-国家工程实验室和天枢智库联合出品-

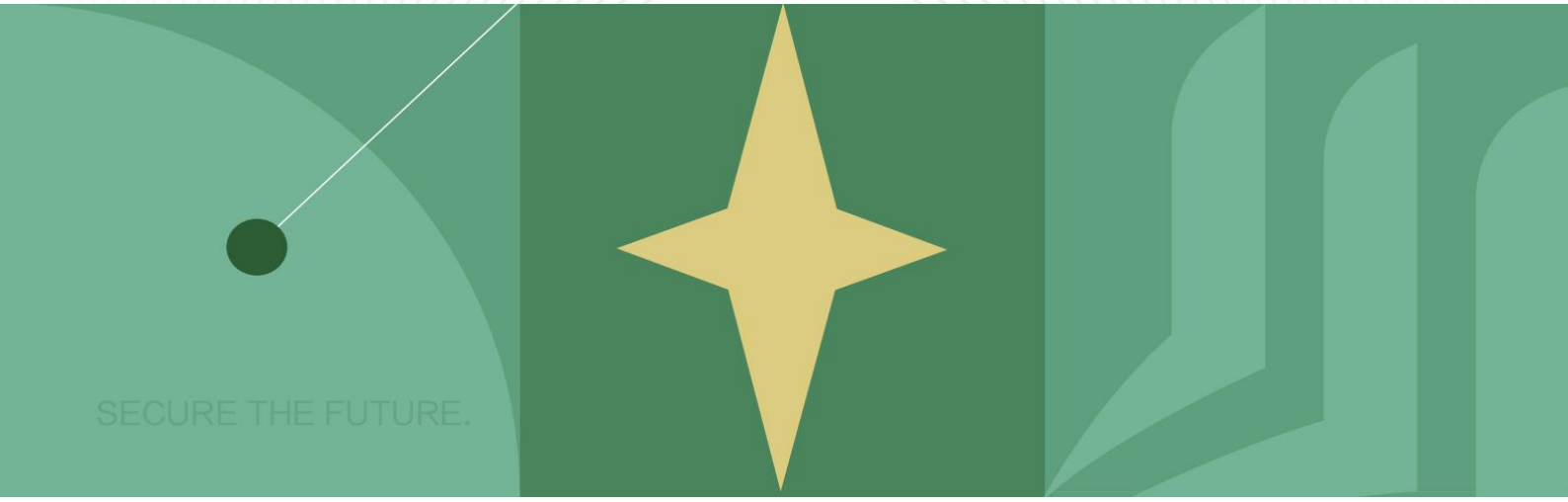
# 安全观察

SECURITY INSIGHT

数据安全专刊 No. 001(总第 52 期)

责编：钟力 zhongli1@360.cn

安全研究 | 大咖观点 | 政策形势 | 安全事件



《安全观察·数据安全专刊》是专注于数据安全领域的专刊，聚焦数据安全动态、政策分析、行业发展、技术研究。第一期《安全观察·数据安全专刊》发布在《数据安全法》实施之际，重点关注《数据安全法》，以后将持续跟进数据安全技术和行业发展趋势。

# 导读

2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议表决通过了《数据安全法》，并宣布于 9 月 1 日起正式施行。值此国内数据安全领域第一部法律落地实施之际，《安全观察·数据安全专刊》第一期也同步推出。同时，《个人信息保护法》也于 8 月 20 日宣布通过表决，并于 11 月 1 日起正式施行。伴随着这两部法律的颁布和落地实施，我国的数据安全与隐私保护工作也将开始有法可依。

《安全观察·数据安全专刊》第一期内容主要包括安全研究、大咖观点、政策形势、安全事件四个板块，主要看点如下：

安全研究方面，本期收录了大数据协同安全技术国家工程实验室关于数据安全方面的研究成果。其中，“《数据安全法》解读”一文对《数据安全法》进行了全面的解读；“《数据安全法》指导下的数据安全发展之路”一文从开发利用与安全的平衡角度，对未来数据安全发展之路提供了可参考的建议；“《个人信息保护法》解读”则结合企业实际对法律重点内容给出详细分析；此外，也有结合汽车数据安全管理以及热门的滴滴网络安全审查事件所做的分析研究。

大咖观点方面，本期汇聚了政府、产业界、学术界等各界大咖的演讲和代表性观点。聚焦数据安全发展热点，以主旨演讲以及研究观点精选的方式，给读者带来一次覆盖数据安全领域不同身份的观点合集，旨在展现数据安全行业新趋势，凝聚行业新气象，解读未来数据安全发展新风向。

