30th ANNIVERSARY 1992 2022

大成 DENTONS

DENTONS CHINA

「大成 30 周年所庆文集」

企业涉个人信息刑事风险合规风控研究报告

大成律师事务所

课题
主持人

吴沈括

高级顾问

地点：大成北京
专业领域：数字治理、跨境投资与贸易、公司与并购、刑事、争议解决

CONTENTS

前言

2021 年 8 月 20 日，历经三次审议，十三届全国人大常委会第三十次会议表决通过了《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》)，并将于 2021 年 11 月 1 日起正式施行。《个人信息保护法》总计 8 章 74 条，根据宪法，在总则、个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任以及附则等八个方面建构制度体系，在条文设计上吸收国际立法、回应中国实际，覆盖全行业全部门以及个人信息流转利用全生命周期，旨在实现保护个人信息权益、规范个人信息处理活动和促进个人信息合理利用的三重立法目的。

整体而言，《个人信息保护法》的法律责任和处罚强度位列全球前列，备受各业关注。特别是在刑事责任和刑事处罚层面明确规定“构成犯罪的，依法追究刑事责任”(第 71 条)，使中国和意大利、法国并列成为动用刑法惩治个人信息相关违法行为的三大主要国家。并且中国《刑法》和《网络安全法》等法律结合规定的剥夺自由刑罚(最高有期徒刑 7 年)、剥夺资格刑罚（最长终身禁止从业）以及特有的单位犯罪制度（单位和个人双重处罚），实质上决定了《个人信息保护法》具备全球最严厉的刑事处罚效力。

《个人信息保护法》全面施行背景下，各大企业面临的最直接刑事风险聚集在《刑法》第 253 条之一所规定的侵犯公民个人信息罪。从该罪名规定的历史沿革看：

(1) 该罪名源自 2009 年《刑法修正案(七)》增加规定的出售、非法提供公民个人信息罪和非法获取公民个人信息罪；

(2) 而后经过 2015 年《刑法修正案(九)》的整合形成侵犯公民个人信息罪，扩大了犯罪主体侵犯公民个人信息犯罪行为的范围。

(3) 2017 年最高人民法院、最高人民检察院联合出台《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，进一步细化侵犯公民个人信息罪的司法适用规则，并就外国人个人信息、行踪轨迹等个人信息特别种类、涉案个人信息计算规则以及从宽处罚等司法焦点问题做出全面回应。

(4) 2018 年最高人民检察院出台《检察机关办理侵犯公民个人信息案件指引》，对侵犯公民个人信息罪的具体罪状进行了明确，对公民个人信息的具体内容、非法获取、出售或提供公民个人信息的具体涉罪行为、涉罪情节等进行了规定。

(5) 2020 年最高人民检察院就整治网络黑灰产业链、提升移动互联网监管执法能力、加大未成年人网络保护力度向工业和信息化部发出第六号检察建议。

(6) 2021 年《个人信息保护法》的颁布施行，对公民个人信息收集、处理的合法程序，以及信息收集处理主体的法律责任等进行了明确的规制，厘定了公民个人信息商业化利用的边界，在刑事司法领域将全面重塑侵犯公民个人信息罪各项构成要件的内涵外延和各级司法裁判活动的运行逻辑。

（图 1：侵犯公民个人信息罪的历史沿革）

本报告立足《个人信息保护法》出台施行的现实背景，通过法律法规梳理、文献著述洞察、司法案例分析，着眼企业涉个人信息刑事风险的合规风控，结合各地区各层级司法机关有关侵犯公民个人信息罪的刑事裁判实践，梳理企业涉侵犯公民个人信息罪的司法态势、司法焦点和司法走向，分析企业涉侵犯公民个人信息罪的行为特征、人员特征和责任特征，并就企业涉侵犯公民个人信息罪的技术风控、组织风控和人员风控提出合理化建议。

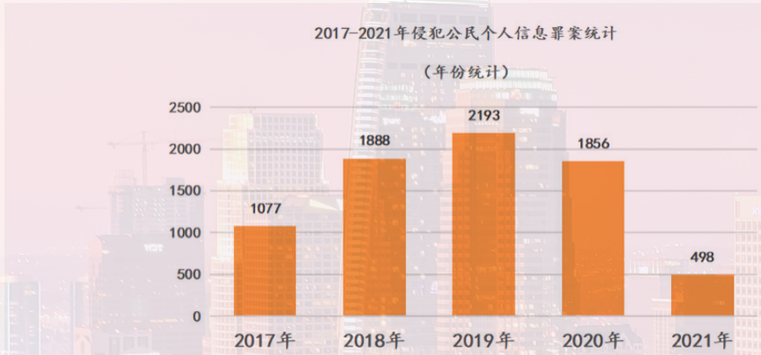
第一章

企业涉侵犯公民个人信息罪的司法态势

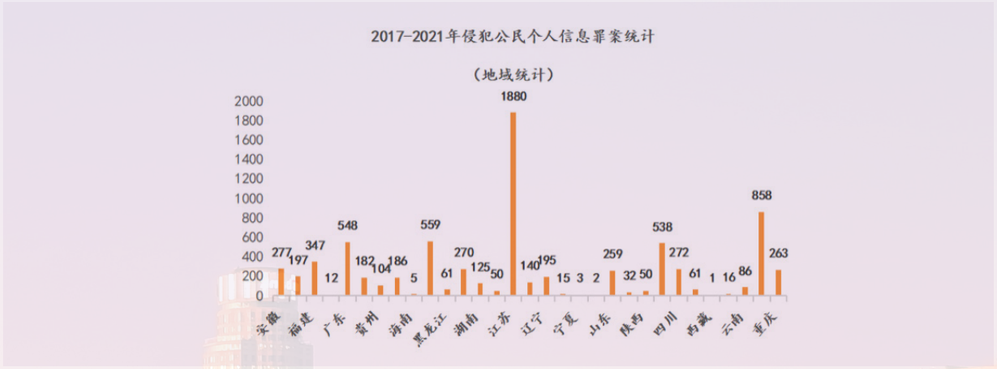
一、企业涉侵犯公民个人信息罪的司法态势

当下中国进入“高质量发展新阶段”，各地区各行业数字化转型加速，数字经济、数字政府和数字社会发展迅速。伴随以数据（个人信息）驱动的各类新型经济模式和商业应用的发展，个人信息的价值日益凸显，成为最重要的基础元素。由此也滋生了对各类数据、信息权益的侵犯行为，特别是公民个人信息被非法收集、泄露、滥用的违法违规案件发生率持续走高，成为行政监管和刑事司法的高压红线区域。

刑事司法裁判大数据显示，网络空间、数字环境已经成为侵犯公民个人信息罪的首要领域，而数字企业作为个人信息收集和处理的主体，往往因为未能洞悉把握明晰的法律规则边界、建立健全全面的合规风控体系，在个人信息相关的技术产品服务研发、业务运营推广、内部人事组织以及商业伙伴管理等方面容易违反刑事法律或者牵涉其中，触发个人和单位刑事责任风险，也是目前刑事司法机关高度专注的重点风险人群和对象。



特别是就侵犯公民个人信息罪而言，与之前不同的是，在数据信息成为数字经济下的生产要素、企业拓展数字盈利模式乃至形成各个行业数据汇聚态势的背景下，公民权益、产业利益、公共和国家安全等多重法益错综交织，一方面推动该罪刑事打击的广度和力度持续走高，另一方面也推动该罪刑事司法的精细化运行，并日益注重对企业内外业务的穿透式、整体性、实质性刑事评价。总体而言，侵犯公民个人信息罪的刑事司法已经对数字企业的业务模式和运营流程等重大方面产生显著影响，并且在《个人信息保护法》全面施行的大环境下，《刑法》与《个人信息保护法》等法律法规的结合适用将作为“红线因素”进一步冲击和改造数字企业在技术研发应用、组织人事架构及整体商业生态层面的现有格局。

