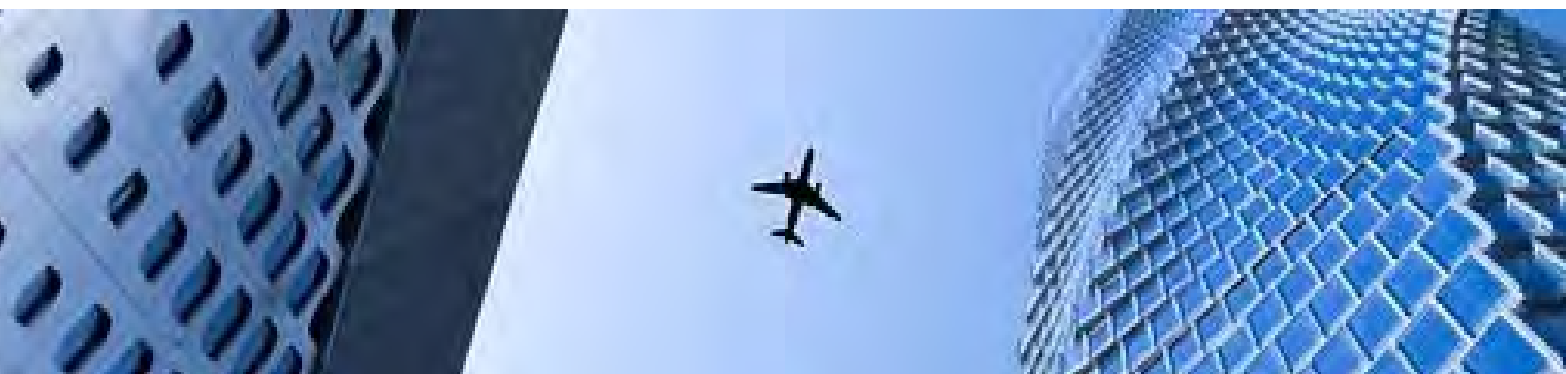
（三）个人信息保护合规建议

针对个人信息保护问题，《中华人民共和国网络安全法》（以下简称《网络安全法》）《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）以及《信息安全技术 个人信息安全规范》（GB/T-35273-2020）等法律法规、国家标准从顶层设计、原则架构以及具体操作层面进行了全方位规定。

在立法不断完善的同时，监管部门的执法要求和力度也在逐渐细化和增强。工信部2019年10月31日发布的《关于开展App侵害用户权益专项整治工作的通知》中对于违规收集和使用用户个人信息的情形进行了明确规定；2021年3月12日，网信办等四部门联合发布的《常见类型移动互联网应用程序必要个人信息范围规定》中也明确要求App不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能，并且针对常见的39类App的必要个人信息范围进行了明确限制。

上述规定要求企业在进行产品及服务设计时，首先重视隐私设计，在设计阶段实施个人信息保护的原则和要求。其次，默认设置应当最大程度地保护个人信息。再次，在系统和产品建设过程中，保证安全和隐私保护措施同步规划、同步建设和同步使用。企业在进行业务开发时，应始终将个人信息保护原则融入产品/服务设计，顺势而为，而非逆向操作，避免企图通过政策法规的空白，超出实际需求对用户个人信息进行收集、使用和处理。

企业同时应当结合自身业务，对可能涉及的个人信息进行整理梳理，构建内部个人信息保护完整性合规清单及层级架构，结合法律指引和国家标准，从个人信息生命周期的全流程，包括收集、存储、使用、共享/委托处理/转让/对外披露、删除、销毁，以及用户行权、安全事件处理等全方面进行制度建设并展开自查，进行内部梳理，防患于未然。特别是针对数据对外共享与数据跨境传输，需要制定严格详细的评估方案。例如，此次公布的《网络安全审查办法》第六条明确要求：掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查；并且网络安全审查主要考量的风险就包括大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险，以及被国外政府影响、控制、恶意利用的风险。



由于《个人信息保护法》第五十八条要求提供基础性互联网平台服务、用户数量巨大、业务类型复杂的平台成立主要由外部成员组成的独立机构，对个人信息处理活动进行监督；对严重违法法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；定期发布个人信息保护社会责任报告，接受社会监督，企业需要进一步建立主动拥抱中介机构审查、平台自律审查以及公众、媒体与监管机构审查的多重监督机制。在面临监管部门审查时，应快速响应、积极配合并落实内部自查和整改。无论是在产品/服务设计、内部制度建设，以及个人信息主体行权落实等方面及时进行合规咨询，保持与监管机构的良好沟通与提前问询，最大程度地避免因个人信息保护不合规而给企业带来风险，以及业务运营、品牌形象上的负面影响。

• 违法违规收集使用个人信息-App/SDK合规自查工具



- 使用方：App开发团队等
- 咨询方：法务、运维
- 使用时间：App上线

App收集使用个人信息负面清单

- 使用方：App开发团队
- 咨询方：法务、运维等
- 使用时间：重要App或重大版本更新上线

App调用权限核查清单

- 使用方：App开发团队等
- 咨询方：法务、运维

App账号注销自查清单

- 使用方：App运营团队
- 咨询方：信息安全、法务
- 使用时间：敏感信息处理、高风险场景、新业务模式等

隐私影响评估报告

三、企业数据出境合规建议

随着如上文所述，本次《网络安全审查办法》重点修订的是企业聚焦数据出境的合规义务，如在第七条中新增了针对“企业赴国外上市的网络安全审查义务”，第十条也适用于国外上市的情景，将“关键信息基础设施，核心数据、重要数据或大量个人信息”纳入审查要点。正如相关专家指出，“企业在国外上市必然带来数据的跨境流动。当然，并不是说只要有数据跨境流动就会带来安全风险，但如果上市企业是互联网企业，且企业在经营过程中会收集产生大量国家核心数据、重要数据和批量个人信息，那么数据的出境安全风险就必须慎重对待。”近期网信部门的执法实践也为拟国外上市的企业，敲响了上市前需进行数据出境合规工作的警钟。

目前我国数据出境的监管方式以安全评估为主，监管的重点数据类型主要包括个人信息和重要数据。以下为我国目前数据出境有关的法规和国家标准，分别为《网络安全法》《个人信息保护法》《数据安全法》《数据出境安全评估办法（征求意见稿）》《信息安全技术数据出境安全评估指南（征求意见稿）》等。目前除《网络安全法》和《数据安全法》外，其余法规和国家标准均尚未生效，但对企业数据出境合规建议具有重要指导意义。

（一）盘点数据出境情况

《数据安全法》建立了以数据分级分类制度为基础的企业合规路径，明确了重要数据处理者的数据安全保障增强义务。如上文所述，《数据安全法》第三十一条对关键信息基础设施运营者以及关键信息基础设施运营者以外的其他重要数据处理者所收集的重要数据出境的情况进行了规定，要求适用国家网信部门会同国务院有关部门制定的管理办法。本次《网络安全审查办法》虽说主旨在于规定对有可能影响国家安全的数据处理活动进行审查，但数据出境到国外被外国政府控制、影响和利用也被视为影响国家安全的因素之一，因此需要遵守的合规的义务与《数据安全法》的精神高度吻合。

由此，企业首先应排查自身数据资产。其次，应针对数据的重要程度、敏感程度对数据进行分类分级的保护，同时，区分一般数据和重要数据，按数据的重要性程度从高到低的顺序进行具体匹配，制定重要数据目录清单。国家信息安全标准化委员会也正在制定《重要数据分类分级指南》；各行业也在加紧研制本行业的数据分类分级标准和重要数据目录，企业需要关注相关动态，及时调整本企业内部数据分级分类的逻辑和标准。最后，根据企业自身身份（如央企、国内、大型互联网平台、一般性企业）和出境目标国家（依政治敏感度与双边关系紧张程度的强、中、弱等级）适配相应的合规义务。

（二）进行数据出境安全评估

《信息安全技术数据出境安全评估指南（征求意见稿）》对数据出境安全评估流程和方式进行了指引，虽然目前仍然处于征求意见稿状态，但企业可以参照后进行数据出境安全评估自查。首先，企业内部需建立出境安全评估制度并制定出境自评估流程等文件。其次，根据业务需求与实际状况，判断是否涉及重要数据出境。如涉及，在企业自评估后，还需要报请行业主管部门与网信部门，因此需要制定和设计监管部门能够接受的评估流程及报请策略。在此过程中，需要对数据出境接受方的安全保障能力等级及所在国际和地区的政治、法律环境、发生安全事件的可能性进行跟踪评估，防止发生变化和调整。最后，综合上述因素，对数据出境活动按照风险等级进行划分，制定企业出境评估报告并提交监管部门申请审查，并与其保持持续沟通与对方案的整改。

（三）安全检测和评估认证

根据《个人信息保护法》第三十八条规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，需按照国家网信部门的规定经专业机构进行个人信息保护认证。《数据安全法》第十八条指明了国家对安全检测评估、认证服务的支持态度。虽然对于数据出境方面的认证机制目前尚未正式出台，但比拟我国网络安全产品与服务、网络关键设备和网络安全专用产品安全认证等均通过中国网络安全审查技术与认证中心，采取强制测评与自愿测评相结合，进行定期和年度检测认证或自愿认证，企业可以根据自身业务所对应的要求选择相关检测与评估，以符合实施数据出境的合规措施。

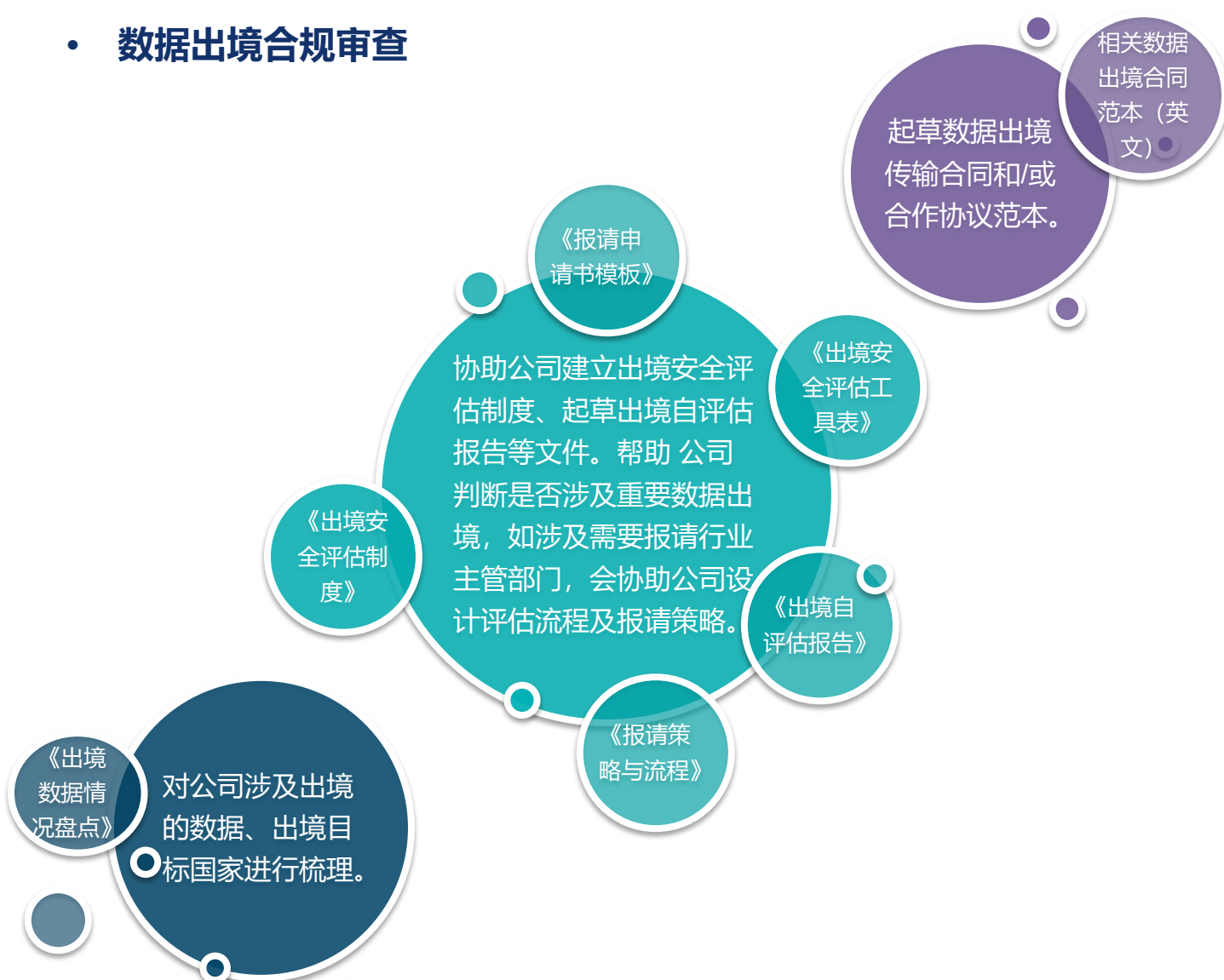
（四）关注数据出境传输合同和/或合作协议范本的制定工作

《个人信息保护法》第三十八条的规定，个人信息处理者因业务需要向境外提供个人信息的，可以按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务，并监督其个人信息处理活动达到个人信息保护法律法规规定的个人信息保护标准。目前，国家网信部门尚未正式颁布数据跨境传输标准合同。但近日媒体报告，知情人士表示国家互联网信息办公室已启动“中国版SCC”——数据跨境传输标准合同的起草工作。企业可密切关注监管部门相关动态并选择最适合本企业的数据出境合规机制。

（五）其他相关合规要求

根据《中华人民共和国电信条例（2016年修订）》（国务院令第666号）、《信息产业部关于公布〈国际通信出入口局管理办法〉的命令》（信息产业部令[2002]第22号），以经营电信业务为目的，通过互联网国际出入口设置虚拟网络的，应当报信息产业部批准；以内部使用为目的，通过互联网国际出入口设置虚拟专用网的，应当报信息产业部备案；与香港特别行政区、澳门特别行政区和台湾地区的通信，参照国际通信管理。

• 数据出境合规审查



总结

通过对《网络安全审查办法》要点的阐述和对企业数据合规建议的分析，笔者希望从事敏感行业和处理大量用户数据信息的平台类企业能够理解监管逻辑，关注监管法律法规和政策的变化，完善数据合规体系制度建设并落实到企业日常运营的过程中。此外，对于近期赴国外上市，宜尽快着手开展数据合规的自查工作，对于不合规事项尽快整改，并考虑适时与监管机构沟通，充分预估受到网络安全审查的可能性及监管不确定性带来的风险。针对以上风险，也建议在相关上市文件中进行充分披露。

密切关注相关配套法规动态，落实合规举措，特别是赴国外上市时更需要审慎评估和自查。



企业数据出境评估指引—— 暨《数据出境安全评估办法 (征求意见稿)》解读

环球律师事务所
孟洁 | 董杰睿 | 戴畅



【前言】

数据出境关乎国家安全，自2017年6月1日起施行的《中华人民共和国网络安全法》（“《网络安全法》”）、2021年9月1日起施行的《中华人民共和国数据安全法》（“《数据安全法》”）和2021年11月1日（暨今天）起施行的《中华人民共和国个人信息保护法》（“《个人信息保护法》”），均从法律层面规范了数据出境的合规机制。从目前数据合规的整体法律体系的构建框架来看，针对数据出境的合规要求，需要针对数据出境主体的不同身份以及拟出境数据的不同类型进行甄别，然后分别按照不同法律法规的要求进行具体规范。本文通过对现行法律法规（包含征求意见稿）中关于数据出境合规要求的梳理，提出相关合规建议，以供同行参考与交流。

针对数据出境不同的合规要求中，其中一项是针对数据出境进行评估。本文主要是基于2021年10月29日国家互联网信息办公室（“网信办”）发布的《数据出境安全评估办法（征求意见稿）》（“《2021年办法（征求意见稿）》”），对数据出境的企业自评估与监管机构的安全评估进行重点评析。另外，“数据出境”和“数据本地化”实质是一个硬币的两面，从境内业务的视角管理数据出境，可以考虑的思路是：**基于数据分类设立“数据本地化”的梯度要求**，对不同类型数据出境机制配备不同层级的本地化要求，并促成**配套的评估、备案/许可和认证机制**。

一、数据出境的基本监管要求

境内数据出境是指网络运营者通过网络等方式将其在中国大陆境内（以下简称“境内”）运营中收集和产生的个人信息或其他数据，通过直接提供或开展业务、提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。

需要说明的是：（1）网络运营者包括所有者、管理者和网络服务提供者，可能是内资公司、外资工作、合资公司等。（2）数据出境有多种形式，不囿于数据境外存储。数据虽未转移存储至本国以外的地方，但被境外机构、组织、个人访问查看的（公开信息、网页访问除外）；网络运营者在境内运营中收集和产生的个人信息（主要指集团内部数据）由境内转移至境外；向境内但不属于我国司法管辖或未在境内注册的主体提供数据。（3）出境的数据既可能是个人信息，也可能是非个人信息但构成重要数据或者国家核心数据，或者是非个人信息且非重要数据、国家核心数据的企业其他业务运营类数据。

因此不难理解，在任何部门或行业中使用网络的任何位于中国境内的企业都有可能属于“网络运营者”，进而受到关于个人信息和重要信息出境的规制。我国目前针对数据跨境传输而言，没有针对外企的“特殊待遇”，内外资企业实施同等国民待遇。内外资企业能够将其在中华人民共和国境内运营的数据出境，实际需要同时满足三个层面的要求：数据跨境的一般性要求、特定行业的数据本地化增强要求、外企准入负面清单要求。

《网络安全法》2016年提出了对于“**关键信息基础设施运营者**”（“**CIIO**”）的数据（无论是个人信息还是重要数据）均有本地化存储和必要时跨境传输时的评估义务要求，实践中引起了监管部门和广大企业的广泛关注。2017年4月《个人信息和重要数据出境安全评估办法（征求意见稿）》（“《2017年办法（征求意见稿）》”）对“个人信息和重要数据”出境的规制主体进一步扩大，由《网络安全法》规定的CIIO扩展到所有的“**网络运营者**”，但对个人信息和重要数据未予区分，规定了一致的出境规则。随后，推荐性国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》（“《数据出境安全评估指南（征求意见稿）》”）于2017年10月13日完成了意见征求，但至今尚未公布。此外，网信办于2019年6月13日发布了《个人信息出境安全评估办法（征求意见稿）》（“《2019年办法（征求意见稿）》”），针对个人信息的出境情形作出了比较严格的规定，但仍然保持着《2017年办法（征求意见稿）》针对整个网络运营者将境内收集个人信息出境的规范立场，重点规定了个人信息出境的安全评估要求，将个人信息和重要数据评估拆分为二，有分别规定评估机制的尝试。

上述这些办法虽然制定时间较早，但目前都仍然处于征求意见稿状态，并且是在上位法还未全面颁布之时仅根据《网络安全法》为依据制定的。如今，《数据安全法》和《个人信息保护法》均已出台并生效，其分别对重要数据出境和个人信息出境的评估要求做出规定：其中，《数据安全法》对于数据出境评估的被规制主体规定为“CIIO”、“重要数据的处理者”以及“其他数据处理者”；《个人信息保护法》对于个人信息出境的被规制主体为“CIIO”和“个人信息处理者”；而《2021年办法（征求意见稿）》将被规制主体设定为“数据处理者”。我国目前已经公布的法律法规、标准尚未对“数据处理者”或“处理者”术语进行定义，在做出判断时，可参考：《个人信息保护法》第七十三条中对“个人信息处理者”的定义，即“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”，以及《数据安全法》第三条中对“数据处理”的定义，即“数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等”的相关规定。

《2021年办法（征求意见稿）》题为“数据出境安全评估办法”，顾名思义，着眼于支撑《数据安全法》下所规定的数据的出境评估，必然包括了“个人信息”及“重要数据”出境评估，更有利于作为《网络安全法》、《数据安全法》及《个人信息保护法》数据安全出境、安全评估相关规定的**实施细则**，为法律落地做出细化规定。其规定了数据出境的**风险自评估与安全评估**的义务主体、监管机构、评估重点等，还细化了数据出境评估申报流程、要求和处理时间节点，为数据安全义务方履行合规义务提供了指引。作为“网络运营者”、“数据处理者”的企业，在参与经济全球化的过程中，时常会涉及各类数据跨境传输的情形，因此，准确界定数据跨境传输行为及其法律合规义务，是企业实施跨境商业运营中最基础的一环。

本文也主要围绕以上内容，厘清风险自评估与安全评估的义务并提出合规建议；最后提示未依法完成评估工作而可能产生的责任，以期为业务中涉及数据出境场景的数据处理者理解《2021年办法（征求意见稿）》并关注后续监管动向，把握合规要点，做好相应的准备工作提供合规思路。



二、数据出境评估相关法律法规

我们在下图中梳理了数据出境评估相关法律法规（含征求意见稿）的发布情况供企业参考：

2017年4月

《个人信息和重要数据出境安全评估办法（征求意见稿）》

第二条规定**网络运营者**在中华人民共和国境内运营中收集和产生的**个人信息和重要数据**，应当在境内存储，因业务需要，确需向境外提供的，应当按照本办法进行安全评估。

明确了**安全评估的适用范围、评估要点、安全评估反馈时间和评估频次等**。

2017年6月《网络安全法》

第三十七条提出**关键信息基础设施的运营者**在中华人民共和国境内运营中收集和产生的**个人信息和重要数据**确需向境外提供的应当进行安全评估。

2018年1月

国家标准《数据出境安全评估指南（征求意见稿）》

规定了数据出境**安全评估流程、评估要点、评估方法**等内容，为国家网信部门、行业主管部门以及网络运营者进行**主管部门评估和安全自评估**提供指引。

2019年5月

《数据安全管理办法（征求意见稿）》

第二十八条规定**网络运营者**发布、共享、交易或**向境外提供重要数据**前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。向境外提供个人信息按有关规定执行。

2019年6月

《个人信息出境安全评估办法（征求意见稿）》

第二条规定**网络运营者**向境外提供在中华人民共和国境内运营中收集的**个人信息**，应当进行安全评估。明确了个人信息出境安全评估的**申报材料、评估重点、网络运营者与个人信息接收者签订的合同或者其他有法律效力的文件（合同）的具体内容、合同中应明确的网络运营者承担的责任和义务等**。经安全评估认定个人信息出境可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全的，不得出境。

2021年9月《数据安全法》

第三十条规定**重要数据**的处理者应当按照规定对其数据处理活动定期**开展风险评估**，并向有关主管部门报送风险评估报告。

2021年11月《个人信息保护法》

第三十六条规定**国家机关处理的个人信息**应当在中华人民共和国境内存储，确需向境外提供的，应当进行**安全评估**。

第四十条规定**关键信息基础设施运营者和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**，应当将在中华人民共和国境内收集和产生的**个人信息**存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估。

2021年10月

《数据出境安全评估办法（征求意见稿）》

第二条规定**数据处理者**向境外提供在中华人民共和国境内运营中收集和产生的**重要数据和依法应当进行安全评估的个人信息**，应当按照本办法的规定进行安全评估。

第三条规定数据出境安全评估坚持**事前评估和持续监督相结合、风险自评估与安全评估相结合**。

除此之外，国家网信部门和行业主管部门已经针对部分行业就特定垂直领域的数据本地化出台了相关文件，包括涉及国家秘密、增值电信、征信信息、审计底稿、地图、网络出版、气象卫星、医疗健康大数据、人类遗传资源、网约车、个人金融信息、网络租赁自行车等行业。**相关行业的企业也应关注此类文件提出的合规义务。**

三、数据出境评估的适用范围

如前所述，“跨境传输”与“本地存储”两者只有有效组合才能**设立较为完善的数据出境监管环境**。**如何设立不同层级的数据本地化严苛度/数据出境自由度，应基于不同“数据类型”而差别对待**，因此“数据分类分级”是数据跨境传输监管的有效抓手和基石。《2021年办法（征求意见稿）》对于评估的适用范围包括针对CIIO及一般网络运营者，“个人信息”及“重要数据”的出境场景。下文将分别对不同类型企业及不同敏感程度的数据出境适用情况做出阐述：

（一）针对CIIO数据的评估适用情况

《网络安全法》规定了CIIO向境外提供数据的安全评估义务；《数据安全法》亦明确CIIO向境外提供重要数据适用《网络安全法》的规定；《个人信息保护法》中明确了CIIO向境外提供个人信息的安全评估义务。《2021年办法（征求意见稿）》回应了《网络安全法》、《数据安全法》和《个人信息保护法》的相关规定，明确**CIIO收集和产生的个人信息和重要数据应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估**。**我们提示，作为CIIO的企业，原则上，在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。确有需要向境外提供数据时，不论数据类型为个人信息或重要数据，不论数据量多少，都应进行安全评估。**

