V&T LAW FIRM
万商天勤律师事务所

www.vtlaw.cn

法律护航数据安全 数字经济行稳致远

——数据合规与个人信息保护

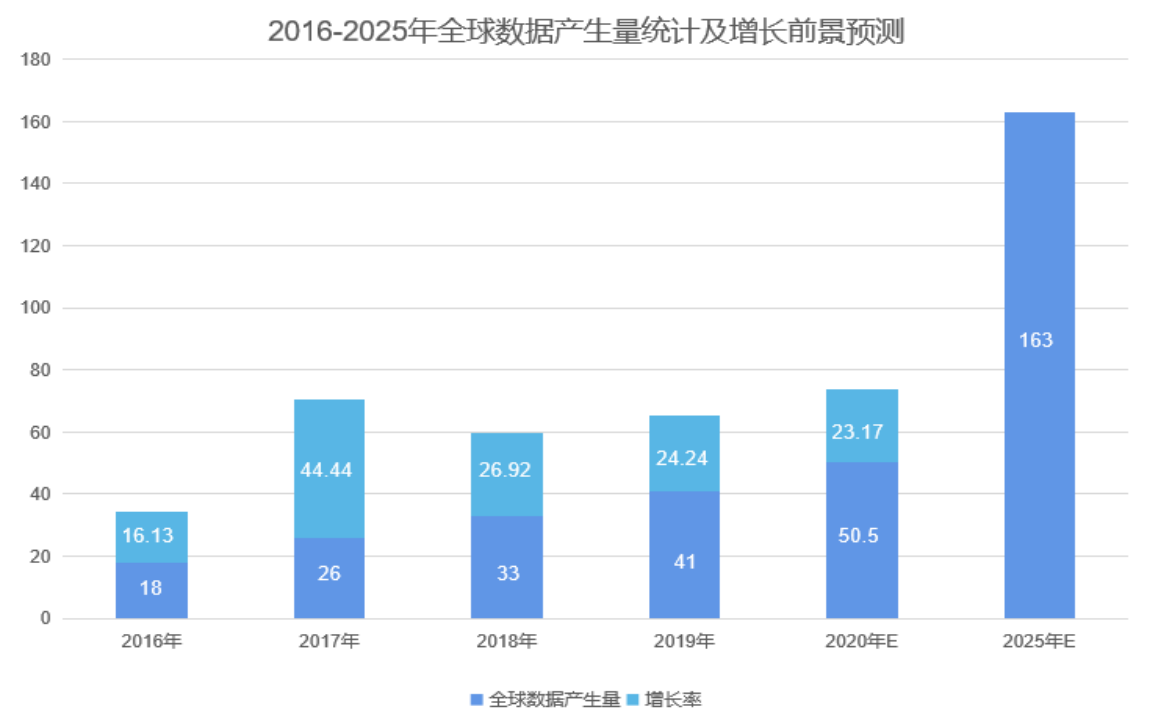
2021 CN

CONTENTS

01

数字经济时代的安全威胁

数字经济发展迅猛

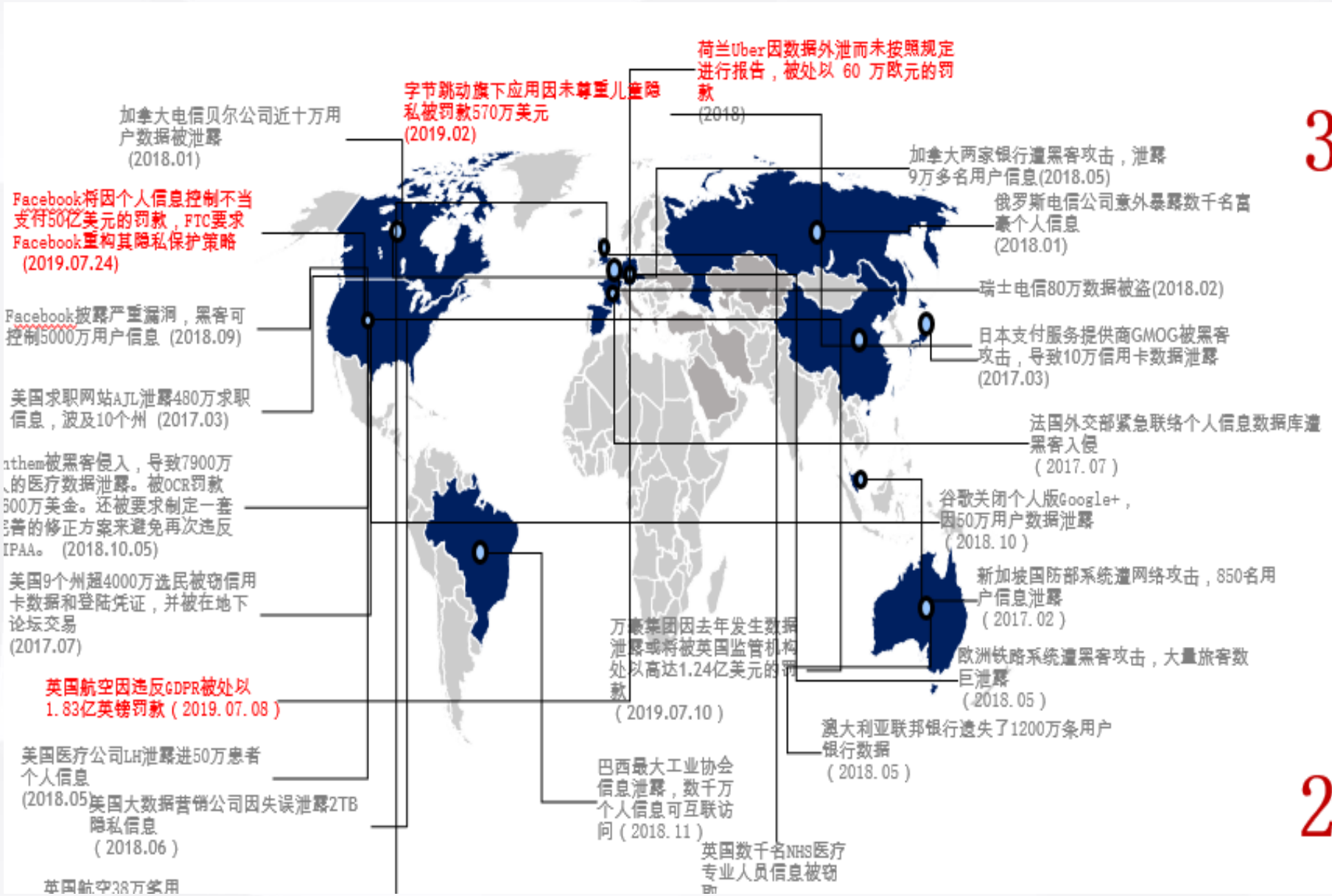


- 国际数据公司IDC预计2025年全球数据量将是2016年的九倍，达到163ZB。
- 全球数据规模呈现爆发增长。

根据中国信息通信研究院发布的《中国数字经济发展白皮书（2021）》显示，2020年我国数字经济规模达到39.2万亿元，占GDP的比重为38.6%，实现9.7%的高速增长，与“十二五”末期相比，数字经济规模翻了一番，总量仅次于美国，增长速度位居世界前列。