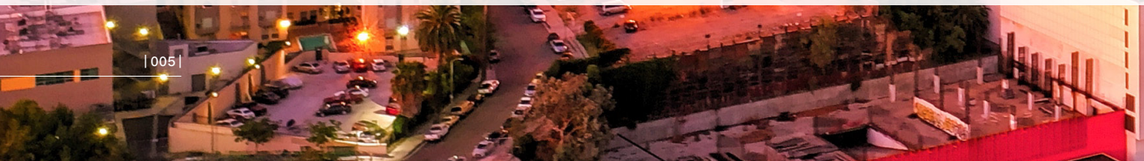


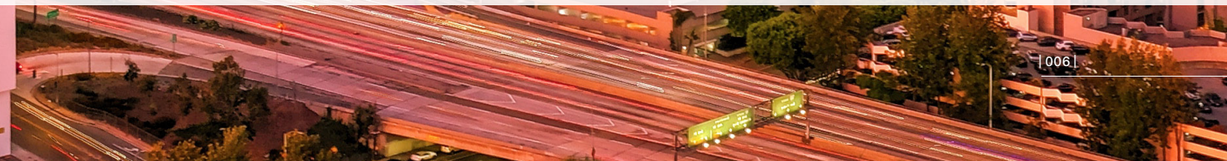
有关侵犯公民个人信息罪的刑事司法裁判大数据显示，自 2017 年《网络安全法》正式施行以来，侵犯公民个人信息罪案发生数量逐年激增，处于高发态势，而且与电信网络诈骗、敲诈勒索、绑架等犯罪呈合流态势，社会危害严重。2017 年 6 月至 2021 年 6 月，全国法院新收侵犯公民个人信息刑事案件 10059 件，审结 9743 件，生效判决人数 21726 人，对 3803 名被告人判处三年以上有期徒刑，比例达 17.50%。从刑事司法现状来看，呈现三大主要特征：

(1) 刑事处罚案件与行政处罚案件同步增长。随着个人信息相关行政监管力度的持续走强，行政处罚案件数量逐年递增，2021 年截止目前的案件数量已经超过了 2020 年的整年数量。与此同时，行政执法中的“刑案移送”以及“一案双查”等机制也推动了刑事处罚案件的实际上升，反映了行政监管与刑事司法日趋紧密的互动态势。

(2) 单位犯罪案件与自然人犯罪案件同步增长。目前单位作为受罚主体的案件数量已占据全国总体违法行为和行政处罚情况的 50% 以上，在刑事司法领域，单位犯罪案件的数量也是逐年增多，同时也是各级刑事司法机关在强化个人信息刑法保护中的重点查办对象。

(3) 2020 年和 2021 年的刑事裁判数量相对回落，并非外界解读的“总体形势好转、打击力度下降”。一方面是因为刑事案件诉讼周期较长，完整、准确案件数量的统计外显有时间后延的规律，另一方面，相当比例的刑事案件因为案情复杂，办案机关放缓诉讼进度，以等待新的法律法规的出台，在“从旧兼从轻”原则指引下为刑事裁判提供更为匹配、直接的法律依据。





二、企业涉侵犯公民个人信息罪的司法焦点

目前各级刑事司法机关在侦办侵犯公民个人信息罪案件过程中，针对数字企业单位犯罪案件，重点关注涉事企业在业务运营中：（A）各类个人信息的获取合法性情况（包括是否依法获得相关主体有效的二次授权等）、（B）入罪门槛条件（涉案个人信息特别是敏感个人信息的种类、重复涉案个人信息的去重计算等）以及（C）公民个人信息的违法处理情况（特别是各种个人信息的非法留存、非法出售、非法加工变现等场景）。更具体而言：

1、企业相关业务“违反国家有关规定”的识别。《刑法修正案（九）》将侵犯公民个人信息罪的前提要件由“违反国家规定”修改为“违反国家有关规定”。根据修法精神，“两高”2017年司法解释第二条规定“违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的‘违反国家有关规定’”，从而把作为刑事违法性判定依据的“国家有关规定”明确扩大到法律、行政法规、部门规章等国家层面的规定。由此推动实务中刑事司法机关倾向于在行为性质判定层面更广泛地综合运用刑法以外的非刑事法律法规和部门规章，这也在实质上扩充了企业刑事风控合规的义务来源。

2、企业为合法经营活动购买、收受公民个人信息的判定。从司法实践来看，购买、收受公民个人信息从事广告推销等活动的情形较为普遍，刑事司法机关在办案中重点关注查证的事项：一是是否为了合法经营活动，对此可以综合全案证据认定，但主要应当由被告方提供相关证据；二是是否限于普通公民个人信息，即不包括可能影响人身、财产安全的敏感信息；三是是否信息没有再流出扩散，即行为方式限于购买、收受。

3、企业非法“提供公民个人信息”的认定。刑事司法机关重点专注企业“合法收集公民个人信息后非法提供”的认定，基于大数据发展的现实需要，在法律适用层面为个人信息交易和流动留有一定空间，目前司法实务中不认定犯罪的处理机制主要是查证是否“经得被收集者同意”或者是否“已做匿名化处理（剔除个人关联）”。

4、企业触犯其他关联犯罪情况的处理。两种关联场景特别受刑事司法机关关注：一是现实中一些数字平台、网站存储、流转公民个人信息量巨大，数字平台、网站建立者、运营者和管理者等虽未直接接触公民个人信息，但牵涉到他人的公民个人信息非法交换、买卖等活动，司法机关重在查证研判侵犯公民个人信息罪和非法利用信息网络罪的选择适用问题。二是一些单位因为履行职责或者提供服务的需要，掌握着海量公民个人信息，侵犯公民个人信息违法犯罪的猖獗，与有关单位保护公民个人信息工作存在疏漏有一定关联，司法机关重在查证判断由侵犯公民个人信息罪转化为拒不履行信息网络安全管理义务罪的适用条件问题。

三、企业涉侵犯公民个人信息罪的司法走向

结合司法实践现状，以下事项是后续需要关注的企业涉侵犯公民个人信息罪的司法走向：

1、伴随《数据安全法》《个人信息保护法》的出台以及正在加速推进中的国家反电信网络诈骗新立法的进程，刑事司法机关针对基础性平台型企业的个人信息保护注意义务和刑事合规要求将持续增强，在办案中将更聚焦数字企业的单位犯罪问题，更倾向于穿透式查证判断企业的业务决策机制及其国内外实质利益结构，同时注重在个人信息相关的代表人诉讼（集团诉讼）、公益诉讼和监管行动中发现和获取刑事犯罪线索。

2、着眼数字企业的单位犯罪问题，各级刑事司法机关在依法做出不批准逮捕、不起诉决定或者根据认罪认罚从宽制度提出轻缓量刑建议等的同时，针对企业涉嫌具体犯罪，结合办案实际，督促涉案企业作出合规承诺并积极整改落实，促进企业合规守法经营，减少和预防企业犯罪，实现司法办案政治效果、法律效果、社会效果的有机统一。

3、不同司法机关在办案思维、办案手段和办案方式上的若干差异将长期存在，例如南北方司法机关针对侵犯公民个人信息犯罪呈现不同的打击力度，其中南方司法机关相对持更为严厉的从重打击立场。对此，一方面需要注意刑事司法机关可能的选择性指定管辖，另一方面需要注意相关方可能的选择性制造管辖，特别是在商业环境中“以刑事手段追求商业目的”的特殊情形。