（二）针对重要数据的评估适用情况

《数据安全法》要求重要数据的处理者对其数据处理活动定期开展风险评估，除CIIO外，其他数据处理者向境外提供重要数据的数据出境安全管理办法，由国家网信部门会同国务院有关部门制定。《2021年办法（征求意见稿）》也结合了《数据安全法》的相应要求，明确**出境数据中包含重要数据出境的业务需要履行数据出境安全评估的要求**。

值得关注是，目前已生效法律法规尚未对“重要数据”做出明确定义，《数据安全法》将重要数据的具体目录的制定工作分配至各地区、各部门，如《汽车数据安全管理办法（试行）》中就对重要数据所包含的具体数据类别做出了划分。在部分法规和标准中我们也可以看到重要数据的相关规定，如《数据安全管理办法（征求意见稿）》对重要数据进行了定义，《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》对重要数据的危险程度识别特征进行了列举；《2017年办法（征求意见稿）》中提到重要数据是与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围需参照国家有关标准和重要数据识别指南。而目前《信息安全技术 重要数据识别指南（征求意见稿）》也尚处于征求意见阶段，尚未正式生效。

《网络安全标注实践指南——数据分类分级指引》中将重要数据作为一个定级概念；部分国家标准也尝试对重要数据的范围做出划分，如《信息安全技术 数据出境安全评估指南（征求意见稿）》附件A对重要数据给出了具体范围，国家推荐性标准《信息安全技术 重要数据识别指南（征求意见稿）》提出了重要数据的特征，明确了识别重要数据的基本流程和对重要数据的描述格式，为识别重要数据提供支撑。同时，《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》也对重要数据出境后的管理提出了进一步的要求，即企业须加强对数据出境后的跟踪掌握。

我们提示，重要数据出境安全评估要求不涉及主体性质和数量多少的限制，即只要出境的数据中包含重要数据，不论数据多少，都应当申报安全评估。因此，建议企业应关注涉及出境的数据是否包含重要数据，并根据要求做好合规评估工作。

（三）针对个人信息的评估适用情况

本次《2021年办法（征求意见稿）》的一大亮点是，明确了《个人信息保护法》第四十条规定的“个人信息达到国家网信部门规定数量的个人信息处理者”的数量级别，并且明确了“达到规定数量”应从两个不同维度的标准计算：

• 处理个人信息达到一百万人的个人信息处理者

我们理解，这是以数据处理者处理个人信息的规模进行的评估，如数据处理者处理个人信息达到一百万人，涉及数据出境业务时，则不论向境外提供个人信息数量多少，都应申请安全评估。在《2021年办法（征求意见稿）》一出台后，很多人会关注的是今年7月发布的《网络安全审查办法（征求意见稿）》中提及的“掌握超过一百万用户个人信息的运营者赴国外上市”的安全审查义务和《2021年办法（征求意见稿）》中的“处理个人信息达到一百万人的个人信息处理者向境外提供个人信息”的安全评估义务是否相互冲突，即完成了网络安全审查是否还需要进行数据出境安全评估。我们理解，根据两个文件的内容来看，申报网络安全审查和数据出境安全评估提交的材料、审查重点、审查主体都不尽相同。有些拟向国外上市的中概股企业根本不涉及重要数据和个人信息跨境传输给境外实体的情况，因此从业务层面而言，不受《2021年办法（征求意见稿）》的规制。但需要注意的是，如果这些企业后续在申报上市过程中可能会被境外监管机构要求提供说明数据运营情况的支持性文件，特别是涉及个人信息和重要数据的情况，那么是既需要进行网络安全审查的申报申请，同时还需要进行数据出境自评估与安全评估的。因此，《2021年办法（征求意见稿）》与网信办于2021年7月10日发布的《网络安全审查办法（修订草稿征求意见稿）》（“网安审查征求意见稿”）不存在替代关系，针对的是网信办所管辖的两项不同行政审批内容。网安审查征求意见稿中“掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”没有被取代，且其详细的申报要求和指南亦未在数据出境评估文件中明确，至于当两个审批事宜发生重合情况时，是否企业只须履行一套流程，尚需等待生效的规定出台以及进一步指引性文件进行阐释。因此，我们建议涉及以上两种场景的企业充分了解《网络安全全审查办法（征求意见稿）》和《2021年办法（征求意见稿）》的合规要求，提前做好合规工作。

• 累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息

我们理解，这是针对数据处理者出境个人信息的规模进行的评估，即不论企业所实际掌握的用户个人信息规模多大，也不论数据处理者单次处理个人信息的数量规模，如果累计向境外提供十万人以上个人信息或者一万人以上敏感个人信息的，则均应当申报数据出境安全评估。

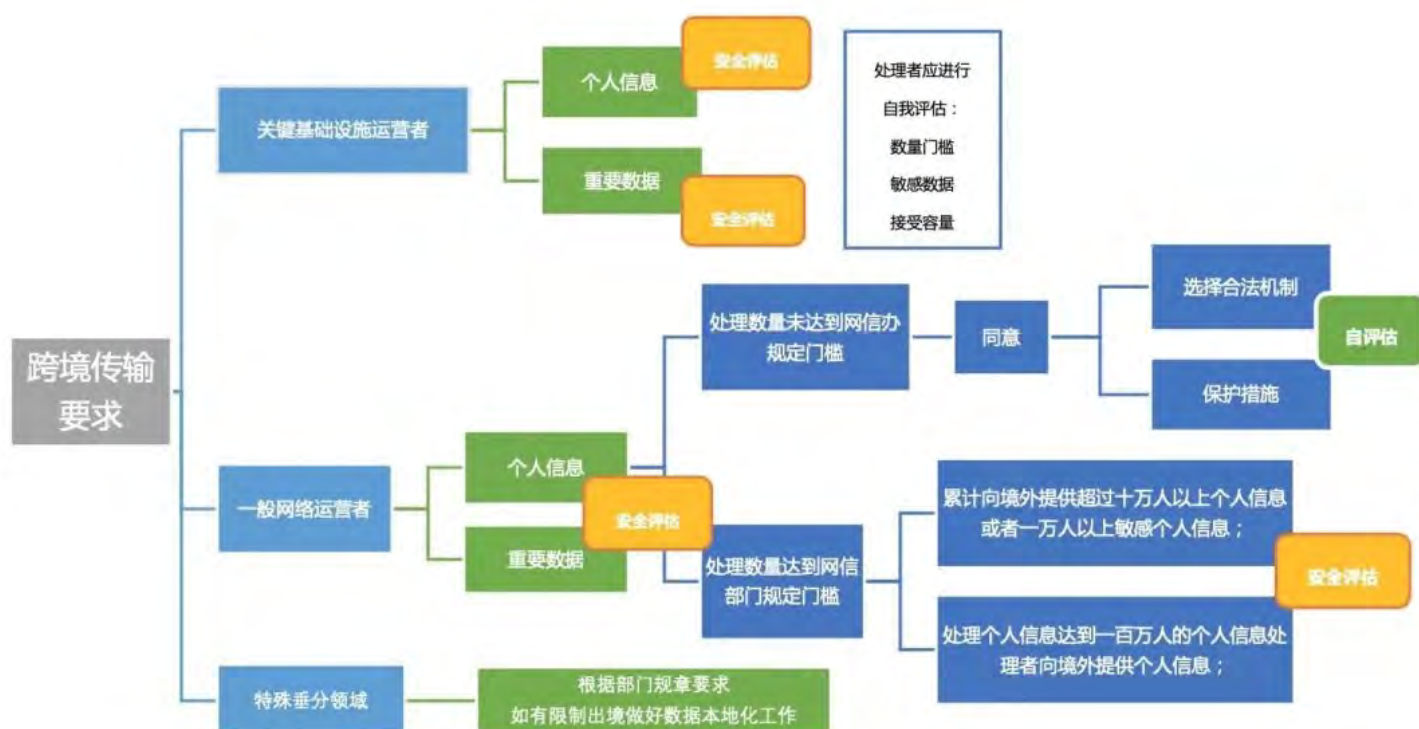
可以看出，《2021年办法（征求意见稿）》中对这两项数量标准设置得相对较低，体现了国家对于数据出境的管控日趋严格，也无形中拟推动了数据本地化的要求。

因此，建议企业尽快开展自查，充分了解内部涉及向境外提供的个人信息数据量及流转情况，判断是否达到了上述规定的标准。需要注意的是，只要满足这两项标准之一，则企业应申报数据出境安全评估。

（四）其他情形

《2021年办法（征求意见稿）》还保留兜底条款，即**国家网信部门规定的其他需要申报数据出境安全评估的情形**，为后期其他细则的规定留出空间，**这就意味着企业应当关注国家网信部门出台的其他文件中对于数据出境安全评估的规定。**

根据目前的法律法规规定，我们梳理了各类数据跨境的场景下数据处理者的安全评估义务，当数据处理者存在数据跨境传输的要求时，应当明确自身性质结合涉及的数据类型，从而判断合规义务：（1）CIIO：涉及个人信息和重要数据出境应当完成安全评估；（2）一般网络运营者：涉及重要数据出境应当进行安全评估，而涉及个人信息则分为两种情况：a.处理个人信息的数量未达到网信办规定的门槛，在获取了个人信息主体的单独同意并选择适当的额外保护措施（如签署标准合同条款等）后，完成风险自评估后可以出境；b.如达到了上文提及的《2021年办法（征求意见稿）》规定的两大类限制出境标准之一的，则应当进行安全评估。除此之外，在做安全评估之前，数据处理者都应该对企业自身的性质、拟出境数量的门槛、出境数据的类型及敏感程度及接受方数据保护能力，以及是否有部门规章对于数据出境或者服务器需要放置于本地有特殊要求等方面做出风险自评估。为了能让企业具有更为清晰的思路，我们做以下图表以供参考：



四、数据出境评估义务的梳理与建议

《2021年办法（征求意见稿）》规定了数据出境的两类评估义务，一是《2021年办法（征求意见稿）》第4条规定的“**数据出境安全评估**”义务，二是《2021年办法（征求意见稿）》第5条规定的“**数据出境风险自评估**”义务。这两类评估义务的适用主体以及评估要求略有不同，与此对应的适用场景也有所不同，下文将具体展开分析企业需要在何种情况下分别履行这两类评估义务。

（一）数据出境风险自评估义务

关于数据出境风险自评估义务，《个人信息保护法》第55条规定，向境外提供个人信息的个人信息处理者应当事前进行个人信息保护影响评估。这是由于根据《个人信息保护法》第38条的规定，在个人信息出境前，企业需要确认境外接收方处理个人信息的活动达到《个人信息保护法》规定的个人信息保护标准，且若选择通过在专业机构进行个人信息保护认证或提交国家网信部门进行安全评估的方式进行出境，则应当提前充分了解出境个人信息的数据、敏感程度、出境目标国家的个人信息保护水平、境外接收方情况以及个人信息出境频率等情况，这决定了个人信息保护影响自评估的必要性。除此之外，《网络安全法》《数据安全法》等现行有效的法律法规均未对风险自评估有所规定，只有2017年发布的《信息安全技术数据出境安全评估指南（征求意见稿）》的国家标准中提到了数据出境安全自评估的相关内容，但由于发布时间较早且未生效，其参考意义有限。

此次出台的《2021年办法（征求意见稿）》第5条规定，数据处理者在向境外提供数据前，应事先开展数据出境风险自评估，**即明确规定了所有数据处理者无论是关键信息基础设施运营者或一般网络运营者，其所处理的数据类型无论是国家核心数据、重要数据或一般数据（包括个人信息与非个人信息），均应当在数据出境前进行风险自评估。**

根据《2021年办法（征求意见稿）》第5条的规定，企业在进行风险自评估时应关注以下要点：

- 数据出境及境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；
- 出境数据的数量、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；
- 数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损等风险；
- 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；
- 数据出境和再转移后泄露、毁损、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等；
- 与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务。

此处需要提醒企业注意的是，上文最后一个评估项“境外接收方订立的数据出境相关合同”并不完全等同于《个人信息保护法》第38条规定的“按照国家网信部门制定的标准合同”，其包括但不限于后续网信部门拟颁布的标准合同模板。在标准合同尚未公布的现阶段，企业仍应履行上述义务。在与境外接收方订立合同时，数据处理者可以参考《2021年办法（征求意见稿）》第九条的规定对数据安全保护责任义务进行明确约定，以确保符合评估要求，具体如下所示：

- 数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；
- 数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者合同终止后出境数据的处理措施；
- 限制境外接收方将出境数据再转移给其他组织、个人的约束条款；
- 境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区法律环境发生变化导致难以保障数据安全时，应当采取的安全措施；
- 违反数据安全保护义务的违约责任和具有约束力且可执行的争议解决条款；
- 发生数据泄露等风险时，妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道。

在风险自评估后，参照《个人信息保护法》第56条以及《2021年办法（征求意见稿）》第6条的规定，企业应当形成《数据出境风险自评估报告》并至少留存三年，以满足留存评估记录或进一步申请进行安全评估的要求。

（二）数据出境安全评估义务

如上文梳理图所示，《网络安全法》《数据安全法》与《个人信息保护法》均规定了数据出境安全评估的要求。本次出台的《2021年办法（征求意见稿）》也是在这三部法律的基础上，填补了此前留待进一步解释的空白地带。因此，在分析《2021年办法（征求意见稿）》中有关数据处理者的数据出境安全评估义务时，需要同时参照《网络安全法》《数据安全法》与《个人信息保护法》这三部上位法的相关规定：

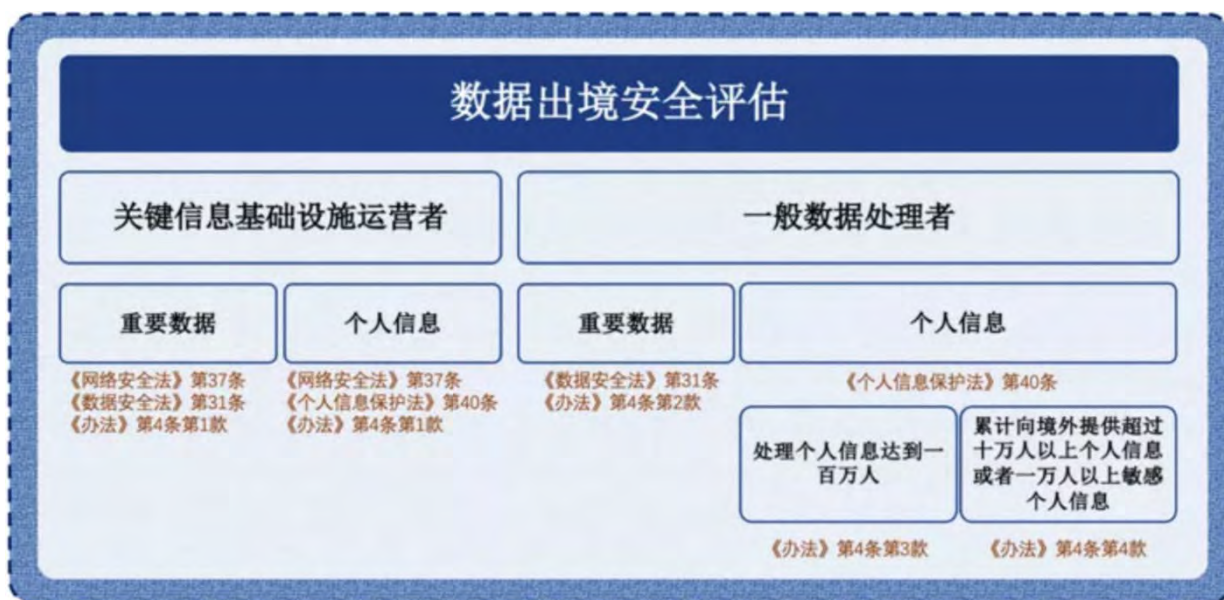
《网络安全法》第37条规定了关键信息基础设施运营者向境外提供在中国境内收集和产生的个人信息和重要数据时，应当进行安全评估。

《数据安全法》侧重规定了重要数据的数据出境安全评估制度，即第31条提到的关键信息基础设施运营者在中国境内收集和产生的重要数据的数据出境适用于《网络安全法》的规定，其他数据处理者在中国境内收集和产生的重要数据的数据出境适用于国家网信部门制定的要求。

《个人信息保护法》第40条规定了，关键信息基础设施运营者和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进行数据出境活动时，应当事先通过国家网信部门组织的安全评估。

总体而言，结合《2021年办法（征求意见稿）》第4条的规定，需要进行数据出境安全评估的主体包括：（1）向境外提供重要数据的所有数据处理者（包括关键信息基础设施运营者与一般数据处理者）；及（2）向境外提供个人信息的关键信息基础设施运营者以及处理数量达到《2021年办法（征求意见稿）》第4条第3、4款规定的一般数据处理者。

具体如下图所示：



若满足上述条件，则企业应该履行数据出境安全评估义务，向所在地省级网信部门向国家网信部门申报数据出境安全评估。根据《2021年办法（征求意见稿）》第8条，安全评估的内容与数据出境风险自评估的内容虽有重合之处，但前者的范围大于后者，即也是符合一般企业在完成自评估后再向国家监管部门履行申报数据出境的安全评估义务。监管机构的安全评估不仅会审查双方合同中对境外接收方义务的约定，而且会更加全方位地审查数据出境活动对于国家以及行业的整体风险系数与其所采取的相应安全保障措施，包括数据处理者对境外接收方的选择是否妥当，是否采取有效的数据安全保护措施、数据安全与个人信息主体的权益是否得到保障以及是否为违反了其他法律法规的要求。

具体而言，安全评估共包括以下七大方面：

- 数据出境的目的、范围、方式等的合法性、正当性、必要性；
- 境外接收方所在国家或者地区的数据安全保护政策法规及网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规规定和强制性国家标准的要求；
- 出境数据的数量、范围、种类、敏感程度，出境中和出境后泄露、篡改、丢失、破坏、转移或者被非法获取、非法利用等风险；
- 数据安全和个人信息权益是否能够得到充分有效保障；
- 数据处理者与境外接收方订立的合同中是否充分约定了数据安全保护责任义务；
- 遵守中国法律、行政法规、部门规章情况；
- 国家网信部门认为需要评估的其他事项。

针对以上评估项，笔者建议若企业的日常经营活动确有数据出境的需要，则应当根据法律法规要求，提前做好合规准备。例如：

- 制定内部数据管理制度和操作规程，对数据实行分类分级管理，根据法律法规要求划分允许出境的数据范围；
- 针对部分需要满足本地化存储要求的数据，如地图数据、人口健康信息、金融信息等，应存储在境内或在完成匿名化后向境外提供；
- 针对未禁止出境的数据，建议制定数据出境安全操作规范指引，明确企业员工进行数据出境活动时遵守的基本原则、操作流程、禁止出境的数据范围、与境外接收方的合同要求、安全自评估流程等等；
- 尽量选择所在国家当地数据保护法律较为完善的境外接收方，如欧盟、英国、日本、韩国、美国加州等；
- 在与境外接收方签署合同时，应当明确双方的权利义务，确保接收方采取了充分的数据安全保护措施，并提供了实现个人信息权益的有效途径等。

根据《2021年办法（征求意见稿）》第6、10与12条的规定，数据处理者申报数据出境安全评估时，应当提交的材料包括申报书、数据出境风险自评估报告、数据处理者与境外接收方拟订立的合同或者其他具有法律效力的文件以及安全评估工作需要的其他材料。国家网信部门会在收到申报材料之日起七个工作日内，确定是否受理评估并书面反馈受理结果。国家网信部门在确认受理后，会组织行业主管部门、国务院有关部门、省级网信部门、专门机构等共同进行安全评估。一般情况下，最终的评估结果会在六十日内以书面通知的形式反馈数据处理者。**数据出境评估结果的有效期为2年。若有效期届满，数据处理者需要继续开展原数据出境活动的，应当在有效期届满六十日前重新申报评估。**



但请企业特别注意的是，在收到评估结果后，若此前被评估的事项发生改变需要重新申报安全评估。如：

- 向境外提供数据的目的、方式、范围和类型发生变化；
- 境外接收方处理数据的用途、方式发生变化；
- 延长个人信息和重要数据境外保存期限；
- 境外接收方所在国家或者地区法律环境发生变化；
- 数据处理者或者境外接收方实际控制权发生变化；
- 数据处理者与境外接收方合同变更等可能影响出境数据安全的情况。

也因此，企业应当注意在数据出境活动时，严格遵守申报时的数据处理目的、方式等。同时，在与境外接收方的合同中明确接收方的如下义务：在处理数据的用途、方式发生变化或者接收方所在国家数据保护相关法律发生可能影响数据处理活动安全的变更时，应及时告知企业并确保采取达到境内法律要求同等水平的保护措施。

五、违反数据出境评估义务的法律责任

目前《2021年办法（征求意见稿）》尚未规定详细的违规责任与惩罚措施，根据《2021年办法（征求意见稿）》第十七条的规定，若违反《2021年办法（征求意见稿）》中的相应规定，则将按照《网络安全法》《数据安全法》《个人信息保护法》进行处理。同时，若数据处理者构成犯罪的，将依法追究刑事责任。以《个人信息保护法》第66条之规定为例，若企业违法处理个人信息，例如未在出境前进行安全评估，则可能面临最高五千万元以下或者上一年度营业额百分之五以下罚款、停业整顿、吊销相关业务许可或者吊销营业执照等严厉的处罚措施；同时，针对直接负责的主管人员和其他直接责任人员，也有可能被处以十万元以上一百万元以下罚款，并在一定期限内禁止担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

由此可见，在《数据安全法》《个人信息保护法》相继生效之际，企业应当更加重视数据出境合规问题，根据法律法规的要求及时履行相关义务，在日常运营中及时梳理数据出境场景并完成风险自评估，依法向网信部门申请进行数据出境安全评估，树立守法合规的企业形象，以避免违法数据出境活动带来的法律责任与负面影响。

苹果将实施史上最严厉隐私保护要求， 定向广告的严冬真的来了？

环球律师事务所
孟洁 | 张淑怡

APPLE CHALLENGED
THE GLOBAL
MOBILE ADVERTISING
INDUSTRY



一、iOS 14：隐私保护的重磅炸弹

2020年6月22日，苹果召开2020年全球软件开发者年会（WWDC2020）。会上，苹果发布了其用于iPhone的新一代操作系统iOS 14、用于iPad的iPadOS 14以及用于Mac系列电脑的macOS 11。在iOS 14与iPadOS 14当中，苹果引入了模糊定位、相册读取范围限制等措施对用户隐私进行保护。而自iOS 14.3、iPadOS 14.3、macOS 11.1起，苹果还要求软件及App开发者在App Store中向用户描述其可能读取或收集的数据种类。可以说，在苹果今年发布的操作系统中，对用户的隐私保护是重中之重。以上措施既能够在一定程度上保护用户隐私，又不会严重影响开发者和广告商的工作及利益。然而，在iOS 14与iPadOS 14中，苹果还推出了一个“杀手锏”级别的、史上最为严厉的措施：征求跟踪许可。

UDID（唯一设备识别码）是苹果iOS或iPadOS设备不可变更的唯一识别码，其作用类似于IMEI，即用于确定特定的设备。UDID曾被收集以用于广告追踪。但由于UDID的敏感性与隐私性，从2013年开始苹果禁止了开发者对UDID的直接收集，并于同年推出了IDFA（广告标识符）作为替代品。从iOS 10开始，用户可以通过“设置”中的跟踪功能对本机的IDFA进行开启或关闭。每台iPhone或iPad的IDFA都是不变且唯一的，开发者与广告商可以通过IDFA对用户进行个性化广告推广与跨应用追踪。但如果用户关闭了广告追踪，广告商就只能收到一串毫无意义的0。然而，这一开关在设置中较难找到，且系统不会主动提示，所以很少有用户会主动关闭。根据Adjust在2016年10月进行的调查显示，中国大陆地区仅有11%的用户选择主动阻止对IDFA的收集。然而在iOS 14与iPadOS 14中，苹果开始强制要求所有App在收集IDFA用于广告追踪前单独弹窗告知用户，征求用户对于广告追踪的许可，用户可以允许或拒绝不同App对IDFA的收集。