✓ 随着数字经济快速发展，数据资产已成为现代经济社会的重要生产要素。
✓ 随着其价值增大，使用面的扩展，与此同时面临的安全风险也越来越高。

数据安全形势日趋严峻



392万美元

全球平均数据泄露总成本

150美元

单条丢失记录成本

25,575条记录

数据泄露平均规模

美国

平均成本最高的国家/地区（819万美元）

279天

识别和遏制数据泄露所需时间

案例一：

英国航空公司数据泄露事件

根据欧盟《通用数据保护条例》规定，企业如未经用户同意收集个人数据，将被处以最高2000万欧元或全球营业额4%的罚款。

2018年9月，也就是在欧盟《通用数据保护条例》（“GDPR”）生效几个月后，英国航空遭受了重大的个人数据泄露事件。该事件导致约 50 万名客户的个人信息被泄露。在该事件中，用户流量被移转到虚假网站，攻击者通过这个虚假网站收集了客户详细信息，包括客户个人信息和银行卡信息，如姓名、地址、邮箱，以及信用卡的号码、有效期和背面的验证码（CVV）等。

英国航空公司向 ICO （英国信息专员办公室）通报该数据泄露事件。

ICO专员伊丽莎白·德纳姆（Elizabeth Denham）说：“用户的个人数据就是他们的私人财产，当一个组织无法保护个人数据免受盗窃和破坏时，这对用户而言绝不仅仅是不方便而已，而是私人财产的损失。法律已经列明，当组织被委托处理个人资料时，必须确保资料的安全。那些没有做好数据资料保护的企业将会面临审查。”2019年7月8日，ICO宣布已发布意向通知书，对英国航空处以1.8339亿英镑的罚款【“意向通知”】。

案例二：

剑桥分析事件

2019年7月24日，美国联邦贸易委员会对社交网络巨头脸书公司开出高达56亿美元的罚单，并对剑桥分析公司(简称剑桥分析) 提出了行政诉讼，指控其采用欺骗手段从脸书数千万用户那里收集个人信息并进行选民分析。

案例三：

“亚马逊”天价罚款事件

根据欧盟《通用数据保护条例》规定，企业如未经用户同意收集个人数据，将被处以最高2000万欧元或全球营业额4%的罚款。

据2021年7月30日彭博社报道，因违反欧盟《通用数据保护条例》（简称“GDPR”），亚马逊可能面临欧盟有史以来最大数据隐私泄露罚款，共计7.46亿欧元（约合8.88亿美元）。而亚马逊在面临天价罚款的同时，还被责令修改没有具体说明的某些商业惯例。

亚马逊方面针对此事做出回应，发言人表示：“保护用户的信息安全，以维系他们的信任，是我们的首要准则。我们没有将任何用户的数据泄露给第三方。我们坚决反对CNPD（卢森堡数据保护委员会）的指控，并将进一步上诉。关于我们是如何向用户投放相关广告这一点，CNPD仅仅是依赖对于欧洲隐私法的主观臆断，对我们作出的判决，况且，就算这项解释成立，罚款金额也远远高出对应标准。”

案例四：

“滴滴出行” 事件

6月30日滴滴在美国挂牌上市

7月2日国家网络安全审查办公室对“滴滴出行”启动网络安全审查

7月4日国家网信办通报要求下架“滴滴出行”

7月9日国家网信办通知应用商店下架滴滴旗下另外25款APP

7月16日七部门进驻滴滴开展网络安全审查

国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等

02

全球数据安全与个人信息保护的立法现状

国际数据保护相关的立法进展

近年来，个人信息保护立法在世界范围内如火如荼地展开，目前已经有 128 个国家通过立法保护个人信息和隐私。其中，结合市场规模，规制范围等因素，以欧盟《通用数据保护条例》(以下简称“ GDPR”)、美国加利福尼亚州隐私保护法(CCPA&CPRA) 为代表。

- **CCPA** 是2018 年 6 月 28 日签署的，是一项旨在增强美国加利福尼亚州居民隐私权和消费者保护的州法规。在其基础上，2020 年 11 月 3 日加州选民投票通过了 CPRA，对 CCPA 的 一些重要条款进行了修正，扩展了 CCPA 的范围并制定了新的执行机制。CCPA 和 CPRA 共同构建了加州隐私保护法的主要制度框架，两者均是对《加利福尼亚民法典》(California Civil Code)第三章第四部分进行的修改。