第二章

企业涉个人信息刑事风险的特征分析

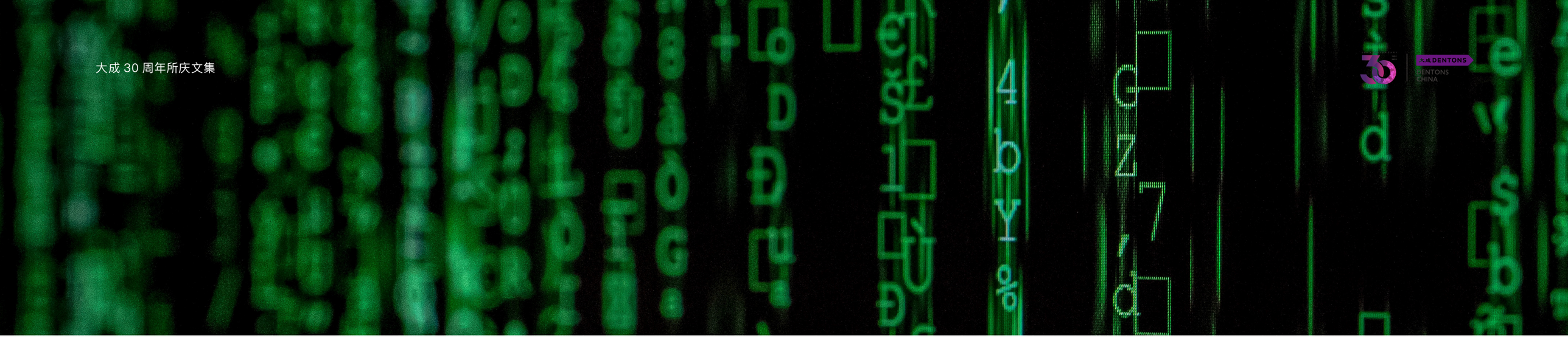
刑法第 253 条之一，由《刑法修正案（七）》引入、经《刑法修正案（九）》修改后，明文规定：

“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。”



一、企业涉侵犯公民个人信息罪的行为特征

由此决定了企业涉个人信息刑事责任的四种典型行为模式：

文件名称	发布时间	发文机关
1、（违反国家有关规定）出售	利用职务业务便利出售 从重处罚	单位犯罪
2、（违反国家有关规定）提供	利用职务业务便利提供 从重处罚	单位犯罪
3、窃取	/	单位犯罪
4、非法获取	/	单位犯罪

有关侵犯公民个人信息单位犯罪的刑事司法裁判大数据显示，单位犯罪中受到刑事处罚的典型行为方式主要包括以下几种：

行为方式
1、非法出售或者提供公民个人信息
2、将职务业务活动中获得的公民信息非法出售或提供给他人
3、通过交换方式非法获取公民个人信息
4、为合法经营活动而非法购买公民个人信息
5、窃取公民个人信息
6、以其他方法非法获取公民个人信息

需要注意的是，《个人信息保护法》全面施行之后，在与《刑法》的结合适用中，企业涉侵犯公民个人信息单位犯罪的典型行为呈现进一步细化和扩充的态势，有必要结合自身业务场景展开深度研判：

《刑法》处罚的行为	单位犯罪	违反《个人信息保护法》的规定
1、（违反国家有关规定）出售	可以构成	第10、13、14、15、17、20–23、25、27、28–32、38–41、44条
2、（违反国家有关规定）提供	可以构成	第10、13、14、15、17、20–23、25、27、28–32、38–41、44条
3、窃取	可以构成	第10条
4、非法获取	可以构成	第10、13、14、15、17、19、20–23、27、28–32、38–41、44、47、49条

此外，《个人信息保护法》第 5–10 条规定的六项基本原则，在刑事司法实务中亦可作为判定单位行为具备“一般刑事违法性”的法律依据，进而在疑难、复杂和新型案件的办理中产生重大刑事意义。

二、企业涉侵犯公民个人信息罪的人员特征

根据刑法第 253 条之一的规定，单位犯侵犯公民个人信息罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员追究刑事责任。2017 年“两高”《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》对此进一步明确，单位犯刑法第 253 条之一规定之罪的，依照该解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。也即典型的刑事“双罚制”：单位领受刑事罚金，同时直接负责的主管人员和其他直接责任人员按照自然人犯罪判处同等刑罚。

有关侵犯公民个人信息单位犯罪的刑事司法裁判大数据显示，单位犯罪中受到刑事处罚的“直接负责的主管人员和其他直接责任人员”，在实务案件中可以具体表现为以下各种身份：

1、高层人员	董事长、董事长助理、法定代表人、总经理（经理）、总裁、副总裁、集团总监、股东等
2、中层人员	总经理助理、商务经理、部门总监（技术部、资源平台部等）、部门经理（运营部、市场部、销售部、产品经理等）、部门主管（运营部、销售主管、客服部主管、业务主管、主管人员等）等
3、基层人员	技术部组长、营销产品部技术组负责人、公司员工（职员、销售员、业务员、电商运营人员、培训人员、业务客服、保安、学习顾问等）、务工人员、建筑工程师等

此外，关于人员主体问题，在目前刑事司法实务中常见存在的单位犯罪直接负责的主管人员和其他直接责任人员的认定方法是：

（1）直接负责的主管人员，是在单位实施的犯罪中起决定、批准、授意、纵容、指挥等作用的人员，一般是单位的主管负责人，包括法定代表人。

（2）其他直接责任人员，是在单位犯罪中具体实施犯罪并起较大作用的人员，既可以是单位的经营管理人员，也可以是单位的职工，包括聘任、雇佣的人员。

（3）对于受单位领导指派或奉命而参与实施了一定犯罪行为的人员，一般不宜作为直接责任人员追究刑事责任。

（4）对单位犯罪中的直接负责的主管人员和其他直接责任人员，应根据其在单位犯罪中的地位、作用和犯罪情节，分别处以相应的刑罚。

（5）主管人员与直接责任人员，在个案中，不是当然的主、从犯关系，有的案件，主管人员与直接责任人员在实施犯罪行为的主从关系不明显的，可不分主、从犯。但具体案件可以分清主、从犯，且不分清主、从犯，在同一法定刑档次、幅度内量刑无法做到罪刑相适应的，应当分清主、从犯，依法处罚。

三、企业涉侵犯公民个人信息罪的责任特征

就刑事处罚的具体适用而言，在 2017 年“两高”《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》的框架下，需要注意的问题是——

一方面，针对单位所受罚金额度的判定，司法解释明确规定，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金，罚金数额一般在违法所得的一倍以上五倍以下。

另一方面，对于单位以及“直接负责的主管人员和其他直接责任人员”而言，

（1）个人存在特定从业禁止的后果，具体实现机制有两种：

A.《刑法》第 37 条之一，即“因利用职业便利实施犯罪，或者实施违背职业要求的特定义务的犯罪被判处刑罚的，人民法院可以根据犯罪情况和预防再犯罪的需要，禁止其自刑罚执行完毕之日或者假释之日起从事相关职业，期限为 3 年至 5 年。”

B.《网络安全法》第 63 条，即“违反本法第二十七条规定，..... 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。”

（2）单位和个人都有获得从宽处罚的可能，其具体规则是：不属于“情节特别严重”，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免予刑事处罚；确有必要判处刑罚的，应当从宽处罚。由此意味着作为单位主体的企业的事后作为能够有效缩小刑事处罚的范围、降低刑事处罚的实际强度，也意味着企业的合规风控工作有必要延伸到“案后”环节。

同时，在单位犯罪案件中，下列常见情形可以成为刑事司法机关认定“不构成单位犯罪”的事由：

1、个人为进行违法犯罪活动而设立的公司、企业、事业单位实施犯罪的，不以单位犯罪论处。

2、多人私下实施并从中获利，违法所得由实施犯罪的个人私分的。

3、实施系个人行为、假借单位名义的。

4、控方证据不足以证明涉案行为系经公司决策机构批准、同意或认可而实施的。

此外，在 2017 年“两高”《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》的框架下，值得注意的、影响刑事责任承担的重要问题还包括：

(1)刑法重点保护的个人信息的分类分级

1、高度敏感个人信息	行踪轨迹信息、通信内容、征信信息、财产信息	50条入罪基准
2、敏感个人信息	住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的个人信息	500条入罪基准
3、普通个人信息	其他个人信息	5000条入罪基准

(2)刑事案件中个人信息的计算规则

1、非法获取公民个人信息后又出售或者提供的	条数不重复计算
2、向不同单位或者个人分别出售、提供同一公民个人信息的	条数累计计算
3、批量公民个人信息的条数	根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外