征求跟踪许可的措施将原本隐藏于后台的IDFA与广告追踪设置推到了前台，不仅让更多用户了解广告追踪的存在，也让用户全面掌握了这一权限的“生杀大权”，相当于阻断了原来“默认开启”的追踪功能。众多分析均认为，该措施会引起用户对自身隐私与信息安全的关注，许多用户可能会选择拒绝广告追踪，避免出现“在某社交App中与朋友聊天时提到某商品，某购物App就马上开始推荐该商品”的情况出现。一旦App无法进行追踪、无法获取IDFA，广告商就无法针对用户推送特定的广告，大大降低广告推送的效率，精准营销、归因监测等目前广告业常用的推广方式将面临重大危机。苹果无疑是向App开发者与广告商扔下了一枚重磅炸弹，海外某媒体甚至戏称“这可能代表着价值超千亿美元产业（即广告业）的彻底完结”。而谷歌也已在2019年推出的Android 10中正式限制非系统级App对于IMEI等信息的读取，且较有可能跟进苹果的步伐，在未来进一步采取措施要求App在进行广告追踪前征求用户同意。

iOS与安卓两大移动端操作系统占领了全球超90%的市场份额，如果苹果和谷歌均采取措施在系统层面上阻断默认开启广告跟踪的功能，全球的广告商无疑都会受到重大冲击。寻找IDFA以及系统层面的广告追踪的替代方案迫在眉睫，也是App开发者以及广告商破除当前困局的重要途径。截止至目前，国内外众多企业与组织已经提出了数个用于替代IDFA的方案。

二、国内外替代方案

苹果原计划于2020年9月iOS 14正式版发布后即启用“征求跟踪许可”的措施，但考虑到这一措施的重大影响，苹果将其推迟至2021年初才开始实施，给予各开发者与广告商时间对新措施进行适配，目前公开可查的替代方案主要有以下几种：

1. 国内方案

在国内，很多移动智能终端设备厂商已经开始试行在其生态内开放基于不同功能，但能够由用户进行重置的设备ID。

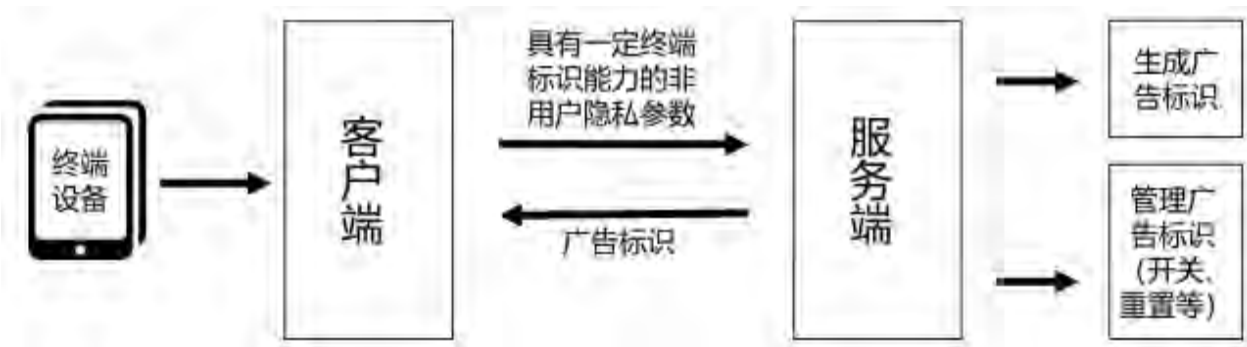
1) OAID

2019年9月，谷歌正式发布Android 10系统。在该版本系统中，谷歌禁止了非系统级App对于原生设备识别码（即IMEI与Device ID）的读取，同时将MAC地址随机化，导致开发者与广告商无法使用识别码和MAC地址对用户进行广告追踪。因此，国内中国信通院通过移动安全联盟联合小米、华为、OPPO、vivo等终端厂商起草了《移动智能终端补充设备标识规范》，其中规定了设备唯一标识符、匿名设备标识符、开发者匿名设备标识符和应用匿名设备标识符这四个设备标识符，以共同构成补充设备标识体系。其中匿名设备标识符，即Open Anonymous Device Identifier（以下简称“OAID”），可以连接所有应用数据的标识符，在移动智能终端系统首次启动后立即生成，生成参数中可包含设备唯一标识符等参数，从而可以链接所有的应用数据。但目前OAID仍处于试用阶段，存在着诸多问题，例如缺失各主体之间对OAID互相识别、配对的机制。这对通过OAID进行精准广告推送业务的开展带来极大困难，广告需求方平台、广告媒体方以及广告联盟均难以拿出客观的监测数据向广告主证明广告点击率高、广告位具有较高的流量与吸引力或广告投放效果较好。因此，有一些公司拟通过软件或用户行为自研设备ID，并与OAID融合后进行相关用户的标签制作；将自研设备ID或OAID提供给如监测机构、广告主和其他合作伙伴等第三方（以下简称“第三方合作方”）来计算广告点击率、曝光量、监测、评估广告效果等，以方便与广告主进行结算费用；或从第三方合作方获取OAID。然而，由于企业制作自研设备ID、拟向第三方合作方提供自研设备ID或OAID的行为和/或从第三方合作方获取OAID的行为，如在不具备充分的前置合规措施时（例如告知并征得用户的同意、与第三方合作方签署安全条款和事中事后的审计监督机制等），也会存在较高的合规风险。

2) CAID

中国广告协会（以下简称“中广协”）互联网广告标识，即CAA Advertising ID（以下简称“CAID”），是中广协与中国信息通信研究院联合研究机构、广告产业链各方提出的广告标识方案。目前，CAID正处于设计与测试阶段，假以时日会正式推广。根据中广协公开的信息显示，CAID的运作机制为：App收集设备非隐私参数后发送至广告标识管理中心，广告标识管理中心通过算法进行计算加密，计算加密后生成统一的广告标识符（CAID）以供使用。在一段时间内，同一个设备上不同时间获取到的设备标识ID保持一致，不同设备上获取到的设备标识ID不相同，以达到阶段性唯一，但生成CAID的算法会遵守保密原则并定期更新，以保证匿名性与强对抗性，避免被逆向破解。同时，CAID会设置相应机制，令用户可以便捷地对CAID进行开启、关闭或重置，以充分尊重用户的知情权与选择权，保障用户设备、个人数据的安全以及隐私，也令CAID的设计符合法律法规与国家标准的要求。同时，CAID方案通过自建服务器、提供SDK或API两种方案供广告运营者使用CAID的服务，在保障用户数据与隐私安全的同时，也能充分保障广告产业的利益。

CAID技术框架*



*援引自GA小站

2. 国外方案

除国内企业厂商外，海外企业与厂商也受到了苹果新政策的冲击。其中，脸书（Facebook）对于苹果的新政策提出了尖锐而严厉的批评，指责其政策“损害了中小企业的利益”。为了应对苹果的新政策，Facebook于2020年10月宣布其名为Audience Network的广告系统在iOS上将从2021年第二季度开始全面采用竞价模式，即由广告商竞拍获得广告投放机会，而抛弃通过获取用户设备信息而进行广告追踪的精准投放模式。在其官方公告中，Facebook称根据其今年所采取的试点研究，竞价模式能够帮助广告商最大程度地改善变现率和转化率，广告商的平均收益有所上涨、用于广告运营的时间花费则有所下降。^[1]但值得注意的是，目前Facebook以及其他美国大型互联网企业仍未对外公开宣布自行开发广告追踪系统或IDFA替代方案的计划。

在宣布实施“征求跟踪许可”的措施后，苹果自身也推出了一些方案，供开发者与广告商顺利衔接该措施。苹果自身提供的方案主要包括两类：一是 SKAdNetwork、二是ATT。SKAdNetwork是苹果官方推出的、让广告平台在不获取IDFA的前提下对用户的点击和安装行为提供的一套追踪解决方案，开发者需要在苹果官方处注册后才能使用该方案。通过SKAdNetwork，广告商可以对用户的点击与安装行为进行追踪，但其能够获得的数据种类则被大幅度缩减，仅能获取App安装时间、广告组、具体的广告，以及运营商等非常有限的信息。该方案在2018年iOS 11.3发布时即已被苹果推出，在iOS 14发布后，苹果推出了其2.0版本，对其进行了优化。在刚推出之时，由于其功能的限制，SKAdNetwork注册数量非常少。但随着iOS 14中有关限制广告追踪政策正式实施的临近，可以预见到这一方案的注册量会大幅提升。ATT全称则为AppTrackingTransparency，是Apple官方配合SKAdNetwork 2.0版本推出的、用于触发向用户展示IDFA同意提示的API。开发者可以通过在App中集成这一API来取得用户的授权同意，以继续使用IDFA。

由于苹果官方推出的解决措施大幅削弱了广告追踪的能力，这些措施并不会成为开发者与广告商的主流选择。但在具有广泛实施可能性的替代方案出现前，这些官方解决措施可以缓解企业的燃眉之急，并起到一定的过渡作用。例如，谷歌公司就计划在自己开发的App中采用ATT方案。从这些官方替代方案中，我们一定程度上也可以观察到苹果官方对于“后IDFA时代”广告追踪的态度，从而协助开发者与广告商及时调整自己的策略。

三、现有替代方案情况分析

首先需要说明的是，目前苹果仍未公开对其他公司、广告商开发的IDFA替代方案发表评论或任何意见。部分大型企业、设备厂商或第三方组织可能正在与苹果进行沟通，希望了解其对于替代方案的官方态度。但不能排除的是，苹果公司在了解到业界可能推出的其他替代广告追踪方案后，可能会发布新的要求禁止此类的广告追踪方案的使用，并采取类似于在App Store下架等强制措施（例如，在苹果近日发布的新隐私功能中，要求App说明收集使用用户数据的目的，尤其是这些数据是否用于广告追踪等，包括需要说明App中整合的第三方工具或SDK是否将数据用于追踪的情况。苹果的专门团队将以人机结合的方式进行不定期抽查审核，未能满足要求的，将会从App Store中移除，严重的会注销开发者账户）。

1. 自研替代方案

目前，国内外多个互联网企业、终端设备厂商均在自行研发对IDFA的替代方案。这些替代方案既包括以Facebook为例的、采取其他方式完全替代广告追踪的方案，也包括自行研发标识符体系方案，以保证未来可以继续广告追踪以及精准投放。毫无疑问的是，自研替代方案可以让互联网企业与设备厂商对产品上的广告追踪与隐私保护掌握全面的话语权，也能够让企业与厂商在符合法律法规、国家标准规定的前提下，建立一套为自己所控制的广告追踪与隐私保护体系，从而可以摆脱苹果的严苛政策。

尽管自研替代方案有如此巨大的优点，但其短板也是显而易见的：自研替代方案由各家企业与厂商自行研发、或少数几个企业厂商间联合研发，这将不可避免地导致各个方案之间的割裂。由于IDFA在iOS系统中的普适性，即在所有App都可以对其进行利用，这使得开发者与广告商可以利用其做到跨应用的广告追踪与精准投放。但对于IDFA的自研替代方案基本仅适用于本企业的产品，虽然开发者与广告商仍能进行广告追踪，但跨应用（特别是跨不同企业的应用）的广告追踪与精准投放则会变得较为困难。如果开发者或广告商决定学习Facebook，自行研制并使用竞价等非广告追踪方式进行未来的广告投放，则可能需要将过去基于广告追踪建立的广告投放体系全部推倒重建。此方案虽会降低个人信息与隐私保护所带来的合规法律风险（因为这些方式不会涉及对用户的数据与行为进行追踪），但根据Facebook的报告显示，经过其试验，采用竞价方式进行的广告投放能在一定程度上失去了追踪与精准投放的广告的价值。当然上述观点目前仍未有定论。

同时，苹果作为业内最为强调隐私保护的企业之一，其一直致力于遵守各国及各地区的个人信息保护法律法规。在采用IDFA时，开发者和广告商基本可以确保对于法律法规的遵守。但在设计自研方案时，企业和厂商需要特别注意对于法律法规、国家标准的遵守，严格依照法律法规与国家标准的規定对方案进行设计，以达到对个人信息与隐私保护的合规。如果企业或厂商在自研替代方案中因故意或过失而没有遵守相关要求，则可能产生合规问题，乃至需要受到处罚、承担法律责任。

2. 第三方替代方案

除各个企业与厂商自行研制的替代方案外，国内也有非企业、厂商的第三方在研制替代方案。我们上文所介绍的OAID与CAID两个替代方案均属于本部分所述的第三方替代方案。第三方替代方案的优点也十分的显著：由于主导者非企业厂商自身，第三方的参与能协助打通企业厂商之间的壁垒，使得第三方替代方案成为可适用于全国各企业各厂商的通用方案。但第三方替代方案也有着自己的缺点与困难之处。这些缺点与困难最为明显的一点在于，开发替代方案的第三方自身需要具有较强的号召力，以吸引开发者、企业与设备厂商采用其开发的方案。只有当数量足够庞大的开发者、企业和厂商选择采用其方案后，方案才能具有通用性，才能打通平台、软件、设备之间的壁垒。因此，第三方应当如何推广自己的方案，真正打造一个通用方案，成为了这一方面最为重要的问题。其次，如果开发者或企业选择使用了第三方方案，可能会面临需要将收集到的用户数据与该第三方共享、委托给该第三方进行处理的问题。根据我国法律法规与国家标准的规定，如果控制者需要将自己收集到的数据与第三方进行共享、委托给第三方进行处理，则可能面临着较为严格的共享、委托标准以及传输、合规等方面的要求。如无法遵守这些标准及要求，开发者或企业就可能面临着合规与监管问题。如果开发者或企业最终决定选择第三方替代方案，则必须制定严格的用户数据保护内部指引，同时与第三方签订严格的合作协议或合同，以充分保护用户的数据安全，并使数据的使用、共享与委托处理符合法律法规、国家标准的要求。此外，我们还建议开发者或企业在使用第三方替代方案时，对其进行监测、扫描，以保证第三方替代方案的功能以及所收集使用的个人信息的合规性。



四、企业合规注意事项

本次苹果在最新版本的iOS与iPadOS系统中的隐私政策调整给移动设备中的广告投放与追踪带来了巨大的冲击。各个企业与厂商需要对自己的广告政策与投放策略进行较大规模的调整，以适应新的变化。在调整过程中，无论是选择根据苹果的新政策继续使用IDFA，还是选择自研、第三方的替代方案，企业厂商都需要注意遵守各类法律法规、国家标准乃至苹果公司自身的新隐私政策要求。以下是我们经过分析后给出的一些合规注意事项以及建议，供大家参考。

1. 应对苹果新政：隐私政策和PbD设计

正如上文所述，iOS 14、iPadOS 14以及macOS 11 Big Sur中最为巨大的隐私政策变化主要集中于两点：一是要求App开发者在App Store中向用户展示“App营养成分标签”，在其中披露App可能会收集的一切信息类型（该功能并未随iOS 14/iPadOS 14/macOS 11正式版推出，但在最近的iOS 14.3/iPadOS 14.3/macOS 11.1更新中正式上线）；二是将用户对于IDFA的使用授权由设备系统层面调整到了单个App层面，用户将被赋予针对单个App授予或拒绝IDFA使用权的权利。对于这两个最为重要的变化，我们建议企业与厂商采取以下措施，以保证符合苹果公司政策以及法律法规、国家标准的要求。

1) 保证App的隐私政策得到更新，与App Store的披露信息一致

自iOS 14.3、iPadOS 14.3以及macOS 11.1更新发布起，苹果要求开发者在App Store中披露App所收集的信息类型，但苹果并未对App自身所使用的隐私政策作出任何内容上的要求。尽管如此，苹果仍然要求开发者在App Store的页面中以及App内提供指向隐私政策的链接，以保证用户可以获取App最为全面的隐私与数据保护政策。

我们在此建议开发者与各个企业利用这一机会，对App的隐私政策文件进行全面的审阅检查，并进行适当的修改。最为重要的一点在于，开发者与企业需要确保其在App Store页面中所披露的隐私相关内容与隐私政策中所描述的内容相一致。如果App的隐私政策未得到及时的检查更新，且被发现与App Store中披露内容不一致，苹果在接到举报后非常有可能对该App作出下架处理，给开发者与企业造成不必要的损失。除此之外，这种情况还可能被视为开发者或企业故意隐瞒App实际收集的信息种类，从而构成对消费者的欺诈，违反《消费者权益保护法》、《网络安全法》等法律法规或相关国家标准的要求，受到市场监管部门或网安部门的处罚。

2) 根据IDFA新政策做好相关的默认隐私设计 (PbD)

全国信息安全标准化技术委员会于2019年6月25日发布了《个人信息安全工程指南》（以下简称“指南”）。该《指南》参考了《通用数据保护条例》对于默认隐私设计的要求，以及欧盟网络与信息安全局（ENISA）发布的相关标准，并为开发者和企业进行默认隐私设计提供了参考标准。总体而言，《指南》为默认隐私设计提供了八个策略：最小化、隐藏、隔离、聚集、通知、控制、强制与证明。根据苹果的新政策，App在使用IDFA前，需要通过ATT进行弹窗提示，并获得用户的同意，这与上述“最小化”策略相关。由于苹果并未要求App一定要在用户初次使用时就弹窗提示，我们建议企业对此进行一定的研究与调查，选择一个最佳时间弹窗提示用户、请求用户对于IDFA使用的授权（例如，开发者可以试着在一开始向用户展示非定向的广告，展示一定时间后，再弹窗请求IDFA的使用授权）。这不仅能够使App符合法律法规、国家标准的要求，也能符合苹果政策、令开发者与广告商的利益最大化。

2. 收集数据：限制使用目的

正如我们上文所述，目前我国绝大多数已初步成型、使用自建标识符作为广告追踪方式的IDFA（或IMEI等设备标识符）替代方案都涉及到了对用户数据的收集。由于无论是苹果的iOS还是谷歌的Android在最新的版本中都已经斩断了App对于IMEI、UDID、MAC地址等设备原生标识符的读取收集渠道，自建标识符的替代方案均开始转向收集其他非高度敏感、但具有特定性的设备与用户数据，以建立自己的标识符。这些“非高度敏感、但具有特定性”的数据包括用户的设备型号、系统版本、系统语言、时区设置等。虽然这些数据并没有IMEI、UDID等数据那么高度敏感，但不可否认的是，他们也可以被用于多种用途。而我国的法律法规、国家标准也明确规定了不得将收集的数据用于与收集目的不一致的其他用途。

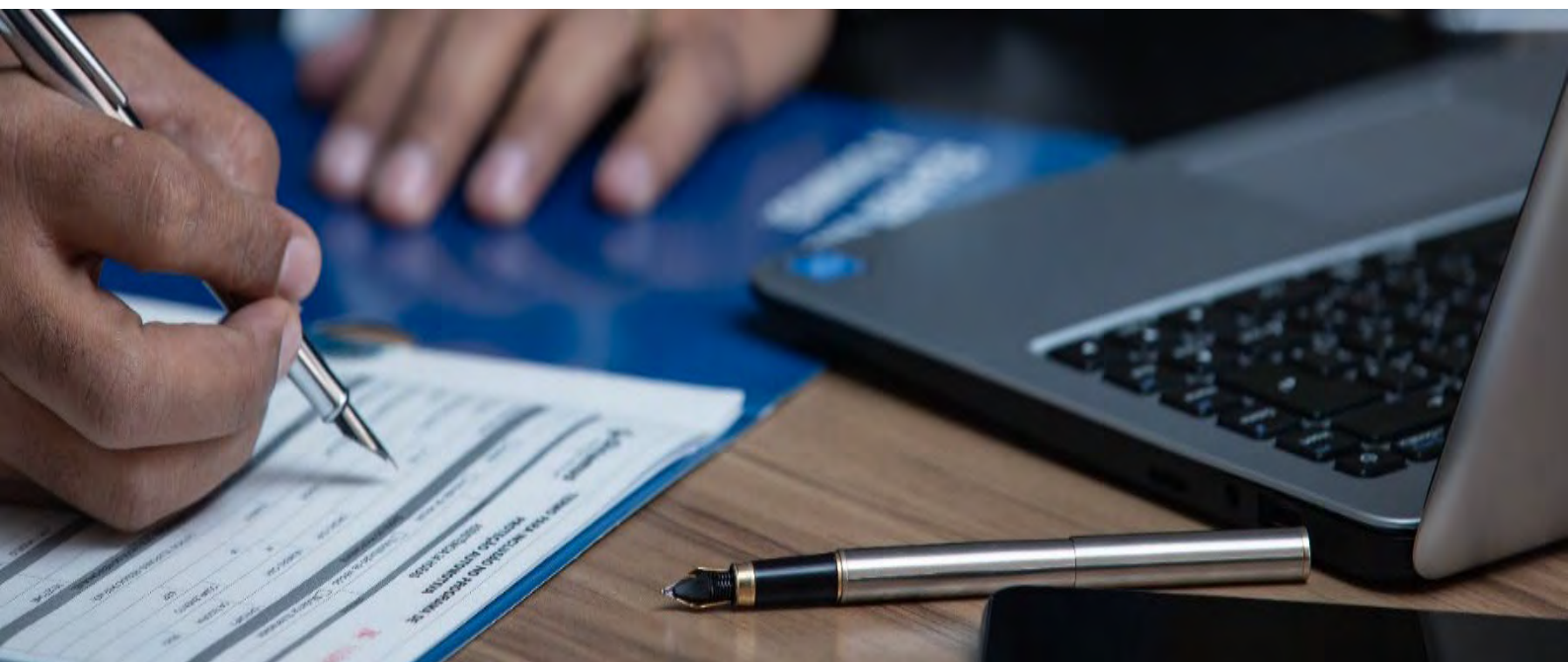
因此，如果企业厂商准备自行研制标识符替代方案，且该替代方案涉及收集用户与设备数据，则其必须确保被收集的数据仅用于生成广告ID等标识符，而不能被用于任何其他用途。第三方机构在研发替代方案时，也需要注意不能随意使用收集的数据。开发者或企业如需使用第三方的方案，建议事先通过合同或协议约定双方权利与义务，从合同层面上禁止第三方服务提供方在收集用户数据后将用户数据挪作他用。如有条件，我们还建议开发者或企业对第三方服务商提供的方案进行安全扫描等检查措施，防止第三方服务商擅自将数据挪作他用。

3. 做好数据流转的进出口管理

数据流转的出口是指将个人数据共享给第三方、或委托给第三方进行处理，在本文语境下是指将用户数据收集后发给第三方以供第三方生成标识符（广告ID）；数据流转的入口是指从第三方处获取个人数据，在本文语境下这指的就是获取第三方根据用户数据生成的标识符（广告ID）。目前，我国包括《个人信息安全规范》、《互联网个人信息安全保护指南》在内的多个国家标准均对个人数据与信息的共享和委托处理作出了较为严格的规定。

我们理解，不是所有开发者与企业都有能力自行研制并部署IDFA替代方案，自研方案也不一定是最具有经济效益、最具有效率的方案，其缺点也十分明显。诸多企业也许都会选择第三方替代方案供自己使用。在这种情况下，开发者和企业需要与第三方共享其通过App收集到的用户数据、或委托其处理这些用户数据，以生成标识符（广告ID）。在进行这些委托与共享时，我们建议双方以合同的形式明确约定委托处理、共享的权利与义务，对双方形成约束，以使数据的委托处理与共享符合国家标准的规定。如部分开发者或企业对于用户数据保护有较高的要求，不愿将用户数据委托或共享给第三方进行处理，但同时必须需要使用第三方方案的，我们建议开发者、企业可以和第三方进行联合，让第三方服务商将用于生成标识符的算法布署到开发者或企业的自有服务器环境中，实现数据的本地化处理以及标识符生成的本地化，最大程度地避免数据的共享。

在数据入口方面，我们则建议开发者、企业与第三方根据国家标准与法律法规的要求，在数据传输过程中采取加密措施、避免遭到破解。同时，第三方在生成标识符的过程中，应当采取不可逆的加密算法，避免他人得到标识符（广告ID）后，能够逆向破解推出原有用户数据，造成用户数据与隐私泄露。



4. 数据主体的权利：退出权与及时响应

根据我国法律法规与国家标准的规定，数据主体有退出权，即有选择不再允许自己的数据被收集以及被处理的权利。无论开发者与企业是选择使用苹果官方提出的IDFA新政策，还是自研或使用第三方的替代方案，都会涉及到对于用户数据的收集与处理。因此，开发者与企业需要采取充分的措施，保障数据主体的退出权。具体而言，我们对开发者与企业提供如下建议。

如开发者或企业选择使用苹果官方的IDFA新政策，我们建议其在App中应当以弹窗或其他显著的形式向用户展示说明IDFA的作用、对IDFA进行授权的后果、以及如何在系统设置中关闭IDFA授权的指引。在用户选择关闭IDFA的授权后，开发者或企业应当立即将用户的IDFA进行删除或进行匿名化处理、并停止利用IDFA为用户提供广告服务。