- **GDPR**于2018年5月25日正式生效，前身是欧盟在1995年制定的《数据保护指令》（95/46/EC）。在GDPR中主要规定了作为数据主体——普通用户的知情、访问权、更正权、删除权、限制处理权、反对权和自动化个人决策等相关权利。并且原则上禁止计算机算法程序处理个人敏感程序包括：种族或民族出身、政治观点、宗教或哲学信仰、工会成员身份、涉及健康、性生活或性取向的数据、基因数据（新）和经处理可识别特定个人的生物识别数据（新），较以往的指令新增了最后两项，并且允许成员国通过制定细则的方式增加新的条件作为GDPR的补充。

中国：作为生产要素的“数据”，日益受到国家的重视

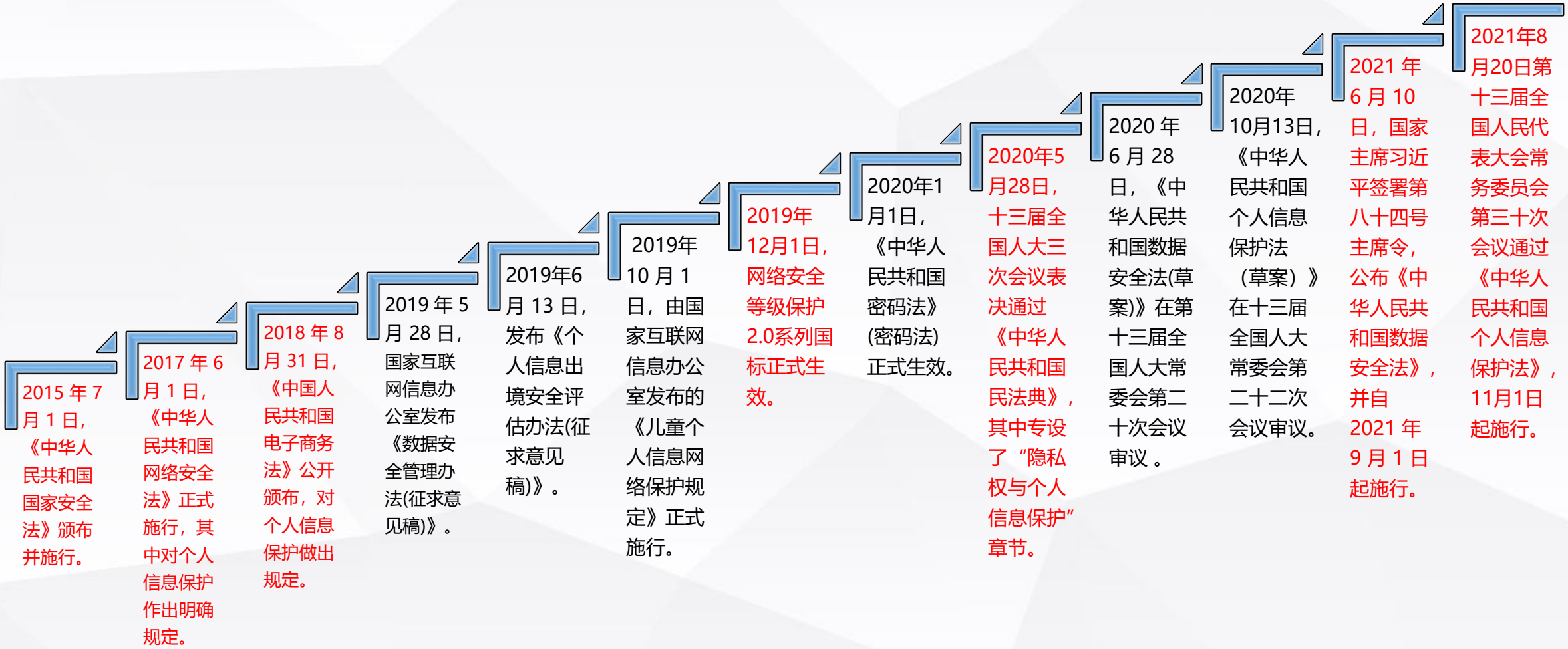
党的十九届四中全会提出，健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制。这是党中央首次提出将数据作为生产要素参与收益分配，体现了在数字经济快速发展背景下社会主义基本经济制度的与时俱进，是一个重大的理论创新。同时，也标志着我国正式进入数字经济“红利”大规模释放的时代，数据作为新生产要素从投入阶段发展到产出和分配阶段。