四、企业涉侵犯公民个人信息罪的信息特征

有关侵犯公民个人信息单位犯罪的刑事司法裁判大数据显示，对照刑事司法解释的分级标准，单位犯罪相关典型案件中所涉及的个人信息类型主要表现为如下三个等级：

1、高度敏感个人信息	个人总资产、现金余额、股票市值、银行卡、业主财产信息、征信信息、车牌号、车辆型号
2、敏感个人信息	房产地址、公民个人房屋权籍调查信息、LAC（位置区代码）、楼盘名称及楼号梯号房号、所在地区
3、普通个人信息	姓名、身份证号、手机号、IP地址、搜索关键词、CELL（基站号）、IMEI（手机串号）、网站访问时间（精确至秒）、URL（上网地址）、学生学号、学生专业名称、企业管理人员单位、企业管理人员职务、公司名称、法人姓名

结合上述案件事实以及司法裁判实践，可以认为：

一方面，涉罪个人信息的具体类型与涉案单位的业务模式呈现正向逻辑关联，特别是涉案互联网企业非法收集的个人信息主要包括姓名、电话、网络浏览轨迹以及 IP 地址等，并且其中大部分涉案企业非法获取个人信息主要是为了用于精准营销的目的。

另一方面，涉案个人的信息类型多元，且呈现范围日益扩大的趋势。司法案例涉案个人信息类型从姓名、手机号、住址等基本信息逐年扩大到个人总资产、现金余额、股票市值、车辆信息等财产信息；企业管理人员单位名称、职务、学生学号专业学历等职业信息；征信信息；企业名称、法人姓名等企业信息以及公民在互联网上的浏览痕迹、IP 地址等其他信息。这在一定程度上与目前“数据经济”持续发展、不断拓展的产业态势呈现正向逻辑关联。

第三章

企业涉个人信息刑事风险的合规风控

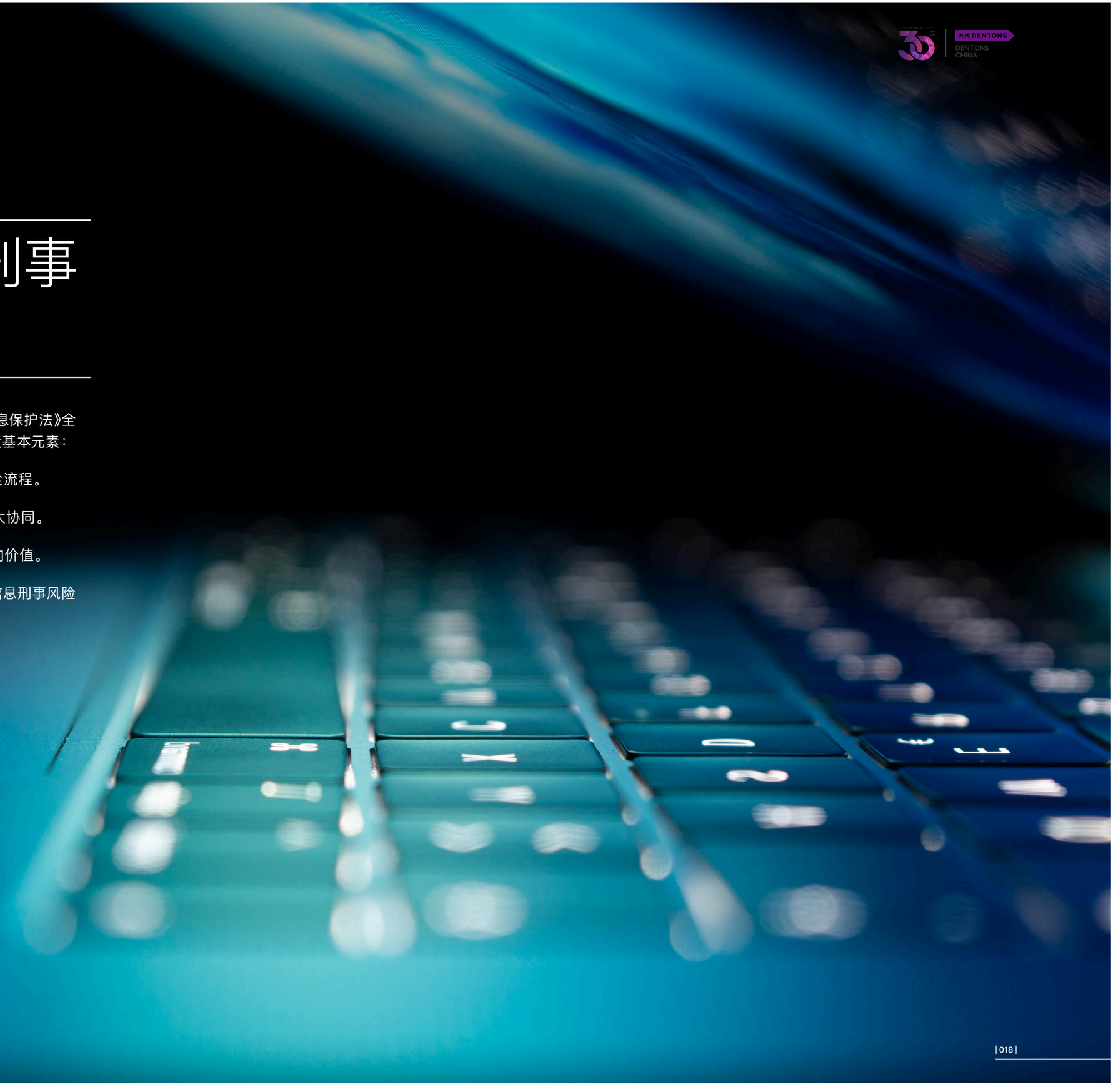
结合法律法规梳理、文献著述洞察和司法案例分析，在《个人信息保护法》全面施行阶段，针对单位犯罪刑事责任的企业合规风控要求有三大基本元素：

1、由法律制度下沉到流程实现，强调法规要求内嵌到企业业务全流程。

2、由业务责任上升到组织责任，强调企业各部门各条线的合规大协同。

3、由法律遵从进阶到战略风控，强调企业的运营活动目标的正向价值。

相应地，根据各地刑事司法机关的实务关切要点，企业涉个人信息刑事风险的合规风控工作需要注意以下三方面的系统性融合——



一、企业涉侵犯公民个人信息罪的技术风控

在刑事风险语境下、数字企业做好技术风控，能使单位本身被认定涉嫌构成犯罪时，作为单位不具备犯罪故意或过失、已尽注意义务等的重要证明，以达到使单位出罪的目的。

1、重点审查企业个人信息保护措施是否满足相关规定

针对企业内已经确定属于个人信息的数据，应全面梳理企业在个人信息的获取、使用、共享、披露、提供等处理方面所采取的技术措施，是否符合我国法律对个人信息的保护规则，尤其是在个人信息的收集方面，能够记录和证明是否得到了个人信息主体的充分授权同意或者具备其他合法性基础。

（2）做好与个人信息流转具体场景匹配的全面风险评估

在个人信息流转使用的过程中，委托、共享及转让应当注重获得信息主体的授权与允许，在相应的用户协议中亦应当标明共享目的、方式以及范围等事项，以避免因共享不当而衍生合规问题。在委托第三方处理个人信息时，除了对受托人应当具有数据信息安全保护能力需要进行全面评估之外，也应当注意委托处理的范围限于与用户主体约定的范围。充分严格地配备信息流转的相关技术措施，实现上述元素必要的留痕溯源以确保在流转的过程杜绝被内部人员不法利用的可能。

（3）构建兼具技术可行性以及成本合理的应急处置机制

企业内部的个人信息安全应急处置机制是不可或缺的技术性配置，如发生任何个人信息泄露的情形，企业在第一时间启动安全应急预案，联合多部门、多人员共同处理，包括借助技术措施展开内部调查、完整记录应对处置流程、评估法律风险、向涉及的个人信息主体发送通知，并向相关监管部门报告，以防个人信息安全后果的传导和扩散。