如开发者或企业选择使用自研或第三方替代方案，则需要自行或根据第三方的要求，向用户提供退出方案。例如，在App的隐私设置中加入供用户选择开启或关闭自研或第三方标识符系统的开关。如果第三方标识符替代方案提供了单独的App供用户对标识符相关信息的收集进行控制，则建议开发者或企业在App隐私设置中的显著位置对用户作出指引，提醒用户下载第三方提供的用于统一关闭广告标识符的App（以下简称“第三方App”），并通过第三方App对个人信息进行控制，并提示其随时可以通过该第三方App选择退出数据收集与处理。

在用户通过App自带隐私设置或第三方App选择不再让自己的数据被收集且接受处理后，开发者和企业也必须立即停止收集处理用户数据、对已收集的用户数据进行删除或不可逆的匿名化处理、并立即停止使用已生成的标识符且将其删除。需要注意的是，如果第三方替代方案提供者为自己的替代方案提供了单独的App进行控制，根据第三方提供者所使用的机制不同，可能涉及到数据收集处理的“全开”或“全关”问题，即一旦用户在第三方App中选择退出信息收集处理，则手机上所有使用该第三方方案的App均会无法使用该第三方方案。例如某购物App使用了第三方的方案，且该第三方有专门的App用于控制个人信息的收集，如果用户不希望该购物App收集自己的信息用于生成标识符，则可以前往第三方的专门App中关闭了信息收集选项，则该用户设备中安装的所有其他使用该第三方方案的其他App有可能也无法再收集任何信息。因此，在选择使用第三方方案时，我们建议开发者和企业详细了解各种方案的机制与特征，选择最适合自己的方案。

根据《个人信息保护法》以及国家标准《信息安全技术 个人信息安全规范》的规定，数据主体还拥有包括数据可携权在内的多项权利。例如，数据主体有权了解开发者和企业收集其个人数据的目的、收集其个人数据的具体内容以及数量。为了保障数据主体的权利，我们建议开发者在隐私协议中以显著的方式对相关内容进行说明。但我们也理解一份隐私政策无法对所有与主体权利相关的内容进行全面、毫无遗漏的覆盖。因此，我们也建议开发者或企业建立一套自己的数据主体权利响应机制，为数据主体提供数据保护与合规部门的联系方式，以供数据主体在有实现自身权利的需要时，能够及时联系相应的人员，以获取保障。同时，开发者或企业还需要明确协助数据主体实现自身权利的时长限制与具体方案。例如，根据《App违法违规收集使用个人信息行为认定方法》对于App端，需要在15个工作日内完成对用户的更正、删除、注销请求、投诉举报的核查和处理。

5. 后台机制的完善：存储安全与保密

无论是开发者和企业决定继续使用苹果官方提供的IDFA替代方案，还是使用自行研制或第三方的标识符替代方案，都会涉及到对个人信息的收集、存储、使用等一系列过程。因此，在对这些信息进行收集、存储、使用乃至共享和委托处理时，企业需要保证自己有一套完善的内部管理与监督措施，以保障用户信息在这些过程中受到充分的保护。在上面几个部分中，我们已经谈到了如何收集用户的信息，并在用户选择退出时如何处理用户的信息。因此，在内部机制完善这一部分中，我们希望向企业给出有关数据信息存储、数据主体权利保障以及安全事件响应方面的建议。

在数据存储方面，如果开发者或企业选择使用自研或第三方的标识符，在此情况下，虽然开发者与企业可能存储的信息已不再是UDID和IMEI等高度敏感的数据，而是设备型号、系统版本、时区等看起来与无法直接与用户个人相联系的数据，但这并不代表着开发者与企业可以掉以轻心、不再注重数据的存储。单个来看，以上数据信息的确无法直接与特定的用户个人相联系，但一旦这些信息被组合起来，形成诸如“运行iOS 14.3系统，时区设置在北京，且工作时间地理位置常位于北京市朝阳区某写字楼的iPhone 12”这样的组合信息，识别出特定的用户个人并非完全不可能。因此，我们建议如果开发者或企业需要收集多种数据以供标识符的生成，则需要将这些数据分别存储在不同的数据库中并进行加密，尽最大努力避免单次数据安全事故造成相关联的数据一起泄露，使非法使用者可以通过相关联数据危害数据主体的个人信息安全。

虽然我们建议企业采取充分的安全措施，避免数据泄露等安全事故的出现，但我们明白，即使采取了百分之二百的安全措施，数据泄露等事故也并非能够完全被避免。在这种情况下，无论是自研广告标识符还是采用第三方方案，都建议通过相关设备所采集的参数进而形成的统一广告标识符对个人信息（特别是敏感个人信息）的依赖程度尽可能小，这样即使有泄露，风险也会较小；并且，建议对统一广告标识符设置成能够可变更和可重置的效果。另外，事故发生后的安全响应措施就显得尤为重要。因此，我们建议企业制定完备的安全响应预案，以便在发生安全事故后迅速通知受影响的主体以及相关政府部门，充分保障数据主体的权利，尽可能降低数据主体所遭受的损失，并符合监管合规要求。

6. 个人信息影响评估 (PIA)

目前而言，我国现行有效法律法规尚未强制要求开发者或企业进行数据保护影响评估。但为了在收集用户信息、生成广告标识符的过程中更好地保护用户的隐私与信息安全，我们仍然建议开发者与企业在条件允许的情况下进行数据保护影响评估。这一概念由欧盟《通用数据保护条例》（GDPR）所规定，并后续被欧盟成员国、英国等不同国家与地区采纳效仿。根据GDPR的定义，数据保护影响评估是指数据控制者对“可能会对自然人的权利和自由造成高风险”的操作进行的评估。在本文语境下，对设备用户数据的存储、与第三方的共享、委托第三方的数据处理都有可能对数据主体的权利造成较高风险。因此我们建议开发者或企业重点对此进行评估。

尽管我国现行法律法规没有规定企业有进行数据保护影响评估的法律义务，但国家标准文件《信息技术安全指南 个人信息安全影响评估》（GB-T 39335-2020）（以下简称为“标准”）为企业进行数据保护影响评估确立了标准，将PIA称为“个人信息安全影响评估”。根据该标准，“个人信息安全影响评估”是指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。企业或相应的组织需要制定评估的责任部门或责任人员，牵头的责任部门通常为法务部门、合规部门或信息安全部门。

企业或组织可根据其需求组织进行个人信息安全影响评估。该评估可被用于合规差距分析，协助企业或组织找出其目前政策及机制与法律法规、国家标准的差距之处。企业或组织也可以在达到合规的基础上，进行评估，以进一步提升自身安全风险管理能力和安全水平目的。在这种情况下，企业或组织是否启动评估，取决于其个人信息安全目标与实际需求。其中，合规差距评估的应用场景包括新服务、新产品的的设计阶段与上线初次评估。鉴于广告追踪替代方案的设计与使用完全可被视为新产品、新服务的设计与使用，我们建议开发者、企业或第三方方案提供者在替代方案的设计阶段与上线初期均开展评估，尽最大可能保证替代方案的合规性，并保证用户的隐私和个人数据安全。即使开发者或企业决定直接采用苹果公司官方提供的替代方案，亦建议开展评估。

在进行评估的前期准备后，我们建议开发者、企业或第三方采取以下步骤进行评估：数据映射分析、风险源识别、个人权益影响分析、安全风险综合分析。完成上述步骤后，评估方应当完成评估报告，标明存在的风险、确定如何处置及改进。

【总结】

本文对苹果在iOS 14以及iPadOS 14中推出的新广告追踪政策进行了简要介绍，并作出了简单分析，为企业提出了合规建议。苹果公司的新政策与措施代表新的发展方向。在未来，各大科技企业、设备厂商以及互联网企业对个人信息以及隐私的保护力度将会逐步加大。而在合规方面，我国《个人信息保护法》（草案）已提交全国人大常委会审议，各类国家标准、团体标准也在不断推出、征求意见之中。进一步加强对于隐私的保护、在网络以及App中减少对个人信息的追踪是大势所趋。我们建议企业关注这一方面的发展趋势，并起草实施更为严格的方案、政策与措施，以做到合规。

注释：

[1]<https://www.facebook.com/audiencenetwork/news-and-insights/audience-network-to-become-bidding-only-beginning-with-ios-in-2021/?filter=blog>



算法相关新型垄断模式的法律风险

环球律师事务所
赵德铭 | 孟洁 | 杨卜 | 潘唯嘉 | 戴畅



【前言】

近年来，大数据、云计算、人工智能等技术工具深度运用于支付清算、借贷融资、财富管理、保险服务等领域，大幅提升了服务效率，但是利用大数据所“训练”出的算法植入在线服务领域，针对算法所描绘的消费者“画像”或者消费特征，自动生成不同的服务条件或者服务价格，形成基于算法的针对不同消费者的服务条件歧视或者价格歧视，俗称“大数据杀熟”，在特定条件下具有构成垄断并侵害个人权益的法律风险。

另外，如果两个及以上互联网平台共同利用算法达成协议或协同限定交易条件排除、限制竞争，则可能构成“算法合谋”从而受到反垄断规制。利用算法实施垄断的行为还包括互联网平台利用市场影响力迫使平台内经营者在该平台及其竞争平台之间“二选一”、“N选一”等模式。执法部门最近的动向

1. 2020年至2021年，多家从事金融业务并且在业内有影响力的网络平台企业为人民银行、银保监会、证监会、外汇局等金融管理部门所“联合约谈”，违规支付业务、不正当竞争等方面的问题，被责令整改；
2. 2021年2月7日，国务院反垄断委员会出台《关于平台经济领域的反垄断指南》，将平台经济领域特有的竞争行为纳入反垄断监管之下；
3. 2021年8月27日，国家互联网信息办公室（“网信办”）发布《互联网信息服务算法推荐管理规定（征求意见稿）》；
4. 2021年9月17日，九部委印发《关于加强互联网信息服务算法综合治理的指导意见》；
5. 2021年10月7日，央行行长易纲在国际清算银行（BIS）监管大型科技公司国际会议上，发表了关于《中国大型科技公司监管实践》的讲话，强调央行将在金融科技监管实践中发挥作用的同时，明确表示央行将与反垄断部门合力应对“算法歧视”等新型垄断问题；
6. 2021年10月19日，《中华人民共和国反垄断法（修正草案）》（以下简称“《反垄断法（修正草案）》”）在第十三届全国人大常委会第三十一次会议上送交初次审议，约束经营者滥用数据、算法、技术及资本优势、平台规则等排除、限制竞争的不当行为，主体并不仅限于平台经济和互联网方面的实体。

算法歧视等新型垄断问题已经成为反垄断监管部门与个人信息保护监管部门的新焦点，同时也成为各监管部门可能“综合治理”的问题。各类采取应用数据、算法等技术开展经营的企业（不限于互联网平台企业），需要及时做出积极合规的姿态。

一、算法相关新型垄断形式

（一）大数据杀熟

大数据“杀熟”，原一般是指互联网平台利用大数据收集、使用并形成用户画像，根据用户使用的设备、消费时所处场所、消费频率的不同而差别定价，通过该等价格歧视实现互联网平台自身利益最大化的行为。随着利用大数据的普及，现今越来越多利用大数据分析用户偏好并提供服务的各类商家也均存在涉及大数据“杀熟”行为的可能。举例而言，在某旅行App预定酒店时，对待老用户的房费明显高于新用户的房费；在某购票App上购买电影票时会员价高于非会员价；使用越贵的手机打车越容易被更贵的车型接单等等现象，都是当前大数据杀熟的具体体现。

需要注意的是，大数据杀熟行为不必然属于垄断行为，而是只有在一定条件下才会受到《中华人民共和国反垄断法》（以下简称“《反垄断法》”）的规制。根据《反垄断法》相关规定，当在相关市场具有市场支配地位的任何互联网平台企业以及平台内经营者采取的歧视性价格被认定为高于市场竞争价格时，则该“杀熟”行为可能被认定为垄断行为。

（二）算法合谋

算法合谋是指特定市场中的两个或两个以上独立的经营者，在算法参与下达成协议、决定或其他协同行为，共同对产品或服务的价格、数量等进行限定，从而排除、限制竞争的行为。需要注意的是，根据《反垄断法》及《反垄断法（修正草案）》中对经营者的界定，从事商品生产、经营、或提供服务的自然人、法人和非法人组织，均纳入经营者范畴。这意味着，通过某个互联网产品中的算法使得哪怕两名自然人达成任何形式的协同行为，只要这种协同行为排除、限制了竞争，就很可能构成算法合谋垄断行为。

与传统的垄断协议相比，算法合谋的核心是算法中权重配比的合谋。揭示算法合谋，只能以不同经营者之间外在价格或者服务条件的相似性为线索，要求这些经营者揭示具体算法，这可能成为主管机关的监管方向。

（三）以算法为垄断的工具

由于“二选一”或者“N选一”的最终实现需要依赖于经营者的规模及影响力，该类垄断行为通常发生在平台与平台内提供商品或者服务的经营者之间。互联网平台的“二选一”政策，主要是指具有市场支配地位的平台以明示或者暗示的方式要求平台内经营者与其签订“独家合作协议”，保证该平台内经营者的商品只通过该平台销售，同时保证不与竞争性平台合作。而“二选一”政策明显构成《反垄断法》所禁止的“没有正当理由，限定交易相对人只能与其进行交易”的滥用市场支配地位行为。而算法可能成为保证该不法垄断的工具。

近日，某外卖平台因滥用在中国境内网络餐饮外卖平台服务市场的支配地位，以实施差别费率、拖延商家上线等方式，促使平台内商家与其签订独家合作协议，并通过收取独家合作保证金和算法等技术手段，追踪商家的“反叛”行为，并对于所发现商家的“反叛”行为予以惩罚，以保障“二选一”行为实施，排除、限制了相关市场竞争，损害平台内商家和消费者的合法权益。基于此，市场监管总局责令其停止违法行为，全额退还独家合作保证金12.89亿元，并处以其2020年中国境内销售额1147.48亿元3%的罚款，计34.42亿元。尽管在“二选一”或者“N选一”的案件中，算法本身可能并不直接导致垄断行为，但是，算法成为了实施垄断的工具，不法垄断者可能遭受严厉的处罚。

二、反垄断监管趋势

随着国务院反垄断委员会《关于平台经济领域的反垄断指南》的生效及实施，相关反垄断执法机构对各大互联网平台的反垄断监管执法力度不断加大，并呈现持续性、常态化的趋势。从初次交审的《反垄断法（修正草案）》来看，各类经营者滥用数据、算法、技术及资本优势、平台规则等排除、限制竞争的行为都将被纳入反垄断法的制度框架中，原有法律制度较为原则宽泛无法跟上数字经济发展、对部分垄断行为处罚力度较轻的情况，将有所改变。《反垄断法（修正草案）》除了提高违法行为的罚款数额，更是对涉及垄断协议的责任规定了“双罚制”，经营者本身及其法定代表人、主要负责人、直接责任人一旦负有个人责任，均可被处以最高一百万元的罚款。

（一）对于大数据“杀熟”的监管趋势

不论是在理论还是实践层面，大数据“杀熟”是否属于“价格歧视”的违法行为、是否可界定为“滥用市场支配地位”从而受《反垄断法》的规制，还存在诸多争议。实践层面的监管与治理也存在制度缺位和监管困难等问题，许多消费者投诉平台“杀熟”的案例常因举证困难等问题，不了了之。

就目前已出台的法律法规而言，《电子商务法》第十八条规定“电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益”；《价格法》则明确了“不正当价格行为”及其罚则；《关于平台经济领域的反垄断指南》第十二条明确了具有市场支配地位的平台经济领域经营者滥用市场支配地位实施不公平价格行为的具体情形；第十七条的规定了上述经营者滥用市场支配地位，无正当理由对交易条件相同的交易相对人实施差别待遇的情形。

未来几年，大数据“杀熟”可能会树立若干典型案例，从而规范和引导平台规范操作，自行整改。同时，《个人信息保护法》的生效和实施也将规范平台企业的大数据使用和用户画像行为，通过约束处理个人信息的行为，从源头上遏制大数据“杀熟”的泛滥。具体而言，《个人信息保护法》明确了自动化决策的定义，并在第二十四条中规定了特定人群的算法歧视、大数据“杀熟”等问题，要求个人信息处理者利用个人信息进行自动化决策时应保证决策的“透明度”和结果的“公平、公正”。该条款并未禁止个人信息处理者进行自动化决策，而是规定了合法进行自动化决策的原则性要件，然而尚未进一步解释实现这些要件的具体规则，有待后续通过实施细则进行明确。关于“透明度”的合规要求，《信息安全技术 个人信息安全规范》（GB/T 35273-2020）规定了经营者须建立个人信息主体对个性化展示所依赖的个人信息自主控制机制，保障其调控个性化展示相关性程度的能力^[1]，这可资企业借鉴，以备政府监管与调查。

此外，《个人信息保护法》第二十四条第二款回应了《电子商务法》第十八条的内容，规定了个人对于自动化决策的知情权，要求企业在进行广告推送等活动时应当同时提供“不针对其个人特征的选项”和“便捷的拒绝方式”；第三款进一步规定了个人对其权益有重大影响的自动化决策（例如基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选等）具有知情权和拒绝权。此外，《个人信息保护法》规定对于利用个人信息进行自动化决策的场景，企业应当进行个人信息安全影响评估。

2021年8月27日，网信办发布《互联网信息服务算法推荐管理规定（征求意见稿）》，根据《个人信息保护法》、《网络安全法》、《数据安全法》和《互联网信息服务管理办法》等法律法规，对算法推荐活动进行监管和规范（附件一将对重点规定进行梳理）。

2021年9月17日，九部委又印发了《关于加强互联网信息服务算法综合治理的指导意见》（下称“《指导意见》”），提出利用三年左右时间，逐步建立治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局。其中值得注意的是，《指导意见》提出**企业应强化主体责任**，对算法应用产生的结果负主体责任；积极开展算法**安全评估和算法备案**工作，严厉打击违法违规行；推动**算法公开透明**；督促企业及时、合理、有效地公开算法基本原理、优化目标、决策标准等信息，做好算法结果解释工作，畅通投诉通道。

由此可见，我国正在加大对算法推荐活动的监管力度，不久的将来，监管将更为严厉。新法律法规及标准将进一步涌现，以明确主体权责并完善算法治理机制。

（二）对于算法合谋的监管趋势

对于明示的算法合谋，例如在合谋过程中把算法作为沟通工具来使用的信使合谋、由第三方提供算法作为工具而各方利用该工具进行合谋的轴辐合谋等，经营者通过明确的协商达成价格算法合谋以实现价格垄断，算法只是实现合谋的工具，其合谋的本质属于经营者之间的垄断协议，违反了《反垄断法》第二章下关于垄断协议、决定或者其他协同行为的禁止性规定。《反垄断法（修正草案）》中增设的条款也明确了“轴辐协议”，即经营者不得组织其他经营者达成垄断协议或者为其他经营者达成垄断协议提供实质性帮助。如该规定草案最终成为法律，“算法合谋”将无需将之识别为横向或纵向垄断协议，而是属于“本身违法”。

此外，修正草案增加了“安全港”制度，规定了达成垄断协议的经营者如果能够证明在相关市场的市场份额低于国务院反垄断执法机构所规定的标准的，原则上不予禁止。对于不同协议类型下“安全港”的市场份额标准，将有待反垄断执法机构予以明确。

（三）平台“二选一”监管趋势

市场监督管理总局已经就多个“二选一”案件作出处罚决定，处罚对象包括前文提及的某外卖平台，某大型电商集团，某品牌特卖平台，等等。

在已有的处罚案例中，反垄断执法机构一般会采用《反垄断法》第十七条第一款第（四）项规制平台“二选一”的垄断行为。具体而言，反垄断执法机构首先会依据以下标准判断平台经营者是否具有市场支配地位：（1）平台所占市场份额；（2）其他综合因素，包括相关市场竞争状况、市场控制力、财力和技术条件、交易上的依赖程度、市场进入难易程度和生态化布局等六个因素。

其次，反垄断执法机构根据下述标准判断平台企业是否实施了“二选一”行为：（1）与平台内经营者所签订的“独家合作”协议的内容；（2）通过多种奖励和处罚措施保证和强制“独家合作”的实施。

以算法为手段以达到垄断目的，可能被认为情节严重，作为执法机关予以重罚的考量因素之一。

三、预防算法歧视垄断行为的合规措施

（一）接轨《个人信息保护法》，谨慎处理用户个人信息

上述算法相关的新型垄断风险，与平台对用户个人信息的收集和使用息息相关，平台企业需要同时防范《个人信息保护法》和《反垄断法（修正草案）》项下的双重风险。平台进行“用户画像”时，必须遵循《民法典》第1035条所规定的“遵循合法、正当、必要原则，不得过度处理”，同时遵守《个人信息保护法》第五至七条规定的“合法、正当、必要、诚信原则”、“目的明确和最小必要原则”、“公开透明原则”，不得利用所收集的信息对用户进行价格歧视，或用于其他不利于用户或未经其同意的使用目的。

值得指出，利用算法仅仅是一种交易的技术工具，在我国现行法律法规的语境下，利用算法本身并不一定意味自动化决策，也并不一定“杀熟”。但是，利用算法与大数据，对于理应给予同等条件的用户不当施以不同的价格待遇，从而影响用户权益时，则涉及到须被规制的自动化决策行为。因此，建议企业作为个人信息处理者在运用自动化决策时，依照《个人信息保护法》、《数据安全法》、《网络安全法》、《电子商务法》、《数据安全管理办法（征求意见稿）》、《个人信息安全规范》、《互联网信息服务算法推荐管理规定（征求意见稿）》等相关法律法规以及立法动态，做好合规工作，合规重点如下：

- 在规划设计阶段或首次使用前及使用过程中定期(至少每年一次)开展**个人信息安全影响评估**，并依评估结果采取有效的保护个人信息主体的措施；
- 保证自动化决策过程的**透明与结果的公平**，并形成合理的机制让个人信息主体感知到透明度；
- 向个人信息主体提供针对自动决策结果的**投诉渠道**，并支持对自动决策的人工复核；
- 形成及时**反馈机制**，在个人信息主体要求个人信息处理者说明自动化决策作出的决定时做出有效反馈，保障信息主体的知情权；
- 形成**合理选择机制**，保障个人信息处理者在拒绝自动化决策做出决定时，权利得以便利地实现；
- 通过自动化决策所作的个性化展示需要同时**提供不针对个人特征的选项**；确保可以实现个人信息主体对自动化决策进行限制的权利，并且，可以关闭个性化推送或者展示；
- 按照相关实施细则，配合监管机构做好**合规审计、安全评估和备案**等合规工作。