2020年4月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，将数据作为与土地、劳动力、资本、技术并列的生产要素，要求“加快培育数据要素市场”。数据要素涉及数据生产、采集、存储、加工、分析、服务等多个环节，是驱动数字经济发展的“助燃剂”，对价值创造和生产力发展有广泛影响，推动人类社会迈向一个网络化连接、数据化描绘、融合化发展的数字经济新时代。

在数据安全保护方面，中国“十四五”提出新的要求：

- **数据跨境传输安全和大数据保护方面**：强调要建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范，推动数据资源开发利用；完善适用于大数据环境下的数据分类分级保护制度。加强数据安全评估，推动数据跨境安全有序流动。
- **公共数据安全方面**：强调要建立健全国家公共数据资源体系，确保公共数据安全，扩大基础公共信息数据安全有序开放。
- **国家数据安全和个人信息保护方面**：明确要保障国家数据安全，加强个人信息保护；加强涉及国家利益、商业秘密、个人隐私的数据保护，加快推进数据安全、个人信息保护等领域基础性立法，强化数据资源全生命周期安全保护。

中国：《个人信息保护法》《数据安全法》与国家安全、网络安全领域法律相衔接并初步构建起体系完整的法律法规



国内网络安全及数据合规整体环境趋严，社会各界重视程度越来越高

1、国有企业的合规要求严厉程度与日俱增；

2、资本市场和各大交易所对于涉及数据合规的问题审查严格；

3、工信部门、网信办高强度密切关注并开展检查；

4、央行、卫健委、教育等行业部门的跟进检查；

5、检察院民事公益诉讼；

6、消费者对于个人信息保护的维权意识不断增强；

7、社会舆论的高度关注；

8、企业商誉的影响。

03

国内立法解读

《民法典》（2021）

- 人格权编中对隐私权和个人信息做了专章规定

- 第1034条 个人信息的定义及其外延
- 第1035条 个人信息处理的定义和原则
- 第1036条 个人信息处理的合法事由
- 第1037条 自然人的查阅、复制、更正、删除权
- 第1038条 处理者的个人信息保护义务
- 第1039条 国家机关及其工作人员的保密义务
- 第1164-1187条 侵权责任的一般规定和损害赔偿
- 第1194-1197条 网络服务提供者通知的义务和侵权责任
- 第1225条 患者查阅、复制病例资料的权利
- 第1226条 医疗机构及其医务人员的保密义务和侵权责任

《刑法》

- **第253条之一 侵犯公民个人信息罪（2015）**
  - 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。

- **第285条第2款 非法获取计算机信息系统数据、非法控制计算机信息系统罪（2009）**
  - 违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，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。
  - 单位犯前款罪的，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。

《刑法》

- **第286条之一 拒不履行信息网络安全管理义务罪（2015）**
  - 网络服务提供者不履行法律、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，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：
  - （一）致使违法信息大量传播的；
  - （二）致使用户信息泄露，造成严重后果的；
  - （三）致使刑事案件证据灭失，情节严重的；
  - （四）有其他严重情节的。
  - 单位犯前款罪的，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，依照前款的规定处罚。
  - 有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