二、企业涉侵犯公民个人信息罪的组织风控

企业内部个人信息保护的组织管理设计以及实务运行情况，如企业的组织架构、监督机制、风险管理、内部控制等事项安排以及企业对于相关法律法规和执法司法走向的理解落实程度等，是刑事司法机关查证判断涉案单位不具备犯罪故意或过失、已尽注意义务等犯罪构成要件的重要方面，在中国结果导向的刑事司法环境中，对于企业的有效出罪具有关键意义。

（1）建立高位阶、跨部门、跨条线的个人信息保护机构

该机构应当由企业领导层高级成员担任领导，统筹建构企业个人信息保护工作体系，负责安全应急响应并组织落实个人信息安全和保护各项事项。该机构的主要工作涵盖评估企业内个人信息保护与相应法律法规在合规要求上存在的差距，明确和作为数据来源的用户所约定的数据使用许可范围以及是否存在过度收集和滥用等情况，监测、审计数据在获取、保存、备份、销毁等全部环节的安全及保护措施。此外，该机构应当承担的职能还包括一旦发生个人信息相关安全事件，及时向数据提供方及监管部门报告，报告内容包含该事件的基本情况和可能的影响、已采取或将要采取的处置措施、降低风险的建议以及补救措施等。

（2）做好企业内外数据资产管理、严防个人信息泄露

企业需要制定详尽的个人信息数据目录和技术性流程，重点审查本企业经营活动、商业模式、业务条线、产品服务、人员管理中所涉及的信息是否属于个人信息或敏感个人信息及其种类和级别。同时严格界定信息收集主体的权限管理和身份认证，对所获取的个人信息实时落实分类分级归属，包括对敏感个人信息进行专门备份以及加密处理等，减少、杜绝个人信息等因保管或处理不当所产生的数据泄露被内部人员或外部人员不法利用的问题。特别地，针对企业内部人员利用职务之便侵犯公民个人信息、进而引发单位刑事责任的多发情形，应当依照最小必要原则，通过控制数据访问的权限和设定多重身份认证技术保护个人信息，并对各级企业人员处理数据的行为进行全流程管控，包括采用专门的数据和技术安全审计，设立日志审计和行为审计多项措施等。

（3）围绕第三方数据合作建构并完善协议管理监督体系

企业与第三方进行数据合作的合规管控，涉及与母公司、合作伙伴之间等多种场景。企业在和第三方合作时，特别是在第三方也能够获得数据的情况下，企业应严格审查第三方的资质，并与之约定对于数据相关法律法规的遵从和对于数据存储安全、防护、应急措施、销毁等措施的承诺，并将相应内容作为合规条款融入主合同，同时通过专岗专人强化合同和协议等的流程管理与执行监督，及时识别和处置异常业务风险。

三、企业涉侵犯公民个人信息罪的人员风控

企业人员，特别是管理层，在企业涉侵犯公民个人信息罪案件中属于法定责任主体，并且其行为容易引发全局性单位刑事责任。因此，做好相关的宣传培训工作，建立全面有效的人员监督、业务操作的权限约束等机制，有助于最大限度地减少个人犯罪引发单位犯罪的可能性。特别要抓好管理层这个关键群体，因为其个人信息保护意识以及工作方式，一则是刑事司法机关判定单位和企业人员整体合规水平的重要指针，二则有利于建构“刑事风险阻隔机制”，避免刑事司法机关将管理层个人意志判定为单位集体决策、将个人行为判定为单位行为。

(1)持续改进企业个人信息风险管理和内部控制的有效性

企业应当持续监测和保障个人信息风险识别与评估、风险管理的组织架构、风险处置与防控机制、应急预案、个人信息保护工作的考核与奖惩机制、举报与投诉处理等各项措施和机制的有效性，使之能够覆盖企业的各级分支机构、附属机构以及各级业务部门、岗位和人员。特别是坚持抓住企业管理层这个“关键少数”，通过有效的“定岗定人”和“定岗定责”确保各项风险管理和内部控制措施的持续性效力。

(2)普及企业个人信息保护事务的全员法治素养培训

通过开展组织对个人信息保护法治等合规事项的持续宣传和培训，提升和拉齐包括企业各级员工(含外包人员等)、各类合作伙伴等在内的全体人员的守法意识和操作技能，避免因为个别员工、商业伙伴刑事法律责任和风险的上下传导而导致社会舆论、监管司法机关做出对企业个人信息保护执行实施缺位的认识和判断，这一点同时也是刑事司法机关查证判断涉案单位本身不具备犯罪故意或过失、已尽合规注意义务等犯罪构成要件的重要方面。

(3)落实个人信息相关关键岗位和人员的高水平管理

企业在对和个人信息保护相关的关键岗位和关键人员进行充分背景调查的基础上，签署相应的保密协议和业务守则，定期对该类人员进行专门的合规培训、安全教育以及设定技能考核等人员管理项目，同时就其业务操作情况和重要外部关系变动形成及时、完整的档案记录，并主要通过该类人员强化落实对外部数据合作方的全流程合规监督与风险处置。

附录：侵犯公民个人信息罪相关法律法规和司法文件

一、《中华人民共和国个人信息保护法》

2021 年 8 月 20 日，第十三届全国人民代表大会常务委员会第三十次会议通过，自 2021 年 11 月 1 日起施行。

第一章　总　　则

第一条　为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条　自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条　在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

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。

第五条　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。

第六条　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。

第七条　处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条　处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条　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。

第十条　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；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条　国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条　国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章　个人信息处理规则

第一节　一般规定

第十三条　符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

（二）为订立、履行个人作为一方当事人的合同所必需，或者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；

（三）为履行法定职责或者法定义务所必需；

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条　基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条　基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条　个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第十七条　个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条　个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

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向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条　除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条　两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条　个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条　个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。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。

第二十三条　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。

第二十四条　个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，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。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条　个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条　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，不得用于其他目的；取得个人单独同意的除外。

第二十七条　个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节　敏感个人信息的处理规则

第二十八条　敏感个人信息是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。

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。

第二十九条　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。

第三十条　个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

第三十一条　个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

第三十二条　法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节　国家机关处理个人信息的特别规定

第三十三条　国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条　国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条　国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条　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。安全评估可以要求有关部门提供支持与协助。

第三十七条　法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章　个人信息跨境提供的规则

第三十八条　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，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）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；

（三）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；

（四）法律、行政法规或者国家网信部门规定的其他条件。

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。

第三十九条　个人信息处理者向中华人民共和国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。

第四十条　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。

第四十一条　中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者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个人信息。

第四十二条　境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条　任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章　个人在个人信息处理活动中的权利

第四十四条　个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条　个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条　个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条　有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（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。

第四十八条　个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条　自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条　个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章　个人信息处理者的义务

第五十一条　个人信息处理者应当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，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第五十二条　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。

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。

第五十三条　本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条　个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条　有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条　个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条　发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

第五十八条　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，应当履行下列义务：

（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；

（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；

（三）对严重违反法律、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；

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条　接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

第六章　履行个人信息保护职责的部门

第六十条　国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条　履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第六十二条　国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

（一）制定个人信息保护具体规则、标准；

（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；

（三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；

（五）完善个人信息保护投诉、举报工作机制。

第六十三条　履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

（一）询问有关当事人，调查与个人信息处理活动有关的情况；

（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查；

（四）检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条　履行个人信息保护职责的部门在履行职责中，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，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条　任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章　法律责任

第六十六条　违反本法规定处理个人信息，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，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；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。

有前款规定的违法行为，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；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。

第六十七条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条　国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条　处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

第七十条　个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条　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。

第八章　附　　则

第七十二条　自然人因个人或者家庭事务处理个人信息的，不适用本法。

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。

第七十三条　本法下列用语的含义：

（一）个人信息处理者，是指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。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）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。