（二）定期严格自查自检整改，规范平台优惠政策及算法运用

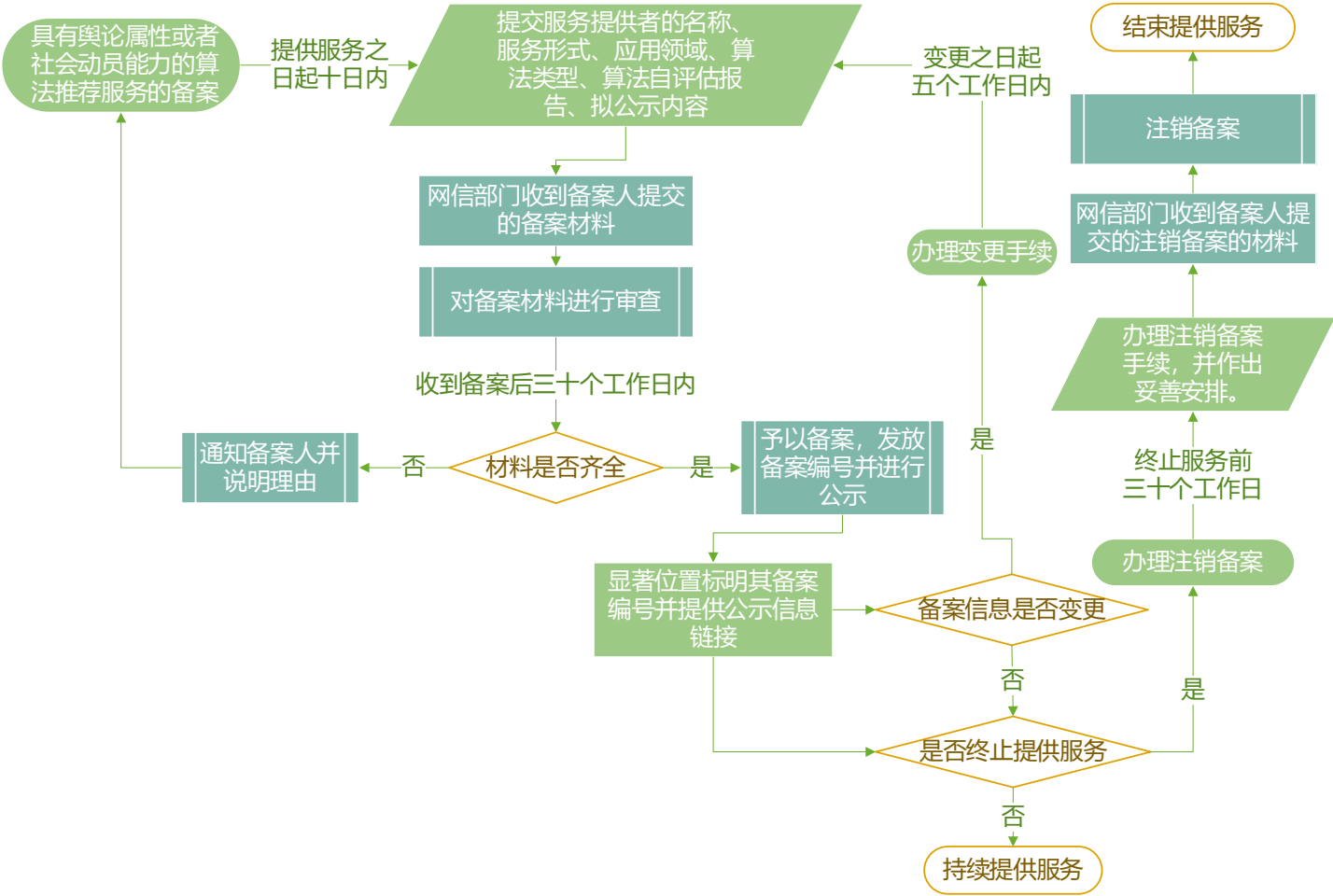
互联网平台推出的会员折扣、满减等优惠活动，既有可能被认定为大数据杀熟的手段，也有可能被视为平台违规进行“二选一”的激励政策，甚至可能被视为算法合谋、价格协同的手段。因此，平台需要定期自检自查其推出的相关政策，判断评估其是否构成

- （1）垄断协议；
- （2）价格歧视；
- （3）独家合作协议的激励或惩罚机制；或
- （4）算法合谋的外化体现。

平台企业的核心合规措施，就是加强对于平台服务所涉及的算法的合规内控筛查，若存在不符合《个人信息保护法》或者《反垄断法》《反垄断法（修正草案）》的情况，需要及时予以整改。鉴于反垄断执法机构可能审查平台企业所提供的服务或者交易条件相关的算法内核，企业需要事先做好预案。

图一：《互联网信息服务算法推荐管理规定（征求意见稿）》主要内容

义务类型	义务的要求
算法推荐服务提供者的义务	
安全主体的义务	应当落实算法安全主体责任，建立健全用户注册、信息发布审核、算法机制机理审核、安全评估监测、安全事件应急处置、数据安全保护和个人信息保护等管理制度，制定并公开算法推荐相关服务规则，配备与算法推荐服务规模相适应的专业人员和技术支撑。（第七条）
算法审查的义务	应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等。（第八条）
被禁止的算法模型	不得设置诱导用户沉迷或者高额消费等违背公序良俗的算法模型。（第八条）
内容审查的义务	应当加强信息内容管理，建立健全用于识别违法和不良信息的特征库，完善入库标准、规则和程序。发现未作显著标识的算法生成合成信息的，应当作出显著标识后，方可继续传输。（第九条第一款）
处置违法信息的义务	发现违法信息的，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向网信部门报告。发现不良信息的，应当按照网络信息内容生态治理有关规定予以处置。（第九条第二款）
用户模型关联的义务	算法推荐服务提供者应当加强用户模型和用户标签管理，完善记入用户模型的兴趣点规则。（第十条）
禁止的用户模型	不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息内容，不得设置歧视性或者偏见性用户标签。（第十条）
价值导向的义务	应当加强算法推荐服务版面页面生态管理，建立完善人工干预和用户自主选择机制，在首页首屏、热搜、精选、榜单类、弹窗等重点环节积极呈现符合主流价值导向的信息内容。（第十一条）
优化规则的义务	算法推荐服务提供者应当综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的透明度和可解释性，避免对用户产生不良影响、引发争议纠纷。（第十二条）
禁止干预舆论的义务	不得利用算法虚假注册账号、非法交易账号、操纵用户账号，或者虚假点赞、评论、转发、网页导航等，实施流量造假、流量劫持；不得利用算法屏蔽信息、过度推荐、操纵榜单或者检索结果排序、控制热搜或者精选等干预信息呈现，实施自我优待、不正当竞争、影响网络舆论或者规避监管。（第十三条）
保障用户权利的义务	算法推荐服务提供者应当以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图、运行机制等。（第十四条）
	算法推荐服务提供者应当向用户提供选择、修改或者删除用于算法推荐服务的用户标签的功能。（第十五条第二款）
	算法推荐服务提供者应当向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭算法推荐服务的选项。用户选择关闭算法推荐服务的，算法推荐服务提供者应当立即停止提供相关服务。（第十五条第一款）提供用户权利救济的义务（第十五条第三款）保护未成年人权利的义务（第十六条第一款）禁止向未成年人推送的内容（第十六条第二款）保护劳动者权利的义务（第十七条）保护消费者权利的义务（第十八条）
具有舆论属性、社会动员能力算法推荐服务提供者的义务	
备案的义务	具有舆论属性或者社会动员能力的算法推荐服务提供者应当在提供服务之日起十个工作日内通过互联网信息服务算法备案系统填报服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息，履行备案手续。（第二十条第一款） 算法推荐服务提供者的备案信息发生变更时，应当在变更之日起五个工作日内办理变更手续。（第二十条第二款）
办理终止备案的义务	算法推荐服务提供者终止服务的，应当在终止服务三十个工作日前办理注销备案手续，并作出妥善安排。（第二十条第三款）
公示备案信息的义务	应当在其对外提供服务的网站、应用程序等显著位置标明其备案编号并提供公示信息链接。（第二十二条）
其他义务	开展安全评估的义务（第二十三条第一款）留存服务日志的义务（第二十三条第二款）配合监管的义务（第二十四条第二款）接受社会监督的义务（第二十六条第一款）建立用户申诉制度的义务（第二十六条第二款）



图二：具有舆论属性、社会动员能力算法推荐的备案流程图

注释：

[1] 根据《信息安全技术个人信息安全规范》（GB/T 35273-2020）7.5 d) 的要求，“在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。”

从《汽车数据安全管理规定》 探索汽车数据的合规与发展

环球律师事务所
孟洁 | 张淑怡



【前言】

随着近些年来国内和国际层面智能网联汽车安全问题的频繁爆发，汽车数据安全逐渐得到人们重视。2021年两会期间，代表委员就车联网安全风险相关议题提交了十余份提案与议案，汽车数据安全已引发代表委员的深入审视。

在这一背景下，2021年8月20日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部联合发布《汽车数据安全管理办法（试行）》（以下简称“《规定》”）。本次试行稿在2021年5月12日发布的征求意见稿（以下简称“征求意见稿”）的基础上，在延续防范化解汽车数据安全风险这一背景的同时，也强调了对于保障汽车数据依法、合理、有效利用的客观需要，对汽车行业数据的健康有序利用起到重要作用，在保障数据安全的同时鼓励汽车产业平稳有序发展。下文我们将聚焦于《规定》的几大亮点，并结合其他相关法律法规，对《规定》的新增内容及《规定》反映出的相应合规要点做解读。

一、适用范围涵盖汽车行业的全部产业链条及市场主体

《规定》第二、第三条对适用范围做出了界定。相比原征求意见稿，其对条款结构做了一定调整，通过明确界定汽车数据、汽车数据处理、汽车数据处理者、个人信息、敏感个人信息、重要数据几个概念的方式，明确其适用范围；也进一步对用词予以明确，改原有的“运营者”为“汽车数据处理者”。

虽然在形式上略作调整，但《规定》并未对适用范围做出缩减。就涵盖的产业链条而言，其包含汽车设计、生产、销售、使用、运维等多个过程中的数据处理；从数据的生命周期角度而言，其对汽车数据处理中从收集到使用、加工等各个不同环节的合规要求作出界定；从数据处理主体的角度而言，其也做了非常广泛的规定，包含各类开展汽车数据处理活动的组织。

此外，在汽车数据处理者的定义上，相比原征求意见稿，《规定》在条文中明确了“出行服务企业”这一主体。一些出行服务企业虽不承担车辆本身的设计、制造、生产等服务，但也需要遵守《规定》的要求，对用户的个人信息及重要数据予以保护。

这一主体的新增和几个月前的滴滴事件不无联系。网约车类App需要收集用户移动电话号码、位置信息及行踪轨迹、支付信息等个人信息。

此外，部分企业拥有电子地图制作的甲级测绘资质，涉及《规定》中定义的重要数据，这些数据的泄露不仅可能对用户个人权益造成影响，还将对国家安全造成严重威胁。我们在此提示各大出行服务企业，关注《规定》中的合规要求，对企业数据合规风险及时作出评估和整改，应对强监管趋势，切实保障用户数据安全及重要数据安全。

二、明确界定汽车领域的个人信息和重要数据

《规定》为与《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）相衔接，调整了个人信息的定义方式，在沿用《个人信息保护法》采用的“已识别+可识别”的定义方式的同时，对汽车领域自然人的范围予以明确。为方便比较查看，我们在此以表格的形式对相关条款予以列举：

《汽车数据安全若干规定》	《个人信息保护法》
第三条 汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等。 个人信息，是指以电子或者其他方式记录的与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。 	第四条 个人信息是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。 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、删除等。



另外，在重要数据的界定上，《规定》衔接了《中华人民共和国数据安全法》（以下简称“《数据安全法》”）对于数据分类分级保护的规定，明确了汽车行业的重要数据具体包含的数据范围，便于对这些数据进行重点保护。也应注意，涉及重要数据处理的企业不仅需要遵守《规定》中的合规要求，更应注意《数据安全法》等上位法律对于重要数据处理者设定的一系列义务。

《数据安全法》	《汽车数据安全若干规定》 (试行)	《汽车数据安全若干规定》 (征求意见稿)
第二十一条	第三条	第三条
国家建立数据分类分级保护制度，...对数据实行分类分级保护。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，加强对重要数据的保护。 ... 各地区、各部门应当按照数据分类分级保护制度，<u>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</u>，对列入目录的数据进行重点保护。	 重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括： （一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据； （二）<u>车辆流量、物流等反映经济运行情况的数据</u>； （三）汽车充电网的运行数据； （四）包含人脸信息、车牌信息等的车外视频、图像数据； （五）<u>涉及个人信息主体超过10万人的个人信息</u>； （六）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。	 本规定所称重要数据包括： （一）军事管理区、国防科工等涉及国家秘密的单位、县级以上党政机关等重要敏感区域的人流车流数据； （二）高于国家公开发布地图精度的测绘数据； （三）汽车充电网的运行数据； （四）道路上车辆类型、车辆流量等数据； （五）包含人脸、声音、车牌等的车外音视频数据； （六）国家网信部门和国务院有关部门明确的其他可能影响国家安全、公共利益的数据。

与原征求意见稿比较而言，《规定》对于重要数据的定义有两点需要特别予以关注：

其一，明确纳入物流类数据。物流企业在货物在途过程中会对车辆位置信息、轨迹信息等予以追踪，应特别注意在相关业务场景下的数据保护。

其二，明确构成重要数据的个人信息的规模。《规定》将涉及个人信息主体超过十万人的个人信息规定为重要数据，与此同时调整了年度报告制度（详见以下第五部分第（四）节的描述）的相关表述。

三、明确数据处理的四大原则

《规定》第六条对原征求意见稿的原则部分做了一定调整，明确了汽车数据处理的四大原则。

其一，车内处理原则，即除非确有必要不向车外提供。该原则从侧面反映了个人信息收集的最小必要原则，将车辆数据保留在车内进行处理，保证了用户对于其个人数据的控制权，也将重要数据的处理限制在车内，有助于减少因对外传输数据造成的泄露风险和安全隐患。

其二，默认不收集原则，即除非驾驶人自主设定，每次驾驶时默认设定为不收集状态。相比原征求意见稿，《规定》对默认为不收集状态的例外情形予以明确，即仅在驾驶人自主设定的情况下才能对不收集数据的默认设定予以变更。

其三，精度范围适用原则，即根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率。这提示企业在数据精度方面应根据自身业务需求设置摄像头、雷达的覆盖范围，如若采集的数据超出业务所必须的精度，不仅可能提高企业运营成本，还会为企业带来不必要的合规风险。

其四，脱敏处理原则，即尽可能进行匿名化、去标识化等处理。这方面特别要注意的是对车外人员信息的脱敏处理。车内摄像头等设备在进行路况信息采集时，不可避免地会采集到路上行人等车外人员的人脸信息。网联汽车在将相关路况信息上传至云进行分析处理时，要特别注意对车外人员的人脸信息以及车牌信息等进行脱敏处理，以对车主以外的个人信息予以保护。不过上述原则仍为倡导性原则。此前也有业内人士建议减少本条不必要的灵活空间，但《规定》仍保留了原征求意见稿“倡导”之用语。这些原则具体在实践中如何得到应用有待进一步观察。这也提示企业在开展合规工作时不仅应密切关注立法动态，也应对行业内有关部门的监管动向予以注意，以便更好地理解、适用和遵守法律。

四、细化汽车处理场景下的告知同意规则

《规定》对汽车数据的处理仍然采纳了告知——同意规则，并针对汽车行业做出了特别规定。第七条规定了汽车数据处理者的告知义务，明确了履行告知义务的可能方式（通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式）以及需要告知的内容。

相较征求意见稿，《规定》新增了对于用户查阅、复制其个人信息的方式和途径的告知义务。与此相关的合规场景最为典型的即为今年四月的某品牌车主维权事件。该事件中，车主对某品牌公布的行车数据的真实性予以质疑，用户缺乏自由查看其车辆行驶数据的途径，而这一风险敞口也引发了企业与用户之间的信任危机。为弥补这一漏洞，该品牌已经着手开发线上信息系统平台，供用户查询获取车机交互数据。这也提示企业应特别注意保障用户查询、复制其个人信息的权利，对查询、复制其个人信息的渠道及时对用户予以告知。

《规定》于第八条明确了用户同意的方式。第二款特别对难以获得主体同意场景下的个人信息处理作出了规定，即对其进行匿名化处理。这一规定认可了目前实践中的通常做法，解决了采集车外人员个人信息难以获得主体同意的难题。

总体而言，《规定》通过规定告知义务、征得同意义务和匿名化要求，促使汽车数据处理者更好地履行个人信息保护责任。此外也可从此看出，无论是在条款中明确车外人员作为个人信息主体，还是对于解决获得车外人员同意方式的难题，《规定》都进一步扩展汽车数据处理所涉及的个人信息主体，对车外人员的权利保障予以重视。

五、细化汽车处理场景下敏感个人信息、生物识别信息的处理规则

《规定》针对处理敏感个人信息的处理的要求进行了额外规定。

从处理的目的来看，需要具有直接服务于个人的目的，包括增强行车安全、智能驾驶、导航等；从告知义务来看，需要通过用户手册、车载显示面板、语音以及汽车使用相关应用程序等显著方式告知必要性以及对个人的影响；从同意要求来看，除了应取得单独同意外，还需要保证用户可以自主设定同意期限；从收集状态来看，需要以适当方式提示收集状态，并保证用户可以便利终止收集个人信息；保障用户删除个人信息的权利。

当处理个人生物识别信息时，还需要具有增强行车安全的目的和充分的必要性。

六、对重要数据处理活动做出规范

《规定》对重要数据的处理作出了较为完整的规范。在第三条对汽车产业的重要数据加以定义后，分别规定了风险评估报告制度、出境安全评估制度、抽查核验制度、年度报告制度及年度补充报告制度这五大制度。

（一）风险评估报告制度

《规定》第十条反映了《数据安全法》第三十条的要求：

《数据安全法》	《汽车数据安全若干规定》（试行）
第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。 风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。	第十条 汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。 风险评估报告应当包括处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。



本条明确了汽车数据处理者在开展重要数据处理活动前，应当进行风险评估报告。本条规定与《数据安全法》基本保持一致的思路，即通过针对特定主体的方式对企业自评义务作出规范。但《个人信息保护法》采取了不同的规范思路，通过界定特定处理行为规定企业的自评义务。相较而言，GDPR采取的也是通过界定特定处理行为的方式规范企业的自评义务。

对于风险评估的范围确定问题，在实践中因具体情形而异，但总体而言这项制度的确立提醒企业应当尽快对其处理的数据类型、开展的处理活动进行系统梳理，以应对《规定》正式生效后产生的风险评估及报告义务。

（二）出境安全评估制度

《汽车数据安全若干规定》（试行）	《个人信息保护法》	《数据安全法》	《网络安全法》
第十一条	第四十条	第三十一条	第三十七条
重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。未列入重要数据的涉及个人信息数据的出境安全管理，适用法律、行政法规的有关规定。	关键信息基础设施运营者和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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，由国家网信部门会同国务院有关部门制定。	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。
我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保留的条款除外。			

本条对重要数据的本地化存储以及出境安全评估制度做了基本的规定。为方便比较分析，上表除《规定》外，另列出了三部上位法对数据本地化及出境评估的相关要求。

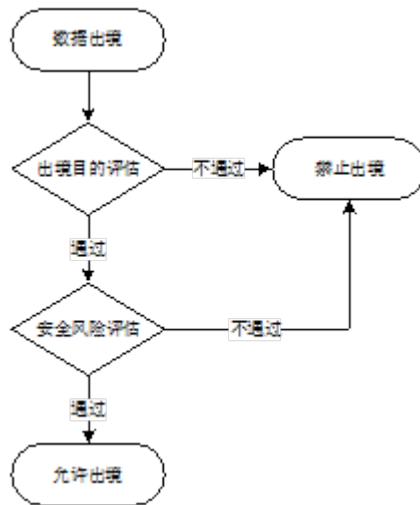
我国在立法框架上目前是将个人信息和重要数据的本地化存储及出境安全评估分别予以规定，在《个人信息保护法》中规定个人信息的出境制度，而在《数据安全法》中，则通过沿用《网络安全法》原有规定的方式规定了重要数据的本地化及出境评估要求。

结合《规定》第三条对重要数据的定义即可发现，《规定》对个人信息和重要数据的本地化和出境评估进行了归拢。其采用的是一种对重要数据加以广义理解的方式，将《个人信息保护法》中对“处理个人信息达到国家网信部门规定数量”这一情形同样纳入“重要数据”的词义范围之中。不仅如此，《规定》进一步对处理个人信息的数量做出明确，即涉及个人信息主体超过十万人的个人信息的，需要执行数据本地化及出境安全评估制度。

虽然数据只有在其流动时才最能彰显其自身价值，但世界各国出于保护本国数据安全及国家安全的目的，也对数据的跨境流动做了一定限制，数据本地化存储的要求即是一种常见的限制数据跨境流动的立法模式。具体至汽车行业，多家车企也受数据本地化要求的影响，先后在境内设立数据中心，以便存储中国境内用户的个人信息以及其他类型的重要数据，符合我国监管要求。

对于数据出境评估的具体要求并未在《规定》抑或上述三部上位法中予以阐明。目前对于数据出境的评估流程及要求主要参照《信息安全技术 数据出境安全评估指南（征求意见稿）》，其中规定的评估要求概括而言包含两个方面：第一，出境目的，应同时满足合法性、正当性和必要性的要求；第二，安全风险，应综合考虑出境数据的属性和数据出境发生安全事件的可能性及影响程度，对个人信息、重要数据、数据发送方的安全保护能力均有特别要求。

下图为该指南中规定的出境评估基本流程：



（三）抽查核验制度

该项制度规定于《规定》第十二条第二款。汽车数据处理者在进行重要数据出境时应当与出境安全评估时明确的基本内容保持一致，国家网信部门会同国务院有关部门以抽查等方式核验的，汽车数据处理者应当予以配合，并以可读等便利方式予以展示。

本条赋予了监管机构对企业出境合规进行抽查检验的权利。企业应特别注意本条的规定，有数据出境情形的应当按照要求进行数据出境安全评估，做好配合有关部门抽查核验的准备，并对抽查核验情况保存相应记录，以便佐证自身履行了配合执法义务。

(四) 年度报告制度

《规定》第十三条从如下表所列的几个方面对年度报告制度予以明确。

范围	开展重要数据处理活动的汽车数据处理者
报告时间	每年十二月二十五日前
报告对象	省、自治区、直辖市网信部门和有关部门
报告内容	(一) 汽车数据安全负责人、用户权益事务联系人的姓名和联系方式； (二) 处理汽车数据的种类、规模、目的和必要性； (三) 汽车数据的安全防护和管理措施，包括保存地点、期限等； (四) 向境内第三方提供汽车数据情况； (五) 汽车数据安全事件和处置情况； (六) 汽车数据相关的用户投诉和处理情况； (七) 国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全情况。

(五) 年度补充报告制度

年度补充报告制度见于《规定》第十四条，针对“向境外提供重要数据”的汽车数据处理者，安排其补充报告以下内容：接收者的基本情况；出境汽车数据的种类、规模、目的和必要性；汽车数据在境外的保存地点、期限、范围和方式；涉及向境外提供汽车数据的用户投诉和处理情况；国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的向境外提供汽车数据需要报告的其他情况。

七、针对智能网联汽车的新增条款

《规定》针对智能网联汽车新增了第十六条。该条款虽然并未对智能网联汽车明确规定合规要求，但反映了国家对于智能网联汽车领域的重视，也反映了《规定》鼓励发展与从严监管并举的基本态度。相关车企在发展自身产业的同时，更应重视合规工作的开展，在法律框架内实现智能网联汽车行业的良好发展。。

八、违反规定的法律责任

对于车企违反《规定》的法律责任，《规定》中并没有加以明确，适用的多是《个人信息保护法》《数据安全法》《网络安全法》三部法律规范中规定的罚则。上述法律规范中规定的罚则相对而言还是较重的，尤其是《数据安全法》《个人信息保护法》中均专章规定了法律责任，企业应当予以关注。概括而言，这些法律责任包括但不限于如下内容：

其一，约谈、责令整改、警告、停业整顿、吊销相关业务许可证或者吊销营业执照；

其二，没收违法所得；

其三，直接负责的主管人员和直接责任人员罚款，构成犯罪的追究相应刑事责任；

其四，罚款。《数据安全法》中规定的最高罚款数额达一千万元，而《个人信息保护法》进一步提高了罚款上限，为五千万元。这一数额相较欧盟GDPR规定的“集团全球营业额4%或2000万欧元取其高”的责任限额已逐渐趋于持平，体现了我国在数据保护方面严监管的决心。

。

九、企业的合规义务

前述内容已对《规定》相关内容做了较为详尽的评述，国家加大监管力度、督促车企开展数据合规建设已经成为不可逆转的趋势，我们建议落入该规定的企业密切关注该部新规，并采取如下措施：

1. 对自身涉及的数据进行详尽的排查梳理，是否涵盖个人信息、敏感个人信息、重要数据等。
2. 收集、处理个人信息的，是否在收集之前告知该个人并征得其同意。
3. 收集、处理敏感个人信息的，是否具有特定的目的，显著告知并征得单独同意、并满足用户的以下权利：自主设定同意期限、便利终止收集、删除个人信息，并开展个人信息保护影响评估等。
4. 收集、处理生物识别信息的，是否具有增强行车安全的目的和充分的必要性。
5. 在个人信息出境前，是否遵循了法律、行政法规的有关规定
6. 对于数据的处理是否符合：车内处理原则、默认不收集原则、精度范围适用原则、脱敏处理原则。
7. 收集重要数据的，是否在开展重要数据处理活动前，开展了风险评估。
8. 重要数据出境前，是否通过了国家网信部门会同国务院有关部门组织的安全评估。
9. 是否配合国家网信部门会同国务院有关部门对重要数据出境的抽查与核验。
10. 处理重要数据的，是否在每年十二月二十五日前向省、自治区、直辖市网信部门和有关部门就重要数据处理情况进行报告；将重要数据出境的，是否在报告里报告了额外内容。