《消费者权益保护法》（2013）

- **第14条　消费者的个人信息保护权**
  - 消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。

- **第29条　合法正当必要原则、同意原则、目的限制原则、经营者的保护义务**
  - 经营者收集、使用消费者个人信息，应当遵循合法、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。经营者收集、使用消费者个人信息，应当公开其收集、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。
  - 经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。
  - 经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

《电子商务法》（2016）

- **第二十四条**
  - 电子商务经营者应当明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件。
  - 电子商务经营者收到用户信息查询或者更正、删除的申请的，应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的，电子商务经营者应当立即删除该用户的信息；依照法律、行政法规的规定或者双方约定保存的，依照其规定。
- **第三十二条**
  - 电子商务平台经营者应当遵循公开、公平、公正的原则，制定平台服务协议和交易规则，明确进入和退出平台、商品和服务质量保障、消费者权益保护、个人信息保护等方面的权利和义务。

《网络安全法》（2017）

- 第41条 合法正当必要原则、同意原则、目的限制原则
- 第42条 网络运营者的个人信息保护义务
- 第43条 个人的删除、更正权
- 第45条 个人信息保护义务
- 第64条 违反第41-43条，处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款

《网络安全法》（2017）

- **第四十一条** 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。
- **第四十二条** 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者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，防止信息泄露、毁损、丢失。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。
- **第四十三条** 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。
- **第四十五条** 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。
- **第六十四条** 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、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；情节严重的，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。
- 违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

《数据安全法》（2021）

适用范围

- 在中华人民共和国境内开展数据处理活动及其安全监管；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。
- 数据是指任何以电子或者其他方式对信息的记录。

制度体系

- 数据分类分级保护、重要数据保护、国家核心数据保护制度
- 数据安全审查制度
- 数据出口管制制度
- 数据安全风险管理和监测预警机制
- 数据安全应急处置机制

监管部门

- 中央国家安全领导机构及各地区、各部门行业主管部门（工业、电信、交通、金融、自然资源、卫生健康、教育、科技等）
- 公安机关、国家安全机关等
- 国务院标准化行政主管部门和国务院有关部门
- 国家网信部门

保护义务

- 处理活动应合法正当，符合社会公德和伦理
- 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，履行数据安全保护义务，并应加强风险监测和事件应急响应
- 重要数据处理者还应明确数据安全负责人和管理机构，定期开展风险评估并报送报告，依据出境管理规定管理出境活动等

法律责任

- 责令改正，给予警告
- 罚款：组织、个人五万元~二百万元；主管、直接负责的主管人员和其他直接责任人员一万元~二十万元，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
- 罚款：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，二百万～一千万元
- 其他：依法追究刑事责任、依法承担民事责任、依法给予治安管理处罚等

《个人信息保护法》（2021）

- 《个人信息保护法》起草过程中借鉴了GDPR的思路和范式

（一）明确个人信息处理的合法基础

《个人信息保护法》列举了个人信息处理的合法基础包括授权同意、为订立或履行个人作为一方当事人的合同所必需、履职必需、应对突发公共卫生事件、在合理的范围内处理已公开的信息、公益目的等等，总体而言采取了优先保护个人权利和社会公共利益的路径。

（二）为个人赋予撤回同意的权利

考虑到实践中普遍存在的不支持注销账户、撤回同意投诉无门等问题，《个人信息保护法》要求个人信息处理者提供便捷的撤回同意方式。就“便捷”而言，依照相关国家标准的精神，其便捷程度宜与给予授权的便捷程度相对等。

（三）将不满十四周岁未成年人的个人信息列入敏感个人信息

《个保法》明确要求将不满十四周岁未成年人的个人信息作为敏感个人信息加以保护。因此相关数据处理者可能需要更改内部数据分级分类的标准，依照我国法律和相关标准对敏感信息的要求对涉及的不满十四周岁未成年人的个人信息进行特别保护。