第七十四条　本法自 2021 年 11 月 1 日起施行。

二、《中华人民共和国刑法》

第二百五十三条之一　侵犯公民个人信息罪

2015 年 8 月 29 日，第十二届全国人大常委会十六次会议表决通过刑法修正案（九），自 2015 年 11 月 1 日起施行。

违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

三、“两高”《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

2017 年 3 月 20 日，由最高法院审判委第 1712 次会议、2017 年 4 月 26 日由最高人民检察院第十二届检察委第 63 次会议通过并公布，自 2017 年 6 月 1 日起施行。

为依法惩治侵犯公民个人信息犯罪活动，保护公民个人信息安全和合法权益，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的有关规定，现就办理此类刑事案件适用法律的若干问题解释如下：

第一条 刑法第二百五十三条之一规定的“公民个人信息”，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

第二条 违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。

第三条 向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。

第四条 违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第五条 非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；

（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；

（三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；

（四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；

（五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；

（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；

（七）违法所得五千元以上的；

（八）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；

（九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；

（十）其他情节严重的情形。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”：

（一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；

（二）造成重大经济损失或者恶劣社会影响的；

（三）数量或者数额达到前款第三项至第八项规定标准十倍以上的；

（四）其他情节特别严重的情形。

第六条 为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

（一）利用非法购买、收受的公民个人信息获利五万元以上的；

（二）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的；

（三）其他情节严重的情形。

实施前款规定的行为，将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准适用本解释第五条的规定。

第七条 单位犯刑法第二百五十三条之一规定之罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第八条 设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。

第九条 网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

第十条 实施侵犯公民个人信息犯罪，不属于“情节特别严重”，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免予刑事处罚；确有必要判处刑罚的，应当从宽处罚。

第十一条 非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。

向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算。

对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。

第十二条 对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。罚金数额一般在违法所得的一倍以上五倍以下。

第十三条 本解释自 2017 年 6 月 1 日起施行。

四、最高人民检察院《检察机关办理侵犯公民个人信息案件指引》

2018 年 11 月 9 日，最高人民检察院第十三届检察委员会第五次会议通过。

根据《中华人民共和国刑法》第二百五十三条之一的规定，侵犯公民罪是指违反国家有关规定，向他人出售、提供公民，或者通过窃取等方法非法获取公民，情节严重的行为。结合《最高人民法院、最高人民检察院关于办理侵犯公民刑事案件适用法律若干问题的解释》（法释〔2017〕10 号）（以下简称《解释》），办理侵犯公民案件，应当特别注意以下问题：一是对“公民”的审查认定；二是对“违反国家有关规定”的审查认定；三是对“非法获取”的审查认定；四是对“情节严重”和“情节特别严重”的审查认定；五是对关联犯罪的审查认定。

（一）审查证据的基本要求

1、审查逮捕

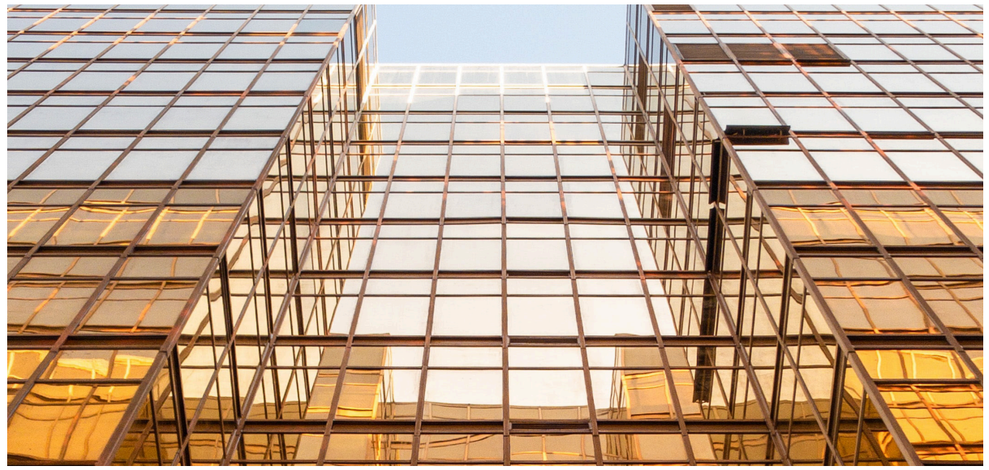
1）有证据证明发生了侵犯公民个人信息犯罪事实

（1）证明侵犯公民个人信息案件发生

主要证据包括：报案登记、受案登记、立案决定书、破案经过、证人证言、被害人陈述、犯罪嫌疑人供述和辩解以及证人、被害人提供的短信、微信或 QQ 截图等电子数据。

（2）证明被侵犯对象系公民个人信息

主要证据包括：扣押物品清单、勘验检查笔录、电子数据、司法鉴定意见及公民信息查询结果说明、被害人陈述、被害人提供的原始信息资料和对比资料等。



2）有证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的

（1）证明违反国家有关规定的证据：犯罪嫌疑人关于所从事的职业的供述、其所在公司的工商注册资料、公司出具的犯罪嫌疑人职责范围说明、劳动合同、保密协议及公司领导、同事关于犯罪嫌疑人职责范围的证言等。

（2）证明出售、提供行为的证据：远程勘验笔录及 QQ、微信等即时通讯工具聊天记录、论坛、贴吧、电子邮件、手机短信记录等电子数据，证明犯罪嫌疑人通过上述途径向他人出售、提供、交换公民的情况。公民贩卖者、提供者、担保交易人及购买者、收受者的证言或供述，相关银行账户明细、第三方支付平台账户明细，证明出售公民违法所得情况。此外，如果犯罪嫌疑人系通过信息网络发布方式提供公民，证明该行为的证据还包括远程勘验笔录、扣押笔录、扣押物品清单、对手机、电脑存储介质、云盘、FTP 等的司法鉴定意见等。

（3）证明犯罪嫌疑人或公民购买者、收受者控制涉案信息的证据：搜查笔录、扣押笔录、扣押物品清单，对手机、电脑存储介质等的司法鉴定意见等，证实储存有公民的电脑、手机、U 盘或者移动硬盘、云盘、FTP 等介质与犯罪嫌疑人或公民购买者、收受者的关系。犯罪嫌疑人供述、辨认笔录及证人证言等，证实犯罪嫌疑人或公民购买者、收受者所有或实际控制、使用涉案存储介质。

（4）证明涉案公民真实性的证据：被害人陈述、被害人提供的原始信息资料、公安机关或相关单位出具的涉案公民与权威数据库内信息同一性的比对说明。针对批量的涉案公民的真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

（5）证明违反国家规定，通过窃取、购买、收受、交换等方式非法获取公民的证据：主要证据与上述以出售、提供方式侵犯公民行为的证据基本相同。针对窃取的方式如通过技术手段非法获取公民的行为，需证明犯罪嫌疑人实施上述行为，除被害人陈述、犯罪嫌疑人供述和辩解外，还包括侦查机关从被害公司数据库中发现入侵电脑 IP 地址情况、从犯罪嫌疑人电脑中提取的侵入被害公司数据的痕迹等现场勘验检查笔录，以及涉案程序（木马）的司法鉴定意见等。

3）有证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

（1）证明犯罪嫌疑人明知没有获取、提供公民个人信息的法律依据或资格，主要证据包括：犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等。

（2）证明犯罪嫌疑人积极实施窃取、出售、提供、购买、交换、收受公民个人信息的行为，主要证据除了证人证言、犯罪嫌疑人供述和辩解外，还包括远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意见、银行账户明细、第三方支付平台账户明细等。

4）有证据证明“情节严重”或“情节特别严重”

（1）公民个人信息购买者或收受者的证言或供述。

（2）公民购买、收受公司工作人员利用公民进行电话或短信推销、商务调查等经营性活动后出具的证言或供述。

（3）公民个人信息购买者或者收受者利用所获信息从事违法犯罪活动后出具的证言或供述。

（4）远程勘验笔录、电子数据司法鉴定意见书、最高人民检察院或公安部指定的机构对电子数据涉及的专门性问题出具的报告、公民资料等。证明犯罪嫌疑人通过即时通讯工具、电子邮箱、论坛、贴吧、手机等向他人出售、提供、购买、交换、收受公民的情况。