除了前述要求外，如果企业涉及处理个人信息、重要数据，还须遵守《个人信息保护法》《数据安全法》以及配套法律法规的额外要求。

附件一：《互联网信息服务管理办法》合规义务清单

合规项	公司合规义务正面清单 (Do)	是	否	违法责任	备注
一般行业的 设立要求	1. 如企业经营属于 电信业务 的互联网信息服务, 应当向电信主管部门 (即省、自治区、直辖市通信管理局) 提出申请 (第 11 条), 并且取得电信主管部门颁发的 电信业务经营许可证 。(第 7 条)	☐	☐	由电信主管部门 ① 责令互联网网络接入服务提供者停止为其提供接入服务; ② 没收违法所得; ③ 可以并处 50 万元以下罚款。	
	2. 如企业经营不属于电信业务的互联网信息服务, 应当向电信主管部门进行 备案 。(第 7 条)	☐	☐		
	3. 备案应当通过互联网网络接入服务提供者向电信主管部门提交以下材料: (第 8 条) (一) 主办者真实身份证明和地址、联系方式等基本情况; (二) 拟开展的互联网信息服务类型、名称, 拟使用的域名、IP 地址、服务器等互联网网络资源, 互联网网络接入服务提供者等有关情况; (三) 拟提供的服务项目, 需要取得相关主管部门许可的, 还应当提供相应的 许可文件 ; (四) 公安机关出具的安全检查意见; (五) 需要提供的其他材料。	☐	☐	/	新增
	4. 如企业不再从事互联网信息服务的, 应 主动注销 相关许可和备案。(第 11 条)	☐	☐	/	新增
	5. 企业从事互联网信息服务, 应当 ① 使用符合 电信主管部门 要求的 网络资源 ; ② 具备符合国家规定的网络安全与信息安全管理制度和技术保障措施。(第 10 条)	☐	☐	由电信主管部门 ① 责令互联网网络接入服务提供者停止为其提供接入服务; ② 没收违法所得; ③ 可以并处 50 万元以下罚款。	新增
		☐	☐		

特定行业的 设立要求	1. 如企业从事互联网新闻信息服务，应当 ① 向网信部门提出申请；（第 12 条） ② 相关从业人员应当依法取得相应资质，接受相应的培训与考核。（第 12 条）	☐	☐	由 网信部门 或者其他有关部门	
	2. 如企业从事文化、出版、视听节目的互联网信息服务，应当取得有关部门的许可。（第 12 条） 注 1：根据《互联网文化管理暂行规定（2017 修订）》第 9 条、第 10 条的规定，从事经营性互联网文化活动，应当经省级文化行政部门（即省、自治区、直辖市文化和旅游局）批准，取得《网络文化经营许可证》。从事非经营性互联网文化活动，应当向省级文化行政部门（即省、自治区、直辖市文化和旅游局）备案。 注 2：根据《网络出版服务管理规定》第 4 条、第 7 条的规定，从事网络出版服务，必须依法向省级出版行政主管部门（即省、自治区、直辖市新闻出版局）提出申请，审核同意后上报，经过出版行政主管部门（即国家新闻出版署）批准，取得《网络出版服务许可证》。 注 3：根据《互联网视听节目服务管理规定》第 7 条的规定，从事互联网视听节目服务，应依法通过省级广播电影电视主管部门（即省、自治区、直辖市广播电影电视局）向国务院广播电影电视主管部门（即国家广播电视总局）提出申请，经批准，取得《信息网络传播视听节目许可证》；从事互联网视听节目转播类服务，应向省级广播电影电视主管部门（即省、自治区、直辖市广播电影电视局）履行备案手续。	☐	☐	① 责令停止相关互联网信息服务； ② 没收违法所得： （1）违法所得 1 万元以上的，并处违法所得 5 倍以上 10 倍以下罚款； （2）违法所得不足 1 万元或者没有违法所得的，可以并处 10 万元以下罚款； ③ 情节严重的，由电信主管部门吊销其电信业务经营许可证件或者取消备案编号。	文化与视听节目这两个行业属于新增。
	3. 如企业从事教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国务院有关决定须经有关部门许可的，应当取得有关部门的许可。（第 12 条） 注 1：目前，根据《国务院关于第二批取消 152 项中央指定地方实施行政审批事项的决定》，开办教育网站和网校不再需要教育行政部门的审批。但根据《教育移动互联网应用程序备案管理办法》第 9 条、第 10 条的规定，开发教育移动应用的，应向省级教育行政部门（即省、自治区、直辖市教育厅）进行备案。 注 2：根据《互联网食品药品经营监督管理办法》（征	☐	☐		

	求意见稿》第7条的规定，从事互联网食品药品经营（包含销售保健食品、药品和医疗器械的行为），应当取得省级食品药品监督管理部门（省、自治区、直辖市市场监督管理局与药品监督管理局）颁发的食品药品经营许可证；从事互联网药品信息服务，应向省级食品药品监督管理部门（省、自治区、直辖市药品监督管理局）备案。				
查验实名信息	1. <u>互联网网络接入服务提供者</u> 为互联网信息服务提供者提供接入服务，应当： ① 要求<u>互联网信息服务提供者</u>提供相应许可证件（电信业务经营许可证，以及上述特定行业设立业务时应取得的各项许可证）或者备案编号； ② 查验上述许可证件及备案编号。（第13条）	☐	☐	由电信主管部门 ① 处10万元以上100万元以下罚款； ② 并可以责令暂停相关业务、停业整顿、吊销其电信业务经营许可证件或者取消备案编号； ③ 对直接负责的主管人员和其他直接责任人员，处1万元以上10万元以下罚款。	新增
	2. <u>互联网信息服务提供者</u>，应当 ① 要求某些利用互联网从事服务的用户，依照法律、行政法规以及国家有关规定取得相应的资质； ② 查验用户提供的具有合法资质的证明文件。（第13条）	☐	☐	由网信部门、电信主管部门、公安机关或者其他有关部门 ① 给予警告； ② 责令限期改正； ④ 没收违法所得； ⑤ 拒不改正或者情节严重的，处10万元以上50万元以下罚款，并可以责令暂停相关业务，停业整顿、关闭网站、由原许可机关吊销相关业务许可证或者吊销营业执照； ⑥ 对直接负责的主管人员和其他直接责任人员，处1万元以上10万元以下罚款。	新增
	3. <u>互联网信息服务提供者</u> 如对其已备案的互联网域名进行转让的，应提前向电信主管部门变更相关的备案信息。（第13	☐	☐	由电信主管部门 ① 处10万元以上100万元以下罚款；	新增

	条)			② 并可以责令暂停相关业务、停业整顿、吊销其电信业务经营许可证件或者取消备案编号； ③ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	
	4. <u>互联网信息服务提供者、互联网网络接入服务提供者、域名注册和解析服务提供者</u> 在与用户签订协议或者确认提供服务时，应当 ① 确保服务对象与身份证件信息或者组织机构代码证书信息等必要的 真实身份信息 一致； ② 记录相关信息。（第 18 条）	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	由网信部门、电信主管部门、公安机关 ① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	新增
	5. <u>互联网信息服务提供者、互联网网络接入服务提供者、域名注册和解析服务提供者</u> 在对任何组织和个人办理、使用互联网网络接入、互联网信息服务、域名注册和解析等互联网服务时，应当要求其 提供真实身份信息 。（第 19 条）	☐ ☐	☐ ☐	对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	新增

亮出证号与 及时变更	1. <u>互联网信息服务提供者</u>	☐	☐	由网信部门、电信主管部门、公安机关或者其他有关部门	
	① 在提供服务时应当明示许可证编号或者备案编号；（第 14 条） ② 当其许可或者备案事项发生变更的，应当向原许可或者备案机关办理变更手续。（第 14 条）	☐	☐	① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿、关闭网站、由原许可机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	
建立网络与 信息安全管 理制度	1. <u>互联网信息服务提供者</u> ，应当	☐	☐	针对互联网信息服务提供者： 由网信部门、电信主管部门、公安机关或者其他有关部门	新增
	① 建立信息发布审核制度；（第 16 条） ② 配备符合网信部门、电信主管部门、公安机关要求的网络与信息安全管理人員。（第 16 条）	☐	☐	① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿、关闭网站、由原许可机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	
建立网络与 信息安全管 理制度	2. <u>互联网信息服务提供者、互联网网络接入服务提供者</u> ，应当	☐	☐	针对互联网网络接入服务提供者： 由网信部门、电信主管部门、公安机关	
	① 建立网络安全与信息安全管理制度； ② 建立用户信息保护制度； ③ 采取安全防范措施； ④ 加强公共信息巡查。（第 16 条）	☐	☐	① 给予警告；	

			② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	
3. <u>互联网信息服务提供者</u> ，应当按照网信部门、电信主管部门、公安机关要求	☐	☐	由网信部门、电信主管部门、公安机关或者其他有关部门 ① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿、关闭网站、由原许可机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	新增
① 建立互联网新业务安全评估制度；	☐	☐		
② 对其通过互联网新开展并取得经营许可的互联网信息服务业务进行安全评估；				
③ 将有关评估结果向网信部门、电信主管部门、公安机关报告。（第 17 条）				
4. <u>互联网信息服务提供者</u> 、 <u>互联网网络接入服务提供者</u> ，应当			针对互联网信息服务提供者： 由网信部门、电信主管部门、公安机关或者其他有关部门 ① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10	新增
① 建立网络信息安全投诉、举报制度；	☐	☐		
② 公布投诉、举报方式等信息；	☐	☐		
③ 及时受理并处理有关网络信息安全的投诉和举报。（第 23 条）	☐	☐		



				万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿、关闭网站、由原许可机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。 <u>针对互联网网络接入服务提供者：</u> 由网信部门、电信主管部门、公安机关 ① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	
信息保存	1. <u>互联网信息服务提供者、互联网网络接入服务提供者、域名注册和解析服务提供者</u> 查验的真实身份信息应当 ① 在提供服务期间同步保存； ② 很在停止服务后保存至少两年以上。（第 18 条）	☐	☐	由网信部门、电信主管部门、公安机关 ① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照；	新增
	2. <u>互联网信息服务提供者</u>，应当 ① 记录其发布的信息和用户发布的信息，并 ② 保存不少于6 个月。（第 20 条）	☐	☐	以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照；	新增

	3. <u>互联网信息服务提供者、互联网网络接入服务提供者</u>，应当 ① 记录并留存网络日志信息，并 ② 保存不少于 6 个月。（第 20 条）	☐	☐	⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	
	4. <u>互联网网络接入服务提供者</u> 通过网络代理、网络地址转换等方式，与他人共享互联网网络接入服务资源，还应①记录并②留存地址转换记录等可确认用户身份的日志信息。（第 20 条）	☐	☐		
	5. <u>互联网信息服务提供者、互联网网络接入服务提供者、域名注册和解析服务提供者</u> 发现网络违法犯罪行为，应当 ① 保存有关记录，并 ② 向网信部门、电信主管部门、公安机关报告。（第 21 条）	☐	☐		新增
	6. <u>互联网信息服务提供者、互联网网络接入服务提供者</u> 发现发布、传输的信息属于《管理办法（征求意见稿）》第二十六条所列内容的，应当 ① 立即停止传输； ② 采取消除等处置措施，防止信息扩散； ③ 保存有关记录； ④ 并向网信部门、电信主管部门、公安机关报告。（第 27 条） 注：《网络信息内容生态治理规定》第 6 条有十一项不良行为；《管理办法（征求意见稿）》第 26 条有九项，但整合了《网络信息内容生态治理规定》的内容，且第 3 项至第 5 项为新添加内容。（在下文负面清单中做了加粗标明。）	☐	☐	针对互联网信息服务提供者、互联网网络接入服务提供者： 由网信部门、电信主管部门、公安机关 ① 责令改正； ② 给予警告； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、由原发证机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。 <u>针对为他人获取、传播被依法阻断的信</u>	新增

			<u>息而提供技术支持或者其他帮助的组 织和个人：</u> 由公安机关 ① 没收违法所得； ② 处 5 日以下拘留，可以并处 5 万 元以上 50 万元以下罚款； ③ 情节严重的，处 5 日以上 15 日以 下拘留，可以并处 10 万元以上 100 万元以下罚款。 单位违反规定的，由公安机关 ① 没收违法所得，处 10 万元以上 100 万元以下罚款； 并对直接负责的主管人员和其他直接 责任人员依照前款规定处罚。	
防止违法犯 罪活动与协 助	1. <u>互联网信息服务提供者、互联网网络接入服务提 供者、域名注册和解析服务提供者</u> ，应当 采取 <u>技术措施和其他必要措施</u> ，防范、发现、制 止所提供的服务被用于实施违法犯罪。（第 21 条）	☐	☐ <	

	条)			万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿。	
	3. <u>互联网信息服务提供者、互联网网络接入服务提供者、域名注册和解析服务提供者</u> ，应当为网信部门、电信主管部门依法履行互联网信息服务监督管理职责，提供必要的技术支持和相关配合。（第 22 条）	☐	☐	由网信部门、电信主管部门 ① 给予警告； ② 责令限期改正； ③ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿。	新增
信息保护与 防泄露	1. <u>互联网信息服务提供者、互联网网络接入服务提供者及其工作人员</u> 对所收集、使用的身份信息、日志信息应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止所收集、使用的身份信息、日志信息泄露、毁损、丢失。（第 23 条）	☐	☐	针对互联网信息服务提供者： 由网信部门、电信主管部门、公安机关或者其他有关部门 ⑥ 给予警告； ⑦ 责令限期改正； ⑧ 没收违法所得； ⑨ 拒不改正或者情节严重的，处 10	新增
	2. <u>互联网信息服务提供者、互联网网络接入服务提供者</u> 在发生或者可能发生信息泄露、毁损、丢失的情况时，应当 ① 立即采取补救措施，并 ② 按照规定及时告知用户并 ③ 向有关主管部门报告。（第 23 条）	☐	☐	万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿、 关闭网站 、由原许可机关吊销相关业务许可证或者吊销营业执照； ⑩ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。 针对互联网网络接入服务提供者： 由网信部门、电信主管部门、公安机关 ⑥ 给予警告； ⑦ 责令限期改正； ⑧ 没收违法所得； ⑨ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、 由原发证机关吊销相关业务许可证或者吊销营业执照； ⑩ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	

遵守标准	企业从事互联网信息服务应当符合国家标准的强制性要求。（第 28 条）	☐	☐	/	新增
应急处置	互联网信息服务提供者、互联网网络接入服务提供者，应当 ① 建立应急机制，并 ② 在必要时及时采取应急处置措施。（第 29 条）	☐	☐	/	新增
配合监督检查	互联网信息服务提供者、互联网网络接入服务提供者，应当 在网信部门、电信主管部门、公安机关和其他有关部门依法履行监督检查等执法职责时，予以配合。（第 32 条）	☐	☐	针对互联网信息服务提供者： 由网信部门、电信主管部门、公安机关或者其他有关部门	新增
				① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务，停业整顿、关闭网站、由原许可机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。 针对互联网网络接入服务提供者： 由网信部门、电信主管部门、公安机关 ① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 拒不改正或者情节严重的，处 10 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。	

合规项	公司合规义务负面清单 (Don'ts)			违法责任	
查验实名认证信息	1. <u>互联网网络接入服务提供者</u> 不得为未取得合法许可证件或者备案编号的互联网信息服务提供者提供服务。(第 13 条)	☐	☐	由电信主管部门 ① 处 10 万元以上 100 万元以下罚款; ② 并可以责令暂停相关业务、停业整顿、吊销其电信业务经营许可证件或者取消备案编号; ③ 对直接负责的主管人员和其他直接责任人员, 处 1 万元以上 10 万元以下罚款。	新增
	2. <u>互联网信息服务提供者</u> 不得为未取得合法资质的用户提供服务。(第 13 条)	☐	☐	由网信部门、电信主管部门、公安机关或者其他有关部门 ① 给予警告; ② 责令限期改正; ③ 没收违法所得; ④ 拒不改正或者情节严重的, 处 10 万元以上 50 万元以下罚款, 并可以责令暂停相关业务、停业整顿、关闭网站、由原许可机关吊销相关业务许可证或者吊销营业执照; ⑤ 对直接负责的主管人员和其他直接责任人员, 处 1 万元以上 10 万元以下罚款。	新增
	3. <u>互联网信息服务提供者、互联网网络接入服务提供者、域名注册和解析服务提供者</u> 在对任何组织和个人办理、使用互联网网络接入、互联网信息服务、域名注册和解析等互联网服务时, 不得违反本办法规定的真实身份查验要求, 实施下列行为: (一) 为使用虚假身份信息、冒用他人身份信息的组织和个人, 办理互联网服务; (二) 为未提供真实身份信息的组织和个人, 获取、使用他人注册的互联网账号、资源; (三) 为他人规避实施真实身份查验的要求, 提	☐	☐	由网信部门、电信主管部门、公安机关 ① 给予警告; ② 责令限期改正; ③ 没收违法所得; ④ 拒不改正或者情节严重的, 处 10 万元以上 50 万元以下罚款, 并可以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照; ⑤ 对直接负责的主管人员和其他直接责任人员, 处 1 万元以上 10 万元以下罚款。	新增

	供技术支持或者帮助。(第 19 条)				
违法 犯罪 行为	1. 任何组织和个人不得设立用于实施违法犯罪的网站、通信群组、网络账号、移动智能终端应用,不得开办用于实施违法犯罪的互联网服务。(第 15 条)	☐	☐	由公安机关 ① 没收违法所得; ② 处 5 日以下拘留,可以并处 5 万元以上 50 万元以下罚款; ③ 情节较重的,处 5 日以上 15 日以下拘留,可以并处 10 万元以上 100 万元以下罚款。 单位违反规定的,由公安机关	新增
	2. 任何组织和个人不得明知他人利用互联网信息服务实施违法犯罪而为其提供技术支持、广告推广、支付结算、代办网络服务等帮助。(第 15 条)	☐	☐	① 没收违法所得; ② 处 10 万元以上 100 万元以下罚款; ③ 并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。	
	3. 任何组织和个人不得倒卖移动电话卡、上网卡、物联网卡。(第 15 条)	☐	☐	① 没收违法所得; ② 处 10 万元以上 100 万元以下罚款; ③ 并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。	
	4. 任何组织和个人不得以营利为目的或为获取其他非法利益,实施下列行为,扰乱网络秩序: (一)明知是虚假信息而发布或者有偿提供信息发布服务的; (二)为他人有偿提供删除、屏蔽、替换、下沉信息服务的; (三)大量倒卖、注册并提供互联网信息服务账号,被用于违法犯罪的; (四)从事虚假点击、投票、评价、交易等活动,破坏互联网诚信体系的。(第 25 条)	☐	☐	由网信部门、电信主管部门、公安机关 ① 给予警告; ② 责令限期改正; ③ 没收违法所得; ④ 拒不改正或者情节严重的,处 10 万元以上 100 万元以下罚款,并可以责令暂停相关业务、停业整顿、关闭网站、由原发证机关吊销相关业务许可证或者吊销营业执照; ⑤ 对直接负责的主管人员和其他直接责任人员,处 1 万元以上 10 万元以下罚款。	新增
	5. 任何组织和个人不得制作、复制、发布、传播含有下列内容的信息,或者故意制作、复制、发布、传播含有下列内容的信息提供技术、设备支持或者其他帮助: (一)反对宪法所确定的基本原则,危害国家安全、荣誉和利益,泄露国家秘密,煽动颠覆国家政权,推翻社会主义制度,煽动分裂国家,破坏	☐	☐	针对互联网信息服务提供者、互联网网络接入服务提供者: 由网信部门、电信主管部门、公安机关 ① 责令改正; ② 给予警告; ③ 没收违法所得; ④ 拒不改正或者情节严重的,处 10 万元以上	新增

国家统一； (二) 宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，破坏民族团结，破坏国家宗教政策，宣扬邪教和封建迷信； (三) 编造、传播扰乱金融市场秩序的信息，以及其他扰乱市场秩序、经济秩序的虚假信息； (四) 编造、传播险情、疫情、警情、自然灾害、生产安全、食品药品等产品安全以及其他方面扰乱社会秩序的虚假信息； (五) 仿冒、假借国家机构、社会团体及其工作人员或者其他法人名义散布的信息，或者为实施违法犯罪而冒用他人名义散布的信息； (六) 散布煽动非法集会、结社、游行、示威或者其他扰乱社会管理秩序、破坏社会稳定的信息； (七) 传播淫秽色情、暴力、赌博、凶杀、恐怖的信息，以及教唆犯罪，传授犯罪手段、方法，制造或者交易违禁物品、管制物品，实施诈骗以及其他违法犯罪活动的信息； (八) 侮辱或者诽谤他人，侵害他人名誉、隐私、知识产权或者其他合法权益，以及危害未成年人身心健康，不利于未成年人健康成长的信息； (九) 法律、行政法规禁止的其他信息。(第 26 条)	☐ ☐	☐ ☐	100 万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、由原发证机关吊销相关业务许可证或者吊销营业执照； ⑤ 对直接负责的主管人员和其他直接责任人员，处 1 万元以上 10 万元以下罚款。 <u>针对其他单位或者个人：</u> 由网信部门、电信主管部门、公安机关 ① 给予警告； ② 责令限期改正； ③ 没收违法所得； ④ 对个人并处 1 万元以上 50 万元以下罚款，对单位并处 10 万元以上 100 万元以下罚款。	
6. 任何组织和个人不得违反国家规定，为他人获取、传播前款被依法阻断的信息而提供技术支持或者其他帮助。(第 27 条)	☐ ☐	☐ ☐	<u>针对互联网信息服务提供者、互联网网络接入服务提供者：</u> 由网信部门、电信主管部门、公安机关 ① 责令改正； ② 给予警告； ③ 没收违法所得；	新增

			④ 拒不改正或者情节严重的,处10万元以上50万元以下罚款,并可以责令暂停相关业务、停业整顿、关闭网站、由原发证机关吊销相关业务许可证或者吊销营业执照; ⑤ 对直接负责的主管人员和其他直接责任人员,处1万元以上10万元以下罚款。 <u>针对为他人获取、传播被依法阻断的信息而提供技术支持或者其他帮助的组织和个人:</u> 由公安机关 ① 没收违法所得; ② 处5日以下拘留,可以并处5万元以上50万元以下罚款; ③ 情节严重的,处5日以上15日以下拘留,可以并处10万元以上100万元以下罚款。 单位违反规定的,由公安机关 ① 没收违法所得; ② 处10万元以上100万元以下罚款; ③ 并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。	
7. <u>互联网信息服务提供者、互联网网络接入服务提供者</u> ,不得拒绝、阻挠网信部门、电信主管部门、公安机关和其他有关部门依法履行监督检查等执法职责。(第32条)	☐	☐	由网信部门、电信主管部门、公安机关 ① 给予警告; ② 责令限期改正; ③ 没收违法所得; ④ 拒不改正或者情节严重的,处10万元以上50万元以下罚款,并可以责令暂停相关业务、停业整顿、由原发证机关吊销相关业务许可证或者吊销营业执照; ⑤ 对直接负责的主管人员和其他直接责任人员,处1万元以上10万元以下罚款。	新增

附件二：《网络交易监督管理办法》合规义务清单

合规义务清单				
合规项	具体内容	是	否	违法责任
经营资质 登记	1. 网络交易经营者应依法办理市场主体登记。(第8条)	☐	☐	(虽然《管理办法》未直接明确相应的法律责任,但仍需参考其他适用规定)
	2. 个人从事的零星小额交易须依法取得行政许可的,应依法办理市场主体登记。(第8条)	☐	☐	
	3. 仅通过网络开展经营活动的平台内经营者申请登记为个体工商户的,可以将网络经营场所登记为经营场所,将经常居住地登记为住所,其住所所在地的县、自治县、不设区的市、市辖区市场监督管理部门为其登记机关。同一经营者有两个以上网络经营场所的,应当一并登记。(第9条)	☐	☐	
	4. 平台内经营者申请将网络经营场所登记为经营场所的,由其入驻的网络交易平台为其出具符合登记机关要求的网络经营场所相关材料。(第10条)	☐	☐	由市场监督管理部门 ① 责令限期改正; ② 逾期不改正的,处一万元以上三万元以下罚款。
区别公示	5. 网络交易经营者应在网站首页或者从事经营活动的主页面显著位置,持续公示经营者主体信息或者该信息的链接标识。鼓励链接到国家市场监督管理总局电子营业执照亮照系统,公示其营业执照信息。(第12条)	☐	☐	对于网络交易经营者: 由市场监督管理部门 ① 责令限期改正; ② 可处一万元以下罚款。 对于网络交易平台经营者: 由市场监督管理部门 ① 责令限期改正; ② 可处二万元以上十万元以下罚款; 情节严重的,处十万元以上五十万元以下罚款。
	(一) 已经办理市场主体登记的,应如实公示下列营业执照信息以及与其经营业务有关的行政许可等信息,或者该信息的链接标识: 1) 企业:营业执照登载的统一社会信用代码、名称、企业类型、法定代表人(负责人)、住所、注册资本(出资额)等信息; 2) 个体工商户:营业执照登载的统一社会信用代码、名称、经营者姓名、经营场所、组成形式等信息; 3) 农民专业合作社、农民专业合作社联合社:营业执照登载的统一社会信用代码、名称、法定代表人、住所、成	☐	☐	