（四）针对自动化决策提出明确要求

针对用户画像、“大数据杀熟”等问题，《个人信息保护法》立足于维护广大人民群众的网络空间合法权益，充分吸收了成熟国家标准与行业实践的内容，从算法伦理、数据获取、数据使用、风险评估和日志记录的方面对自动化决策进行了规制。

（五）全面规范个人信息跨境的规则

《个人信息保护法》设置专章对个人信息跨境提供的规则进行了全面的规范，与《数据安全法》《网络安全法》形成了完善的法律体系衔接。

（六）明确个人信息侵权行为的归责原则为过错推定

《个人信息保护法》明确了当个人信息权益因个人信息处理活动受到侵害时，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。

04

对企业的影响

理解企业的多重身份

网络运营者

重要数据处理者

个人信息处理者

国家核心数据处理者

数据处理者

关键信息基础设施运营者

- 部分企业可能涉及重要数据的处理
- 少数企业可能涉及国家核心数据的处理和（或）关键信息基础设施运营

严苛的法律责任（《数据安全法》）

- **第四十五条**　**开展数据处理活动的组织、个人**不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，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；**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，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。**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。
- **第四十六条**　违反本法第三十一条规定，**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。
- **第四十七条**　从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，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，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，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一万元以上十万元以下罚款。

严苛的法律责任（《个人信息保护法》）

- **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。

05

企业应怎么做？

数据合规和个人信息安全规范要求的简介

企业内部管理制度和操作规程的完善

法律依据：《数据安全法》

第二十七条 开展数据处理活动应当依照法律、法规的规定，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。

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。

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

法律依据：《个人信息保护法》

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。

企业个人信息安全事前影响评估

法律依据：《个人信息保护法》

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：

（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；

依据：《信息安全技术个人信息安全规范》3.9、11.4

- 国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020 年第 26 号），GB/T 39335-2020《信息安全技术个人信息安全影响评估指南》
- 欧盟《通用数据保护条例》第25条数据保护影响评估

定期开展
风险评估/合规审计

法律依据：《个人信息保护法》

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。

法律依据：《数据安全法》

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。

- **中国科学技术法学会T/CLAST 001—2021《个人信息处理法律合规性评估指引》团体标准**

企业个人信息出境合规

法律依据：《个人信息保护法》

- 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。

企业个人信息出境合规

法律依据：《数据安全法》

第三十一条　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办法，由国家网信部门会同国务院有关部门制定。

《个人信息出境安全评估办法》（征求意见稿）

数据安全教育培训

法律依据：《数据安全法》

第二十七条规定“开展数据处理活动应当依照法律、法规的规定，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。
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。”

法律依据：《个人信息保护法》

第五章第五十一条规定：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：
（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；

数据保护官

- 依照欧盟《一般数据保护条例》（即GDPR）的要求，为有需要的企业委派有DPO资质的专业人士承担企业数据保护合规职责。

- 对企业的GDPR合规性以及数据保护工作进行监管；
- 参与和管理企业的data protection impact assessments(DPIAs) 工作；
- 作为沟通渠道同欧洲GDPR监管部门保持联系，负责数据外泄的紧急汇报和协调处理；
- 负责同数据主体沟通和联系，协助实现数据主体的数据权利；
- 客观独立的履行自己的职责，不因行政命令或企业高管意见而影响客观事实和结论；
- 有权直接向企业最高管理决策层汇报工作。

企业个人信息保护负责人外包服务，或者成为企业个人信息保护工作机构成员

法律依据：《个人信息保护法》

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。

法律依据：《数据安全法》

第二十七条 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。

依据：《信息安全技术个人信息安全规范》

11.1 明确责任部门与人员

成立主要由外部成员组成的独立机构
&
定期发布个人信息保护社会责任报告

法律依据：《个人信息保护法》

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。

事件应对与处理

数据相关法律纠纷的处理及争议解决

谢谢

声明