（5）银行账户明细、第三方支付平台账户明细。

（6）死亡证明、伤情鉴定意见、医院诊断记录、经济损失鉴定意见、相关案件起诉书、判决书等。

2、审查起诉

除审查逮捕阶段证据审查基本要求之外，对侵犯公民个人信息案件的审查起诉工作还应坚持“犯罪事实清楚，证据确实、充分”的标准，保证定罪量刑的事实都有证据证明；据以定案的证据均经法定程序查证属实；综合全案证据，对所认定的事实已排除合理怀疑。

1）有确实充分的证据证明发生了侵犯公民个人信息犯罪事实。该证据与审查逮捕的证据类型相同。

2）有确实充分的证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的。

（1）对于证明犯罪行为是犯罪嫌疑人实施的证据审查，需要结合《解释》精神，准确把握对“违反国家有关规定”“出售、提供行为”“窃取或以其他方法”的认定。

（2）对证明违反国家有关规定的证据审查，需要明确国家有关规定的具体内容，违反法律、行政法规、部门规章有关公民个人信息保护规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。

（3）对证明出售、提供行为的证据审查，应当明确“出售、提供”包括在履职或提供服务的过程中将合法持有的公民出售或者提供给他人的行为：向特定人提供、通过信息网络或者其他途径发布公民、未经被收集者同意，将合法收集的公民（经过处理无法识别特定个人且不能复原的除外）向他人提供的，均属于刑法第二百五十三条之一规定的“提供公民”。应当全面审查犯罪嫌疑人所出售提供公民的来源、途经与去向，对相关供述、物证、书证、证人证言、被害人陈述、电子数据等证据种类进行综合审查，针对使用信息网络进行犯罪活动的，需要结合专业知识，根据证明该行为的远程勘验笔录、扣押笔录、扣押物品清单、电子存储介质、网络存储介质等的司法鉴定意见进行审查。

（4）对证明通过窃取或以其他非法方法获取公民等方式非法获取公民的证据审查，应当明确“以其他方法获取公民”包括购买、收受、交换等方式获取公民，或者在履行职责、提供服务过程中收集公民的行为。

针对窃取行为，如通过信息网络窃取公民个人信息，则应当结合犯罪嫌疑人供述、证人证言、被害人陈述，着重审查证明犯罪嫌疑人侵入信息网络、数据库时的 IP 地址、MAC 地址、侵入工具、侵入痕迹等内容的现场勘验检查笔录以及涉案程序（木马）的司法鉴定意见等。

针对购买、收受、交换行为，应当全面审查购买、收受、交换公民的来源、途经、去向，结合犯罪嫌疑人供述和辩解、辨认笔录、证人证言等证据，对搜查笔录、扣押笔录、扣押物品清单、涉案电子存储介质等司法鉴定意见进行审查，明确上述证据同犯罪嫌疑人或公民购买、收受、交换者之间的关系。

针对履行职责、提供服务过程中收集公民的行为，应当审查证明犯罪嫌疑人所从事职业及其所负职责的证据，结合法律、行政法规、部门规章等国家有关公民保护的规定，明确犯罪嫌疑人的行为属于违反国家有关规定，以其他方法非法获取公民的行为。

（5）对证明涉案公民真实性证据的审查，应当着重审查被害人陈述、被害人提供的原始信息资料、公安机关或其他相关单位出具的涉案公民与权威数据库内信息同一性的对比说明。对批量的涉案公民的真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

3）有确实充分的证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

（1）对证明犯罪嫌疑人主观故意的证据审查，应当综合审查犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等，结合国家公民个人信息保护的相关规定，夯实犯罪嫌疑人在实施犯罪时的主观明知。

（2）对证明犯罪嫌疑人积极实施窃取或者以其他方法非法获取公民个人信息行为的证据审查，应当结合犯罪嫌疑人供述、证人证言，着重审查远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意见、银行账户明细、第三方支付平台账户明细等，明确犯罪嫌疑人在实施犯罪时的积极作为。

4）有确实充分的证据证明“情节严重”或“情节特别严重”。该证据与审查逮捕的证据类型相同。

(二)需要特别注意的问题

在侵犯公民个人信息案件审查逮捕、审查起诉中,要根据相关法律、司法解释等规定,结合在案证据,重点注意以下问题:

1、对“公民个人信息”的审查认定

根据《解释》的规定,公民是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息,包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。经过处理无法识别特定自然人且不能复原的信息,虽然也可能反映自然人活动情况,但与特定自然人无直接关联,不属于公民的范畴。

对于企业工商登记等信息中所包含的手机、电话号码等信息,应当明确该号码的用途。对由公司购买、使用的手机、电话号码等信息,不属于个人信息的范畴,从而严格区分“手机、电话号码等由公司购买,归公司使用”与“公司经办人在工商登记等活动中登记个人电话、手机号码”两种不同情形。

2、对“违反国家有关规定”的审查认定

《中华人民共和国刑法修正案(九)》将原第二百五十三条之一的“违反国家规定”修改为“违反国家有关规定”,后者的范围明显更广。根据刑法第九十六条的规定,“国家规定”仅限于全国人大及其常委会制定的法律和决定,国务院制定的行政法规、规定的行政措施、发布的决定和命令。而“国家有关规定”还包括部门规章,这些规定散见于金融、电信、交通、教育、医疗、统计、邮政等领域的法律、行政法规或部门规章中。

3、对“非法获取”的审查认定

在窃取或者以其他方法非法获取公民的行为中,需要着重把握“其他方法”的范围问题。“其他方法”,是指“窃取”以外,与窃取行为具有同等危害性的方法,其中,购买是最常见的非法获取手段。侵犯公民犯罪作为电信网络诈骗的上游犯罪,诈骗分子往往先通过网络向他人购买公民,然后自己直接用于诈骗或转发给其他同伙用于诈骗,诈骗分子购买公民的行为属于非法获取行为,其同伙接收公民的行为明显也属于非法获取行为。同时,一些房产中介、物业管理公司、保险公司、担保公司的业务员往往与同行通过 QQ、微信群互相交换各自掌握的客户信息,这种交换行为也属于非法获取行为。此外,行为人在履行职责、提供服务过程中,违反国家有关规定,未经他人同意收集公民,或者收集与提供的服务无关的公民的,也属于非法获取公民的行为。

4、对“情节严重”和“情节特别严重”的审查认定

在窃取或者以其他方法非法获取公民的行为中,需要着重把握“其他方法”的范围问题。“其他方法”,是指“窃取”以外,与窃取行为具有同等危害性的方法,其中,购买是最常见的非法获取手段。侵犯公民犯罪作为电信网络诈骗的上游犯罪,诈骗分子往往先通过网络向他人购买公民,然后自己直接用于诈骗或转发给其他同伙用于诈骗,诈骗分子购买公民的行为属于非法获取行为,其同伙接收公民的行为明显也属于非法获取行为。同时,一些房产中介、物业管理公司、保险公司、担保公司的业务员往往与同行通过 QQ、微信群互相交换各自掌握的客户信息,这种交换行为也属于非法获取行为。此外,行为人在履行职责、提供服务过程中,违反国家有关规定,未经他人同意收集公民,或者收集与提供的服务无关的公民的,也属于非法获取公民的行为。

1)关于“情节严重”的具体认定标准,根据《解释》第五条第一款的规定,主要涉及五个方面:

(1)信息类型和数量。①行踪轨迹信息、通信内容、征信信息、财产信息,此类信息与公民人身、财产安全直接相关,数量标准为五十条以上,且仅限于上述四类信息,不允许扩大范围。对于财产信息,既包括银行、第三方支付平台、证券期货等金融服务账户的身份认证信息(一组确认用户操作权限的数据,包括账号、口令、密码、数字证书等),也包括存款、房产、车辆等财产状况信息。②住宿信息、通信记录、健康生理信息、交易信息等可能影响公民人身、财产安全的信息,数量标准为五百条以上,此类信息也与人身、财产安全直接相关,但重要程度要弱于行踪轨迹信息、通信内容、征信信息、财产信息。对“其他可能影响人身、财产安全的公民”的把握,应当确保所适用的公民涉及人身、财产安全,且与“住宿信息、通信记录、健康生理信息、交易信息”在重要程度上具有相当性。③除上述两类信息以外的其他公民,数量标准为五千条以上。