	员出资总额等信息。(第 12 条) (二) 无需登记的经营者应根据自身实际经营活动类型, 如实公示以下自我声明以及实际经营地址、联系方式等信息, 或者该信息的链接标识: 1) “个人销售自产农副产品, 依法不需要办理市场主体登记”; 2) “个人销售家庭手工业产品, 依法不需要办理市场主体登记”; 3) “个人利用自己的技能从事依法无须取得许可的便民劳务活动, 依法不需要办理市场主体登记”; 4) “个人从事零星小额交易活动, 依法不需要办理市场主体登记”。(第 12 条) 8. 公示的信息发生变更的, 应当在十个工作日内完成更新公示。(第 12 条)	☐	☐	
个人信息保护	1. 网络交易经营者收集、使用消费者个人信息, 应当: i. 遵循合法、正当、必要的原则, 明示收集、使用信息的目的、方式和范围, 并经消费者同意。(第 13 条) ii. 公开其收集、使用规则, 不得违反法律、法规的规定和双方的约定收集、使用信息。(第 13 条) 2. 网络交易经营者收集、使用个人生物特征、医疗健康、金融账户、个人行踪等敏感信息的, 应当逐项取得消费者同意。(第 13 条) 3. 网络交易经营者及其工作人员应当对收集的个人信息严格保密。(第 13 条) 4. 网络交易经营者不得采用一次概括授权、默认授权、与其他授权捆绑、停止安装使用等方式, 强迫或者变相强迫消费者同意收集、使用与经营活动无直接关系的信息。(第 13 条) 5. 网络交易经营者未经被收集者授权同意, 不得向包括关联方在内的任何第三方提供。(第 13 条)	☐	☐	由市场监督管理部门 ① 责令限期改正; ② 可处五千元以上三万元以下罚款。
消费者权	1. 消费者评价中包含法律、行政法规、规章禁止发布或者传输的信息	☐	☐	(虽然《管理办法》未

益保护	的, 网络交易经营者可以依法予以技术处理。(第 15 条)			直接明确相应的法律责任, 但仍需参考其他适用规定)
	2. 网络交易经营者以直接捆绑或者提供多种可选项方式向消费者搭售商品或者服务的, 应以显著方式提醒消费者注意。(第 17 条)	☐	☐	
	3. 网络交易经营者应全面、真实、准确、及时地披露商品或者服务信息, 保障消费者的知情权和选择权。(第 19 条)	☐	☐	
	4. 网络交易经营者向消费者提供商品或者服务使用格式条款、通知、声明等的, 应当以显著方式提请消费者注意与消费者有重大利害关系的内容, 并按照消费者的要求予以说明。(第 21 条)	☐	☐	
	5. 网络交易经营者发送商业性信息时, 应明示其真实身份和联系方式, 并向消费者提供显著、简便、免费的拒绝继续接收的方式。(第 16 条)	☐	☐	由市场监督管理部门 ① 责令限期改正; ② 可处五千元以上三万元以下罚款。
	6. 网络交易经营者采取自动展期、自动续费等方式提供服务的, 应当 i. 在消费者接受服务前和自动展期、自动续费等日期前五日, 以显著方式提请消费者注意, 由消费者自主选择; ii. 在服务期间内, 应当为消费者提供显著、简便的随时取消或者变更的选项。(第 18 条)	☐	☐	
	7. 通过网络社交、网络直播等网络服务开展网络交易活动的网络交易经营者, 应当以显著方式展示商品或者服务及其实际经营主体、售后服务等信息, 或者上述信息的链接标识。(第 20 条)	☐	☐	由市场监督管理部门 ① 责令限期改正; ② 逾期不改正的, 处一万元以下罚款。
	8. 网络直播服务提供者对网络交易活动的直播视频保存时间自直播结束之日起不少于三年。(第 20 条)	☐	☐	
	9. 网络交易经营者应按照国家市场监督管理总局及其授权的省级市场监督管理部门的要求, 提供特定时段、特定品类、特定区域的商品或者服务的价格、销量、销售额等数据信息。(第 22 条)	☐	☐	由市场监督管理部门 ① 责令限期改正; ② 逾期不改正的, 处五千元以上三万元以下罚款。

10. 网络交易经营者自行终止从事网络交易活动的，应提前三十日在其网站首页或者从事经营活动的主页面显著位置，持续公示终止网络交易活动公告等有关信息，并采取合理、必要、及时的措施保障消费者和相关经营者的合法权益。（第 23 条）	☐	☐	<u>对于网络交易经营者：</u> 由市场监督管理部门 ③ 责令限期改正； ④ 可处一万元以下罚款。 <u>对于网络交易平台经营者：</u> 由市场监督管理部门 ③ 责令限期改正； ④ 可处二万元以上十万元以下罚款； ⑤ 情节严重的，处十万元以上五十万元以下罚款。
11. 网络交易经营者提供多种可选项方式的向消费者搭售商品或者服务的，不得将搭售商品或者服务的任何选项设定为消费者默认同意，不得将消费者以往交易中选择的选项在后续独立交易中设定为消费者默认选择。（第 17 条） 12. 网络交易经营者向消费者提供商品或服务使用格式条款、通知、声明等的，不得作出含有下列内容的规定： （一）免除或者部分免除网络交易经营者对其所提供的商品或服务应当承担的修理、重作、更换、退货、补足商品数量、退还货款和服务费用、赔偿损失等责任； （二）排除或者限制消费者提出修理、更换、退货、赔偿损失以及获得违约金和其他合理赔偿的权利； （三）排除或者限制消费者依法投诉、举报、请求调解、申请仲裁、提起诉讼的权利；（四）排除或者限制消费者依法变更或者解除合同的权利； （五）规定网络交易经营者单方享有解释权或者最终解释权；	☐ 	☐ 	（虽然《管理办法》未直接明确相应的法律责任，但仍需参考其他适用规定）

	(六) 其他对消费者不公平、不合理的规定。(第 21 条)			
	13. 网络交易经营者未经消费者同意或者请求,不得向其发送商业性信息。(第 16 条)	☐	☐	由市场监督管理部门
	14. 网络交易经营者消费者明确表示拒绝的,应当立即停止发送商业性信息,不得更换名义后再次发送。(第 16 条)	☐	☐	① 责令限期改正;
	15. 网络交易经营者采取自动展期、自动续费等方式提供服务的,在服务期间内,不得收取不合理费用。(第 18 条)	☐	☐	可处五千元以上三万元以下罚款。
核验身份 &信息	1. 网络交易平台经营者应要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息,进行核验、登记,建立登记档案,并至少每六个月核验更新一次。(第 24 条)	☐	☐	由市场监督管理部门
	2. 网络交易平台经营者对未办理市场主体登记的平台内经营者进行动态监测,对个人从事网络交易活动、年交易额累计超过 10 万元的,及时提醒其依法办理市场主体登记。(第 24 条)	☐	☐	① 责令限期改正;
	3. 网络交易平台经营者对平台内经营者及其发布的商品或者服务信息建立检查监控制度。(第 29 条)	☐	☐	② 逾期不改正的,处二万元以上十万元以下罚款;
	4. 网络交易平台经营者发现平台内的商品或者服务信息有违反市场监督管理法律、法规、规章,损害国家利益和社会公共利益,违背公序良俗的,应当依法采取必要的处置措施,保存有关记录,并向	☐	☐	③ 情节严重的,责令停业整顿,并处以十万元以上五十万元以下罚款。
				(虽然《管理办法》未直接明确相应的法律责任,但仍需参考其他适用规定)
				由市场监督管理部门
				① 责令限期改正;
				② 可处一万元以上三万元以下罚款。

	平台住所地县级以上市场监督管理部门报告。（第 29 条）			
报送信息	1. 依照法律、行政法规的规定，网络交易平台经营者应分别于每年 1 月和 7 月向住所地省级市场监督管理部门报送平台内经营者的下列身份信息： (一)已办理市场主体登记的平台内经营者的名称(姓名)、统一社会信用代码、实际经营地址、联系方式、网店名称以及网址链接等信息； (二)未办理市场主体登记的平台内经营者的姓名、身份证件号码、实际经营地址、联系方式、网店名称以及网址链接、属于依法不需要办理市场主体登记的具体情形的自我声明等信息； 其中，对从事网络交易活动、年交易额累计超过 10 万元的平台内经营者进行特别标示。（第 25 条）	☐	☐	由市场监督管理部门 ④ 责令限期改正； ⑤ 逾期不改正的，处二万元以上十万元以下罚款； ⑥ 情节严重的，责令停业整顿，并处以十万元以上五十万元以下罚款。
	2. 鼓励网络交易平台经营者与市场监督管理部门建立开放数据接口等形式的自动化信息报送机制。（第 25 条） 3. 网络交易平台经营者为平台内经营者依法履行信息公示义务提供技术支持。平台内经营者公示的信息发生变更的，应当在三个工作日内将变更情况报送平台，平台应当在七个工作日内进行核验，完成更新公示。（第 26 条）	☐ ☐	☐ ☐	(虽然《管理办法》未直接明确相应的法律责任，但仍需参考其他适用规定)
信息公示	1. 网络交易平台经营者以显著方式区分标记已办理市场主体登记的经营者和未办理市场主体登记的经营者，确保消费者能够清晰辨认。（第 27 条）	☐ ☐	☐ ☐	由市场监督管理部门 ① 责令限期改正； ② 可处一万元以上三万元以下罚款。
	2. 网络交易平台经营者修改平台服务协议和交易规则的，应当完整保存修改后的版本生效之日前三年的全部历史版本，并保证经营者和消费者能够便利、完整地阅览和下载。（第 28 条） 3. 网络交易平台经营者依据法律、法规、规章的规定或者平台服务协议和交易规则对平台内经营者违法行为采取警示、暂停或者终止	☐ ☐	☐ ☐	



	服务等处理措施的，应当自决定作出处理措施之日起一个工作日内予以公示，载明平台内经营者的网店名称、违法行为、处理措施等信息。警示、暂停服务等短期处理措施的相关信息应当持续公示至处理措施实施期满之日止。（第 30 条）			
信息保存	网络交易平台经营者对平台内经营者身份信息的保存时间自其退出平台之日起不少于三年；对商品或者服务信息、支付记录、物流快递、退换货以及售后等交易信息的保存时间自交易完成之日起不少于三年。法律、行政法规另有规定的，依照其规定。（第 31 条）	☐	☐	由市场监督管理部门 ⑦ 责令限期改正； ⑧ 逾期不改正的，处二万元以上十万元以下罚款； ⑨ 情节严重的，责令停业整顿，并处十万元以上五十万元以下罚款。
反不正当竞争	网络交易平台经营者不得违反《中华人民共和国电子商务法》第三十五条的规定，对平台内经营者在平台内的交易、交易价格以及与其他经营者的交易等进行不合理限制或者附加不合理条件，干涉平台内经营者的自主经营。具体包括： (一) 通过搜索降权、下架商品、限制经营、屏蔽店铺、提高服务收费等方式，禁止或者限制平台内经营者自主选择在多个平台开展经营活动，或者利用不正当手段限制其仅在特定平台开展经营活动； (二) 禁止或者限制平台内经营者自主选择快递物流等交易辅助服务提供者； 其他干涉平台内经营者自主经营的行为。（第 32 条）	☐ ☐ ☐	☐ ☐ ☐	由市场监督管理部门 ① 责令限期改正； ② 可处五万元以上五十万元以下罚款； 情节严重的，处五十万元以上二百万元以下的罚款。
配合监督	1. 经市场监督管理部门要求，网络交易平台经营者应提供提供有关的平台内经营者身份信息、商品或者服务信息、支付记录、物流快递、退换货以及售后等交易信息，并在技术方面积极配合市场监督管理部门开展网络交易违法行为监测工作。（第 34 条） 2. 为网络交易经营者提供宣传推广、支付结算、物流快递、网络接	☐ ☐	☐ ☐	(虽然《管理办法》未直接明确相应的法律责任，但仍需参考其他适用规定)

	入、服务器托管、虚拟主机、云服务、网站网页设计制作等服务的经营者(以下简称其他服务提供者),应当及时协助市场监督管理部门依法查处网络交易违法行为,提供其掌握的有关数据信息。法律、行政法规另有规定的,依照其规定。(第 34 条) 3. 市场监督管理部门发现网络交易经营者有违法行为,依法要求网络交易平台经营者、其他服务提供者采取措施制止的,网络交易平台经营者、其他服务提供者应当予以配合。(第 34 条)	☐	☐	
--	--	--------------------------	--------------------------	--

附件三：App收集使用个人信息企业自评估核对清单

【备注】

2020年3月19日，全国信息安全标准化技术委员会发布《网络安全标准2020自评估指南—移动互联网应用程序(App)收集使用个人信息自评估指南(征求意见稿)》(以下简称《2020自评估指南》)。我们将这份最新文件与2019年3月1日App违法违规收集使用个人信息专项治理工作组发布的《App违法违规收集使用个人信息自评估指南》(以下简称《2019自评估指南》)与2019年11月28日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局签发并于12月30日正式对外发布的《App违法违规收集使用信息行为认定方法》(以下简称《2019认定方法》)进行了全面比对，分析其异同并进行简要评析。

在此基础上，我们以2020年3月6日发布的国家标准GB/T 35273-2020《信息安全技术·个人信息安全规范》为导向，按照个人数据生命周期顺序并考虑到不同企业的需求，整合出目前关于App收集使用个人信息的企业自评估要点核对清单，以供相关企业在实践中参考。

注：2021年，随着《个人信息保护法》《常见类型移动互联网应用程序必要个人信息范围规定》等系列法律法规生效，监管对App提出了更多合规要求。附件三中表格系前期已发布的内容，具体评估项未细化到实践可操作层面且有待进一步更新。相关企业如有核查需要，欢迎垂询北京市环球律师事务所孟洁律师（联系方式见后附）。

App 收集使用个人信息企业自评估 Checklist					
评估维度	序号	具体评估项	企业自评		规定出处
			是	否	
1.形式要求	1	App 是否在首次运行或用户注册时通过弹窗等明显方式提示用户阅读隐私政策？	☐	☐	《2020 自评估指南》第 1.1 条
	2	用户进入 App 主功能界面后，是否可以通过 4 次（含）以内的点击访问到隐私政策？	☐	☐	《2020 自评估指南》第 1.3 条
	3	在 App 界面中是否能够找到隐私政策？（包括通过弹窗、文本链接、常见问题（FAQs）等形式）	☐	☐	《2020 自评估指南》第 1.1 条
	4	是否在 App 常规交互界面展示隐私政策？	☐	☐	《2020 自评估指南》第 1.3 条
	5	是否仅在注册/登录界面展示隐私政策或只能以咨询客服等方式查看隐私政策？	☐	☐	《2020 自评估指南》第 1.3 条
	6	App 在执行下一步注册/登录动作之前，是否主动提示用户阅读隐私政策等收集使用规则？	☐	☐	《2020 自评估指南》第 3.5 条
	7	隐私政策文本链接是否有效且可以正常显示？	☐	☐	《2020 自评估指南》第 1.2 条
	8	隐私政策链接是否使用灰色字体、缩小字号、键盘遮挡、置于边缘等方式未突出显示？	☐	☐	《2020 自评估指南》第 1.2 条
	9	隐私政策是否以单独成文的形式发布？	☐	☐	《2020 自评估指南》第 1.3 条
	10	隐私政策是否只是作为用户协议、用户说明等文件的一部分存在？	☐	☐	《2020 自评估指南》第 1.3 条
	11	隐私政策文本文字显示方式（字号、颜色、行间距、清晰度等）是否会造成阅读困难？	☐	☐	《2020 自评估指南》第 1.4 条
	12	隐私政策文本文字是否过小、或过密、或颜色过淡、或模糊不清？	☐	☐	《2019 认定方法》第一项第 4 条
	13	隐私政策内容是否符合通用的语言习惯、使用标准化的数字、图示？	☐	☐	《2020 自评估指南》第 1.4 条
	14	是否提供简体中文版隐私政策？	☐	☐	《2020 自评估指南》第 1.4 条
	15	隐私政策是否说明所适用的产品和服务范围及个人信息主体类型？	☐	☐	《个人信息安全规范》附录 D
	16	隐私政策是否详细列举 App 收集和使用个人信息的业务功能？	☐	☐	《个人信息安全规范》附录 D
	17	隐私政策是否对 App 运营者基本情况（至少包括组织或公司名称、注册地址或常用办公地址、及个人信息保护工作机构或相关负责人联系方式）进行描述？	☐	☐	《2020 自评估指南》第 1.6 条
	18	隐私政策是否明确外部争议解决机构（如法院、行业自律协会等）及其联络方式？	☐	☐	《个人信息安全规范》附录 D
	19	隐私政策是否说明发布、生效或更新日期？	☐	☐	《2020 自评估指南》第 1.6 条
	20	隐私政策中是否出现错别字或有歧义的语句？	☐	☐	《2020 自评估指南》第 1.4 条
	21	隐私政策中有关收集使用规则的内容是否简练、结构清晰、重点突出？	☐	☐	《2020 自评估指南》第 2.4 条
	22	隐私政策中有关收集使用规则的内容是否使用晦涩难懂的词语（如使用大量专业术语等）和冗长繁琐的篇幅？	☐	☐	《2020 自评估指南》第 2.4 条
	23	隐私政策中是否使用“等”“例如”等概括性语言综述或不完整列举？	☐	☐	《2020 自评估指南》第 2.1 条
	24	隐私政策中是否包含收集使用个人信息规则的相关内容？	☐	☐	《2020 自评估指南》第 1.1 条
	25	如 App 运营者将个人信息用于用户画像、个性化展示等，隐私政策是否说明其应用场景和可能对用户产生的影响？	☐	☐	《2020 自评估指南》第 1.6 条
	26	隐私政策是否对用户权利（包括个人信息查询、个人信息更正、个人信息删除、用户账户注销、撤回已同意的授权、获取个人信息的副本、对系统自动决策结果进行投诉）和相关操作方法进行明确说明？	☐	☐	《2020 自评估指南》第 1.6 条 《个人信息安全规范》第 5.5 条
	27	隐私政策是否对 App 运营者在个人信息保护方面遵循的基本原则采取的管理措施和技术手段和具备的安全能力进行说明？（如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等）（必要时可公开数据安全和个人信息保护相关的合规证明）	☐	☐	《2020 自评估指南》第 1.6 条 《个人信息安全规范》第 4 条 《个人信息安全规范》第 5.5 条
	28	隐私政策是否说明用户提供个人信息后可能存在的安全风险及不提供个人信息可能产生的影响？	☐	☐	《个人信息安全规范》第 5.5 条
	29	隐私政策是否表明在发生个人信息安全事件后会 App 及运营者及时告知用户并承担相应法律责任？	☐	☐	《个人信息安全规范》附录 D
	30	用户协议、服务协议、隐私政策等文件中是否出现免除自身责任、加重用户责任、排除用户主要权利条款？	☐	☐	《2019 自评估指南》第 14 条
3.更新	31	如隐私政策所载内容发生变化，隐私政策是否及时更新并通过电子邮件、信函、电话、推送通知等方式及时告知用户？	☐	☐	《个人信息安全规范》第 5.5 条 《个人信息安全规范》附录 D
	32	更新隐私政策，是否以信息、邮件、弹窗等方式提醒用户阅读发生变化的条款，并以适当方式通知用户收集个人信息的目的、方式、范围发生了变化？	☐	☐	《2020 自评估指南》第 2.2 条

个人敏感信息	33	在要求用户提供个人敏感信息时，App 是否通过显著方式（如弹窗提示、文字备注、文本链接等）同步、明确、易懂地告知用户其目的？	☐	☐	《2020 自评估指南》第 2.3 条	
	34	隐私政策是否对个人敏感信息类型进行显著标识和突出显示（如字体加粗、标星号、下划线、斜体、不同颜色等）？	☐	☐	《2019 自评估指南》第 8 条 《个人信息安全规范》第 5.5 条	
	35	App 收集、转让、共享个人敏感信息前，是否征得个人信息主体明示同意？	☐	☐	《个人信息安全规范》第 5.4 条	
	36	App 收集、转让、共享个人敏感信息前，是否告知共享、转让个人信息的目的、数据接收方的类型、可能产生的后果、涉及的个人敏感信息类型及数据接收方的身份和数据安全能力？	☐	☐	《个人信息安全规范》第 5.4 条	
	37	因业务需要，确需共享、转让个人生物识别信息的，是否征得个人信息主体的明示同意并单独、专门向个人信息主体告知目的、方式、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力以及存储时间等规则？	☐	☐	《个人信息安全规范》第 5.4 条 《个人信息安全规范》第 9.2 条	
个人信息收集	1.一般规定	38	在收集个人信息或打开可收集个人信息权限前，隐私政策是否完整、真实、清晰、准确地逐一说明各业务功能收集个人信息的目的、类型、方式、及范围？	☐	☐	《2020 自评估指南》第 2.1 条 《个人信息安全规范》附录 D
		39	隐私政策是否明确描述哪些类型的个人信息属于特定业务功能所必需？	☐	☐	《个人信息安全规范》附录 D
		40	App 运营者是否保证收集了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？	☐	☐	《2020 自评估指南》第 4.4 条 《个人信息安全规范》第 5.2 条
		41	App 运营者是否保证自动采集个人信息的频率是实现产品或服务的业务功能所必需的最低频率？	☐	☐	《个人信息安全规范》第 5.2 条
		42	收集个人信息的频度是否超出业务功能实际需要？	☐	☐	《2020 自评估指南》第 4.4 条
		43	App 运营者是否保证间接获取个人信息的数量是实现产品或服务的业务功能所必需的最少数量？	☐	☐	《个人信息安全规范》第 5.2 条
		44	App 是否仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息？	☐	☐	《2020 自评估指南》第 4.3 条
		45	在未打开 App 或后台运行 App 时，App 是否收集用户个人信息？（App 业务功能需要后台运行时继续提供服务除外，如导航功能）	☐	☐	《2020 自评估指南》第 4.4 条
		46	如 App 提供无需注册可使用（如浏览、游客）的业务模式，当用户拒绝支持浏览、游客等模式以外的个人信息收集行为时，App 是否拒绝提供服务？	☐	☐	《2020 自评估指南》第 4.2 条
	2.同意	47	App 收集个人信息前，是否获得个人信息主体的授权同意，提供由用户主动选择同意或不同意（包括退出、上一步、关闭、取消等）的选项？	☐	☐	《2020 自评估指南》第 3.1 条 《个人信息安全规范》第 5.4 条
		48	在首次运行 App 或用户注册时，是否采用默认勾选隐私政策等非明示方式征求用户同意？	☐	☐	《2020 自评估指南》第 3.5 条
		49	注册（包括登录即代表注册）的选项与同意隐私政策等的因果逻辑关系是否清楚？	☐	☐	《2020 自评估指南》第 3.5 条
		50	是否根据用户主动填写、点击、勾选等自主行为作为 App 各个业务功能打开或开始收集使用个人信息的条件？	☐	☐	《2020 自评估指南》第 4.3 条
		51	App 是否将同意收集其他业务功能所需的个人信息或同意打开其他业务功能所需可收集个人权限作为业务功能打开的前提条件？	☐	☐	《2020 自评估指南》第 4.2 条
		52	App 新增业务功能申请收集的个人信息超出用户原有同意范围时，是否因用户不同意而拒绝提供原有业务功能？（新增业务功能取代原有业务功能的除外）	☐	☐	《2020 自评估指南》第 4.3 条
		53	用户明确表示不同意收集后，App 是否在每次重新打开 App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意收集个人信息或询问是否同意打开可收集个人信息的权限以干扰用户正常使用？（用户选择使用 App 的某一具体功能触发征得同意的动作，不属于频繁干扰情形）	☐	☐	《2020 自评估指南》第 3.3 条
		54	App 设置用户选择同意与不同意的途径和方式是否同样方便？	☐	☐	《个人信息安全规范》第 5.3 条
	3.权限	55	未征得用户同意时，是否已经开始收集个人信息或打开可收集个人信息权限？	☐	☐	《2020 自评估指南》第 3.1 条
		56	App 未经用户同意是否私自更改用户设置的收集个人信息权限？	☐	☐	《2020 自评估指南》第 3.6 条
		57	是否以欺诈、诱导等不正当方式诱导用户同意收集个人信息或打开可收集个人信息的权限？	☐	☐	《2020 自评估指南》第 3.8 条
		58	App 是否以捆绑方式强制要求用户一次性同意打开多个可收集个人信息权限？（如将安卓版 App 的 targetSdkVersion 值设置低于 23，通过声明机制，在安装 App 时要求用户一次性同意打开多个可收集个人信息权限。）	☐	☐	《2020 自评估指南》第 4.3 条
		59	App 更新升级后是否自动将用户设置的权限恢复到默认状态？	☐	☐	《2020 自评估指南》第 3.6 条
		60	在申请打开可收集个人信息的权限（如：iOS 系统：定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康；Android 系统：日历、通话记录、相机、通讯录、位置、麦克风、电话、传感器、短信、存储）时，App 是否通过显著方式（如弹窗提示）同步告知用户其目的？	☐	☐	《2020 自评估指南》第 2.3 条
		61	App 是否收集与业务功能无关的个人信息或申请打开与业务功能无关的可收集个人信息的权限？	☐	☐	《2020 自评估指南》第 4.1 条
		62	App 收集业务功能非必要的个人信息或申请打开非必要权限时，是否向用户明示其目的并征得用户同意？	☐	☐	《2019 自评估指南》第 26 条
		63	用户是否可拒绝收集非必要信息或打开非必要权限？	☐	☐	《2020 自评估指南》第 4.2 条
		64	在用户通过拒绝提供个人信息、不同意收集使用规则、拒绝提供或关闭权限等操作明确拒绝 App 收集某类个人信息后，App 是否以任何形式收集该类个人信息或打开可收集个人信息的权限？	☐	☐	《2020 自评估指南》第 3.2 条
		65	App 在用户不同意收集非必要信息或打开非必要权限时，是否拒绝提供相应业务功能？	☐	☐	《2020 自评估指南》第 4.2 条



个人信息存储		66	个人信息存储时间是否最小化？	☐	☐	《个人信息安全规范》第 6.1 条
		67	隐私政策是否对个人信息存放地域(境内、境外哪个国家或地区)、存储期限(法律规定范围内最短期限或明确的期限)及超期处理方式 进行明确说明？	☐	☐	《2020 自评估指南》第 1.6 条
个人信息出境		68	如存在个人信息出境情形，隐私政策是否将个人出境信息类型列出并显著标识（如字体加粗、标星号、下划线、斜体、不同颜色等）？	☐	☐	《2020 自评估指南》第 1.6 条
		69	如果因业务需求、政府和司法监管要求存在跨境信息传输情况，隐私政策是否详细说明需要进行跨境传输的数据类型，以及跨境传输遵守的标准、协议和法律机制(合同等)？	☐	☐	《个人信息安全规范》附录 D
		70	如不存在个人信息出境情形，隐私政策是否进行明确说明？	☐	☐	《2020 自评估指南》第 1.6 条
		71	如委托的第三方或嵌入的第三方代码、插件直接将个人信息传输至境外，是否明确说明跨境传输个人信息的目的、类型和接收方等？	☐	☐	《2020 自评估指南》第 2.1 条
个人信息使用		72	个人信息的使用是否超出与收集个人信息时所声称的目的具有直接或合理关联的范围？	☐	☐	《个人信息安全规范》第 7.3 条
		73	如个人信息收集和使用目的发生变化，App 是否说明并再次征得用户同意？	☐	☐	《2020 自评估指南》第 3.10 条
个人信息委托处理、转让、共享、公开披露		74	App 运营者作出委托行为是否超出已征得个人信息主体授权同意的范围？	☐	☐	《个人信息安全规范》第 9.1 条
		75	如存在个人信息对外共享、转让等情况，是否事先征得个人信息主体的授权同意？	☐	☐	《个人信息安全规范》第 9.2 条
		76	如存在个人信息对外共享、转让等情况，隐私政策是否明确对外共享、转让个人信息的目的、涉及的个人信息类型、接收方类型或身份、接收方使用个人信息的目的、对数据接收方的管理约束规则、转让、共享中的安全措施、可能产生的后果(是否产生高风险)以及各自的安全和法律责任？	☐	☐	《2020 自评估指南》第 1.6 条 《个人信息安全规范》第 5.5 条 《个人信息安全规范》第 9.2 条 《个人信息安全规范》附录 D
		77	既未经用户同意也未做匿名化处理的情况下，个人信息传输至 App 后台服务器后，App 运营者是否向第三方提供其收集的个人信息？	☐	☐	《2020 自评估指南》第 5.1 条
		78	如 App 违反法律法规规定或违反与用户的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，App 运营者是否立即停止共享、转让的行为并通知第三方及时删除？	☐	☐	《个人信息安全规范》第 8.3 条
		79	经法律授权或具备合理事由确需公开披露时，是否说明原因、事先征得个人信息主体明示同意、向个人信息主体告知公开披露个人信息的目的、类型，是否对个人信息主体带来高危风险，并准确记录和存储个人信息的公开披露的情况？	☐	☐	《个人信息安全规范》第 9.4 条 《个人信息安全规范》附录 D
个人信息主体权利	1. 查询、更正、删除	80	App 是否提供有效的查询、更正、删除个人信息的途径？	☐	☐	《2020 自评估指南》第 6.2 条
		81	查询、更正和删除个人信息的过程是否简单易操作？	☐	☐	《2020 自评估指南》第 6.2 条
		82	对查询、更正和删除个人信息是否设置不必要或不合理的条件？	☐	☐	《2020 自评估指南》第 6.2 条
		83	用户更正、删除个人信息或注销用户账号等操作已执行完毕时，App 后台是否同步执行完成？	☐	☐	《2020 自评估指南》第 6.2 条
	2. 注销	84	App 是否提供有效的注销账号的途径（如在线操作、客服电话、电子邮件等）？	☐	☐	《2020 自评估指南》第 6.1 条
		85	注销账号的过程是否简单易操作？	☐	☐	《2020 自评估指南》第 6.1 条
		86	注销账号是否设置不必要或不合理的条件？	☐	☐	《2020 自评估指南》第 6.1 条
		87	注销如需要身份核验，要求用户再次提供的个人信息类型是否多于注册、使用等服务环节收集的个人信息类型？	☐	☐	《个人信息安全规范》第 8.5 条
		88	注销过程是否提出额外要求增加用户义务？（如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等）	☐	☐	《个人信息安全规范》第 8.5 条
		89	注销账号需要提供额外的个人敏感信息用于身份验证时，是否明确注销所需个人敏感信息在注销成功后会立即删除或做匿名化处理？	☐	☐	《2020 自评估指南》第 6.1 条 《个人信息安全规范》第 8.5 条
		90	用户注销账户后，App 是否及时删除个人信息或进行匿名化处理？（法律法规另有规定的除外）	☐	☐	《2020 自评估指南》第 6.1 条
		91	因法律法规规定需要在注销后留存个人信息的，是否将其再次用于日常业务活动中？	☐	☐	《个人信息安全规范》第 8.5 条
	3. 响应请求	92	如果个人信息主体行使权利的过程产生费用，个人信息控制者是否明确说明收费的原因和依据？	☐	☐	《个人信息安全规范》附录 D
		93	如果个人信息主体提出行使权利的需求后需要较长时间才能响应，个人信息控制者是否明确说明响应的时间节点，以及无法短时间内响应的原因？	☐	☐	《个人信息安全规范》附录 D
		94	查询、更正、删除个人信息的在线操作请求是否可以在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理？	☐	☐	《2020 自评估指南》第 6.2 条
		95	如用户无法通过在线操作方式及时响应个人信息查询、更正、删除请求（需要人工处理的），App 运营者是否在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理？	☐	☐	《2020 自评估指南》第 6.2 条
		96	受理注销账号请求后，App 运营者是否在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理？	☐	☐	《2020 自评估指南》第 6.1 条
		97	如果个人信息控制者拒绝个人信息主体对个人信息进行访问、更正、删除、撤回授权同意等的要求，是否明确说明拒绝的原因和依据？	☐	☐	《个人信息安全规范》附录 D

	4.投诉管理	98	App 运营者是否建立并公布可受理个人信息安全问题相关的投诉、举报渠道（包括在线操作、客服电话、电子邮件等方式）？	☐	☐	《2020 自评估指南》第 6.3 条
		99	隐私政策中是否至少提供以下一种申诉渠道：1）电子邮件；2）电话；3）在线客服；4）在线表单？	☐	☐	《2020 自评估指南》第 1.6 条
		100	App 运营者是否妥善受理用户关于个人信息相关的投诉、举报？	☐	☐	《2020 自评估指南》第 6.3 条
		101	App 运营者是否在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理投诉和举报？	☐	☐	《2020 自评估指南》第 6.3 条
	5.拒绝定向推送	102	App 是否存在利用用户个人信息合算法定向推送信息的情形？（包括利用个人信息和算法推送新闻和信息、展示商品、推送广告等）	☐	☐	《2020 自评估指南》第 3.7 条
		103	App 是否提供拒绝接受定向推送信息、或者停止、退出、关闭相应功能的机制？	☐	☐	《2020 自评估指南》第 3.7 条
		104	App 是否提供不基于个人信息、用户画像等推送（即非定向推送信息）的模式、选项？	☐	☐	《2020 自评估指南》第 3.7 条
	6.撤回同意	105	App 是否向用户提供撤回同意收集个人信息的途径、方式并在隐私政策等使用规则中予以明确？	☐	☐	《2020 自评估指南》第 3.9 条
		106	用户撤回同意后，App 是否还在处理相应的个人信息？	☐	☐	《个人信息安全规范》第 8.4 条
		107	如用户拒绝或撤回特定业务功能收集个人信息的授权，App 是否暂停提供其他业务功能或降低其他业务功能的服务质量？	☐	☐	《2020 自评估指南》第 3.9 条
		108	用户拒绝或撤回可收集个人信息的权限是否会影响用户正常使用与该权限无关的功能？（该权限是保证 App 正常运行所必须的除外）	☐	☐	《2020 自评估指南》第 3.9 条
第三方接入（含 SDK）		109	如 App 接入第三方应用，用户使用第三方应用的情况下，App 是否未事先征得用户同意就向第三方应用提供个人信息？（用户获知应用为第三方且知悉收集使用个人信息规则后，自行同意提供给第三方的除外）	☐	☐	《2020 自评估指南》第 5.1 条
		110	App 接入第三方应用时，是否提醒用户关注第三方应用收集使用个人信息的规则？	☐	☐	《2020 自评估指南》第 4.4 条
		111	如 App 嵌入了第三方代码、插件（如 SDK）收集个人信息，是否以隐私政策、弹窗提示、文字备注、文本链接等形式说明第三方类型，及收集个人信息的目的、类型、方式？	☐	☐	《2020 自评估指南》第 2.1 条
		112	App 是否私自截留第三方应用收集的个人信息？	☐	☐	《2020 自评估指南》第 4.4 条
		113	既未经用户同意也未做匿名化处理的情况下，App 是否从客户端直接向第三方发送个人信息（包括通过 App 客户端嵌入第三方代码、插件 SDK 等方式）？	☐	☐	《2020 自评估指南》第 5.1 条
Cookie 等同类技术		114	如 App 内使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接等）收集个人信息，是否向用户说明使用该等技术收集个人信息的目的、类型、方式？	☐	☐	《2020 自评估指南》第 2.1 条
		115	在征得用户同意前，App 是否利用 Cookie 等同类技术或私自调用可收集用户个人信息权限等方式收集个人信息？	☐	☐	《2020 自评估指南》第 3.1 条



环球数据合规团队 编制

主编：孟洁

邮箱/E. mengjie@glo.com.cn

电话/T. (86 10) 6584 6768

手机/M. (86 10) 158 1105 0850

参编：

高亚鹏、李楠、戴畅

订阅/E.

dataprotection@glo.com.cn

请您知悉，本集锦的所有内容均不构成任何形式的法律意见。

如您欲进一步了解本集锦所涉及的内容，您可以通过上述方式联系我们。

版权声明

本报告每篇文章版权属于相应作者所有或者共有，并受法律保护。您可以转载、摘编方式使用本报告每篇文章的文字或者观点，但不得对本报告所选取的文章进行改编、汇编、翻译或出版。在使用时应注明每篇文章（包括附件）的“来源”以及作者名字。违反上述声明者，将追究其相关法律责任。



扫二维码 | 关注我们

M姐 数据合规评论

微信号 | [M_DigitalLawandLife](#)



环 球 律 师 事 务 所
GLOBAL LAW OFFICE

主编简介

孟洁



孟洁 | 合伙人

环球律师事务所
mengjie@glo.com.cn

执业资格

中国执业律师

孟洁律师为环球律师事务所常驻北京的合伙人。主要执业领域为网络安全、个人信息与隐私保护、互联网、电商合规、反腐败反商业贿赂合规、垄断与不正当竞争合规。

孟律师曾在诺基亚等世界五百强跨国公司和知名律师事务所工作超过十余年，担任知名人工智能独角兽公司总法律顾问、DPO。曾经及目前向大型跨国公司、知名互联网企业、车企、IoT、电信、云服务、人工智能、电商、金融、医疗、工业互联网、广告、大数据等领域的国内外企业提供境内/境外的数据合规体系建设与数据合规专项及常年法律服务，总结出不少可落地的实操方法论，颇受客户好评。

孟律师曾是国际隐私保护协会（IAPP）中国区联席主席；成为钱伯斯2022年“数据隐私保护”和“TMT”领域的上榜律师；被LEGAL 500评为2020年“TMT领域特别推荐律师”；2021及2022年连获“TMT领域领军人物”“数据保护领域领军人物”“Fintech领域头部律师”；被LEGALBAND评为“2021年中国律师特别推荐榜：消费与零售”“2021年中国律师特别推荐榜：汽车与新能源”“网络安全与数据合规特别推荐15强”“2020年中国律师特别推荐榜15强：网络安全与数据合规”；被北京市律协评为全国千名涉外专家律师。

孟律师在各大期刊、公号发表过数百篇专业文章、著作，并且，与中国信息通信研究院合著《SDK安全与合规白皮书》V1.0版与V2.0版，与中国信息通信研究院和南都个人信息保护研究中心共著《个性化展示安全与合规报告》，与威科数据库合作出版《数据全球化与隐私保护指引》，与小米集团合作发布《Cookie合规指引报告》，与微软公司合作发布《国内外标准兼容下的个人信息合规体系建构》，以及单独发布的《个人信息保护监管要求对标分析报告（2021版）》《致礼2022成熟的数据合规年——监管动态总结与趋势预判》。近期，《新技术新应用数据合规指引》《从TCF框架看单独同意获取的落地方式》等报告也将陆续发布。

环球律师事务所

环球律师事务所由中国国际贸易促进委员会在1979年创建，是中国改革开放后成立的第一家律师事务所。经过四十多年来的不懈努力和发 展，我们已成为中国律师业中最优秀的大型综合性律师事务所之一。

自成立伊始，我们即确立了“以国际化的视野、国际化的团队、国际化的质量服务于国内外客户”的宗旨，这使我们置身于多变的全球经济形势之中，却始终能够保持不变的业界领先地位。我们连续多年被众多的国内外权威法律评级机构评选为顶级的中国律师事务所之一，包括《钱伯斯》、《法律500强》、《亚洲法律杂志》等。

我们的律师均毕业于中国一流的法学院，其中绝大多数律师拥有法学硕士以上的学历，多数律师还曾学习或工作于北美、欧洲、澳洲和亚洲等地一流的法学院和国际性律师事务所，部分合伙人还拥有美国、英国、澳大利亚、瑞士、新西兰、香港等地的律师执业资格。

我们能够来自广泛行业的国内外客户，提供跨业务领域综合的一站式法律服务。我们深耕的行业包括但不限于银行、金融、保险、证券、投资、贸易、能源、矿业、化工、钢铁、制造业、交通运输、基础及公共设施、生命科学及医疗、电信、传媒、高科技、文娱体育、房地产、酒店休闲、餐饮、大消费等众多的细分领域。

四十多年来，我们凭借精湛的法律知识、丰富的执业经验、高度的敬业精神以及良好的职业道德，向国内外客户展示和证明了我们的价值，同时也赢得了国内外客户的信赖。在未来的日子里，我们将继续凭借我们独到的优势助力国内外客户取得更为持久和长远的成功。



北京总部



上海办公室



深圳办公室



成都办公室

中国领先的律
师事务所
逾700名专业律师



环球监管与合规业务

- 作为该领域最佳律师事务所之一，我们在法律风险评估、合规政策制定、合规培训、合规调查以及违规举报等方面具有丰富的经验，能够提供客户在合规与风控方面所需要的所有法律服务。我们能够帮助企业、金融机构、专业服务机构、政府和非政府组织以及企业家发现行业及法律监管方面的漏洞，理顺监管和报告体系，制定并落实有效的预防措施。当客户面临监管机关的调查时，我们能够在第一时间内指导客户依法有效地应对调查。
- **我们能够帮助客户建立有效的合规与风控体系。**我们能够帮助企业、金融机构、专业服务机构、政府和非政府组织以及企业家发现行业及法律监管方面的漏洞，理顺监管和报告体系，制定并落实有效的预防措施。同时，我们能够通过对风险的预判、分析、处置，为企业建立有效的法律风险控制体系，控制或降低企业运营、流程操作中存在的潜在风险，帮助企业提高防范和化解法律风险的能力，保障企业高效稳健安全运营，提高经营管理水平，增强竞争力。
- **我们能够帮助客户依法应对各种法律风险事件和法律合规调查。**企业一旦出现相关风险事件，我们将会在第一时间介入和分析，从而提出解决方案和媒体沟通方案。发现和核实企业内部风险事件的线索，协助企业进行日常的合规调查和处理。当客户面临监管机关的调查时，我们能够在第一时间内指导客户依法有效地应对调查。
- **我们能够为企业的合规与风控工作提供全面而及时的法律信息服务支持。**我们可以帮助企业收集相关行业领域新出台的法律法规和相关负面新闻。例如，在央视3·15后，紧急开展对相关监管信息的研判，帮助被点名企业顺利完成整改合规工作等；在《常见类型移动互联网应用程序必要个人信息范围规定》以及主管部门的整改通知发出后，预先将有关分析报告递交相关客户，协助客户有效改进数据合规落地工作，在关键时刻作客户的坚强后盾。

环球网络安全与数据合规业务

- **境内、外丰富的数据合规经验。**团队律师们长期从事各国数据保护法的实务与研究，曾经翻译过美国、欧盟、印度、巴西、俄罗斯等国的数据保护法案，撰写过大量数据与隐私保护方面的专著与文章。已经完成的数据合规项目涵盖了广泛的行业，包括互联网、通讯、IoT（含车联网）、媒体内容、文化娱乐、银行、保险、投资担保公司、金融科技、医疗健康与医药、教育、汽车（自动驾驶）、电器、制造业等。代表中国企业“走出去”项目中涉及支持境外法域数据合规的国家已经多达三十几个，帮助客户搭建及完善全球统一化的数据合规体系。
- **企业内、外部的数据合规经验。**我们的团队律师有1/3曾在企业法务从事企业内部产品研发和运营合规工作的实务经验。并且，他们在公司内部从事法律工作。我们对公司一线业务有更为深入的认知，能够更清晰明确地了解客户的实际需求，为我们的客户提供更贴合业务实际情况的个性化法律服务，从而指导企业如何进行合规落地，为客户提供满足其商业运营需求和产品与技术结合发展需要的优质法律服务。
- **前、中、后端相结合的数据合规经验。**我们的合伙人深入一线积极参与各法律法规的征求意见反馈及标准的制定，熟谙前沿法规政策动态，与国家和地方政府机构有良好的沟通咨询与磋商经验。我们还有长期战略合作的外部技术专家与PR专家团队，可协同提供专业的数据合规技术服务与数据危机处理的整体化解决方案。
- **面向技术和产品落地方案实现的合规建议。**环球律师事务所是标准化制定组织TC260成员单位之一，积极参与各项标准的立项与制定的讨论，有着行业内领先的解决问题的能力。我们与中国信息通信研究院建立长期合作关系，如您需要提供技术支持/测评时，信通院将与我们提供一体化的解决方案。
- **快速高效响应客户需求。**我们的律师团队在业内以“提供服务时反应迅速”而闻名。我们的客户普遍对我们提供服务时反应速度之快感到满意。我们十分清楚地认识到，客户的任何需求都期待我们在第一时间给予答复和反馈。我们也意识到，只有以最快的反应速度来提供法律服务才是赢得市场的最好法宝和回报客户对我们的信任的最佳方式。因此，我们的服务宗旨是在力所能及的范围内、以最快的反应速度向客户交出满意的“答卷”。在我们“以非常快的速度”来回应客户的法律需求的同时，我们所提供的法律服务仍然可以达到优秀的水平。

环球律师事务所

2021年度业界嘉许

- 通信媒体业务位列“领先的中国律师事务所”，《钱伯斯亚太》
 - 科技、媒体与通信业务位列“领先的律师事务所”，《亚太法律五百强》
 - 科技、媒体与通信业务位列“领先的中国律师事务所”，《LEGALBAND》
 - 科技与电信业务位列“领先的中国律师事务所”，《亚洲法律概况》
 - 媒体及娱乐业务位列“领先的中国律师事务所”，《亚洲法律概况》
-
- 数据保护业务位列“领先的中国律师事务所”，《亚太法律五百强》
 - 网络安全与数据业务位列“一流的律师事务所”，《LEGALBAND》

该团队活跃于TMT领域，运用其丰富的私募股权融资经验，为高科技等企业就各类并购和投融资业务提供全方位的法律服务。并在数据保护和隐私方面提供专业的法律服务。

——《钱伯斯亚太2021》

给一位客户留下深刻印象：
“他们在文件起草及审查、
尽职调查方面一丝不苟。”

——《钱伯斯亚太2021》



环球律师事务所

Chambers
AND PARTNERS

数据保护业务位列“领先的中国律师事务所”

《亚太法律五百强》
2021

LEGAL
500

合规业务位列
“领先的中国律师事务所”

《亚太法律五百强》
2018 - 2020

asialaw
PROFILES

合规业务位列
“领先的中国律师事务所”

《亚洲法律概况》
2019 - 2022

CHINA BUSINESS
LAW JOURNAL

荣获“年度卓越律所大奖
——企业合规”

《商法杂志》
2020

CHINA BUSINESS
LAW JOURNAL

荣获“年度卓越律所大奖
——反腐败及合规”

《商法杂志》
2019

LEGALBAND

合规业务位列
“一流的中国律师事务所”

《LEGALBAND》
2021

LEGALBAND

合规业务位列
“顶级的中国律师事务所”

《LEGALBAND》
2020

LEGALBAND

合规业务位列
“领先的中国律师事务所”

《LEGALBAND》
2016 - 2019

LEGALBAND

网络安全与数据业务业务位列
“一流的中国律师事务所”

《LEGALBAND》
2019 - 2021

ASIAN LEGAL
BUSINESS

TMT业务提名
“年度沿海地区科技、媒体与
电信律师事务所大奖”

《亚洲法律杂志》
2021

ASIAN LEGAL
BUSINESS

合规业务提名
“年度沿海地区合规律师事务
所大奖”

《亚洲法律杂志》
2021

ASIAN LEGAL
BUSINESS

合规业务提名
“年度最佳合规律师事务所大奖”

《亚洲法律杂志》
2014 - 2016、2018 - 2021

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层
邮编: 100025
15 & 20/F Tower 1,
China Central Place,
No. 81 Jianguo Road, Chaoyang
District, Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市徐汇区淮海中路999号
环贸广场办公楼一期35层&36层
邮编: 200031
35 & 36/F
Shanghai One ICC, No. 999
Middle Huai Hai Road, Xuhui District,
Shanghai 200031, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区深南大道9668号
华润置地大厦B座27层
邮编: 518052
27/F Tower B,
China Resources Land Building,
No. 9668 Shennan Avenue, Nanshan
District, Shenzhen 518052, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987

成都市高新区天府大道北段966号
天府国际金融中心11号楼37层
邮编: 610041
37/F Building 11,
Tianfu International Finance Center,
No. 966 Tianfu Avenue North Section,
High-tech Zone, Chengdu 610041, China
电话/T. (86 28) 8605 9898
传真/F. (86 28) 8313 5533