(2)违法所得数额。对于违法所得,可直接以犯罪嫌疑人出售公民个人信息的收入予以认定,不必扣减其购买信息的犯罪成本。同时,在审查认定违法所得数额过程中,应当以查获的银行交易记录、第三方支付平台交易记录、聊天记录、犯罪嫌疑人供述、证人证言综合予以认定,对于犯罪嫌疑人无法说明合法来源的用于专门实施侵犯公民个人信息犯罪的银行账户或第三方支付平台账户内资金收入,可综合全案证据认定为违法所得。

(3)信息用途。公民被他人用于违法犯罪活动的,不要求他人的行为必须构成犯罪,只要行为人明知他人非法获取公民用于违法犯罪活动即可。

(4)主体身份。如果行为人系将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人的,涉案信息数量、违法所得数额只要达到一般主体的一半,即可认为“情节严重”。

(5)主观恶性。曾因侵犯公民受过刑事处罚或者二年内受过行政处罚,又非法获取、出售或者提供公民的,即可认为“情节严重”。

2）关于“情节特别严重”的认定标准，根据《解释》，主要分为两类：

一是信息数量、违法所得数额标准。二是信息用途引发的严重后果，其中造成人身伤亡、经济损失、恶劣社会影响等后果，需要审查认定侵犯公民个人信息的行为与严重后果间存在因果关系。

对于涉案公民数量的认定，根据《解释》第十一条，非法获取公民后又出售或者提供的，公民的条数不重复计算；向不同单位或者个人分别出售、提供同一公民的，公民的条数累计计算；对批量出售、提供公民的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。在实践中，如犯罪嫌疑人多次获取同一条公民，一般认定为一条，不重复累计；但获取的该公民内容发生了变化的除外。

对于涉案公民的数量、社会危害性等因素的审查，应当结合刑法第二百五十三条和《解释》的规定进行综合审查。涉案公民数量极少，但造成被害人死亡等严重后果的，应审查犯罪嫌疑人行为与该后果之间的因果关系，符合条件的，可以认定为实施《解释》第五条第一款第十项“其他情节严重的情形”的行为，造成被害人死亡等严重后果，从而认定为“情节特别严重”。如涉案公民数量较多，但犯罪嫌疑人仅仅获取而未向他人出售或提供，则可以在认定相关犯罪事实的基础上，审查该行为是否符合《解释》第五条第一款第三、四、五、六、九项及第二款第三项的情形，符合条件的，可以分别认定为“情节严重”“情节特别严重”。

此外，针对为合法经营活动而购买、收受公民的行为，在适用《解释》第六条的定罪量刑标准时须满足三个条件：一是为了合法经营活动，对此可以综合全案证据认定，但主要应当由犯罪嫌疑人一方提供相关证据；二是限于普通公民，即不包括可能影响人身、财产安全的敏感信息；三是信息没有再流出扩散，即行为方式限于购买、收受。如果将购买、收受的公民非法出售或者提供的，定罪量刑标准应当适用《解释》第五条的规定。

5、对关联犯罪的审查认定

对于侵犯公民犯罪与电信网络诈骗犯罪相交织的案件，应严格按照《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（法发〔2016〕32 号）的规定进行审查认定，即通过认真审查非法获取、出售、提供公民的犯罪嫌疑人对电信网络诈骗犯罪的参与程度，结合能够证实其认知能力的学历文化、聊天记录、通话频率、获取固定报酬还是参与电信网络诈骗犯罪分成等证据，分析判断其是否属于诈骗共同犯罪、是否应该数罪并罚。

根据《解释》第八条的规定，设立用于实施出售、提供或者非法获取公民违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪；同时构成侵犯公民罪的，应当认定为侵犯公民罪。

对于违反国家有关规定，采用技术手段非法侵入合法存储公民的单位数据库窃取公民的行为，也符合刑法第二百八十五条第二款非法获取计算机信息系统数据罪的客观特征，同时触犯侵犯公民罪和非法获取计算机信息系统数据罪的，应择一重罪论处。

此外，针对公安民警在履行职责过程中，违反国家有关规定，查询、提供公民的情形，应当认定为“违反国家有关规定，将在履行职责或者提供服务过程中以其他方法非法获取或提供公民”。但同时，应当审查犯罪嫌疑人除该行为之外有无其他行为侵害其他法益，从而对可能存在的其他犯罪予以准确认定。

（三）社会危险性及羁押必要性审查

1、审查逮捕

1. 犯罪动机：一是出售牟利；二是用于经营活动；三是用于违法犯罪活动。犯罪动机表明犯罪嫌疑人主观恶性，也能证明犯罪嫌疑人是否可能实施新的犯罪。

2. 犯罪情节。犯罪嫌疑人的行为直接反映其人身危险性。具有下列情节的侵犯公民犯罪，能够证实犯罪嫌疑人主观恶性和人身危险性较大，实施新的犯罪的可能性也较大，可以认为具有较大的社会危险性：一是犯罪持续时间较长、多次实施侵犯公民犯罪的；二是被侵犯的公民数量或违法所得巨大的；三是利用公民进行违法犯罪活动的；四是犯罪手段行为本身具有违法性或者破坏性，即犯罪手段恶劣的，如骗取、窃取公民，采取胁迫、植入木马程序侵入他人计算机系统等方式非法获取信息。

犯罪嫌疑人实施侵犯公民个人信息犯罪，不属于“情节特别严重”，系初犯，全部退赃，并确有悔罪表现的，可以认定社会危险性较小，没有逮捕必要。

2、审查起诉

在审查起诉阶段，要结合侦查阶段取得的事实证据，进一步引导侦查机关加大捕后侦查力度，及时审查新证据。在羁押期限届满前对全案进行综合审查，对于未达到逮捕证明标准的，撤销原逮捕决定。

经羁押必要性审查，发现犯罪嫌疑人具有下列情形之一的，应当向办案机关提出释放或者变更强制措施的建议：

1. 案件证据发生重大变化，没有证据证明有犯罪事实或者犯罪行为系犯罪嫌疑人、被告人所为的。

2. 案件事实或者情节发生变化，犯罪嫌疑人、被告人可能被判处拘役、管制、独立适用附加刑、免予刑事处罚或者判决无罪的。

3. 继续羁押犯罪嫌疑人、被告人，羁押期限将超过依法可能判处的刑期的。

4. 案件事实基本查清，证据已经收集固定，符合取保候审或者监视居住条件的。

经羁押必要性审查，发现犯罪嫌疑人、被告人具有下列情形之一，且具有悔罪表现，不予羁押不致发生社会危险性的，可以向办案机关提出释放或者变更强制措施的建议：

1. 预备犯或者中止犯；共同犯罪中的从犯或者胁从犯。

2. 主观恶性较小的初犯。

3. 系未成年人或者年满七十五周岁的人。

4. 与被害方依法自愿达成和解协议，且已经履行或者提供担保的。

5. 患有严重疾病、生活不能自理的。

6. 系怀孕或者正在哺乳自己婴儿的妇女。

7. 系生活不能自理的人的唯一扶养人。

8. 可能被判处一年以下有期徒刑或者宣告缓刑的。

9. 其他不需要继续羁押犯罪嫌疑人、被告人的情形。

30th ANNIVERSARY 1992 2022

大成 DENTONS

DENTONS CHINA

大成律师事务所

微信扫描二维码
关注公众号

地址: 北京市朝阳区朝阳门南大街10号
兆泰国际中心B座 16–21 层
邮编: 100020
总机: +86 10 5813 7799
传真: +86 10 5813 7788
网站: www.dentons.com
邮箱: beijing@dentons.cn