政策形势方面，主要围绕《数据安全法》，选取了 2021 年 TOP 10 数据安全领域的政策消息。其中囊括了本年度备受瞩目的《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》《汽车数据安全管理若干规定（试行）》、地方政府颁布的数字经济条例以及美国颁布的网络安全和数据隐私保护法律等。

安全事件方面，本期主要选取了 2021 年第三季度内泄露数据量较大、关注度较高的热点事件，主要类型集中在数据泄露、勒索攻击以及合规挑战方面。其中比较吸引眼球的是美国电信巨头 T-Mobile 超 1 亿用户的数据泄露事件，这是继美国油气管道遭勒索攻击后的又一起针对基础设施的攻击事件，据悉，攻击者的这次行动是为了进行打击报复美国。另外还值得关注的是，亚马逊因违反数据隐私法规被欧盟处以 8.88 亿美元罚款，创下了 GDPR 有史以来最大的数据隐私泄露罚单记录。

# 目 录

## 第一部分 安全研究



## 第二部分 大咖观点



## 第三部分 政策形势

## 第四部分 安全事件

# （一）安全研究

## 《数据安全法》解读

大数据协同安全技术国家工程实验室

2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议通过了《数据安全法》，这是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于 2021 年 9 月 1 日起施行。经过三次审议稿陆续收集到社会各界的广泛意见，本次终稿终于浮出水面。终稿能够在很短的时间内得到人大审核通过，说明了数字经济发展对安全的关键需求，《数据安全法》的发布具有很强的紧迫性和重大的意义。《数据安全法》将给数据安全产业带来巨大利好，未来国家也将陆续出台不同行业不同领域的数据安全指引。为此，大数据协同安全技术国家工程实验室主要从大数据安全开发利用的角度，对《数据安全法》进行解读。

### 一、《数据安全法》的主要目的

**（1）保障国家数据资源安全。**核心的目标是保障国家所拥有的数据资源免于遭受来自国内或国外的篡改、破坏、泄漏或者非法获取、非法利用（第 1 条）。

**（2）促进国内数据开发利用和产业发展。**包括鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进数字经济发展（第 1，2，7，11 条）。

**（3）保障组织和公民的数据权益**（第 2，7，8，21 条）。

**（4）保障国际数据活动中国家安全、主权和利益。**包括保障数据跨境安全自由流动，国际数据和数据开发利用技术反歧视（第 2，11，25，26，36 条）。

## 二、重点解读

### 1、明确数据安全各方职责

法律明确了建立工作协调机制，加强对数据安全工作的统筹，国家各个层级机构对于数据安全工作的职责定位，并细化了相关的法律责任和经济处罚，为各部门、各行业、各领域在后续执行数据安全工作奠定了基础，做到有法可依、违法必究。归定了“一委多部门”的数据安全领导和监管体系，即由中央国家安全领导机构总体负责和统筹，公安机关、国家安全机关、国家网信部门、行业主管部门（工信部、自然资源部、卫健委、教育部、国防科工局、央行、银保监会、证监会等）分头监管（第 5，6 条）。

### 2、鼓励数据安全、合法、有序流动

法律明确了数据作为数字经济发展的关键要素，需要被组织和个人依法合理有效利用，国家鼓励数据安全有序自由流动（第 7，11，21 条）。同时，明确了跨境传输场景的数据安全要求（第 36 条）。

### 3、数据开发利用和数据安全相互促进

法律明确了国家在实施大数据战略进程中，要以数据安全保障数据的开发利用和产业发展（第 14 条）。而且，在国家支持开发利用数据提升公共智能化水平的同时，要充分考虑老年人、残疾人的条件与需求（第 15 条）。

### 4、建立数据安全管理制度

法律明确了国家建立数据分类分级保护制度，确定了数据分类分级的基本原则，要求制定重要数据目录，并明确了核心数据的定义与管理要求（第 21 条）；明确了国家建立集中统一数据安全风险评估、报告、信息共享、监测预警机制（第 22 条），国家建立数据安全应急处置机制（第 23 条），以及国家建立数据安全审查制度（第 24 条），并要求数据安全保护与等级保护制度相结合（第 27 条）。

### 5、确保政务数据安全

法律明确在国家十四五规划进程中，国家将大力推进电子政务建设，政务数据开放将进一步提升政府工作效能，政务数据在采集、存储、加工过程中的安全非常关键，政务数据需要被合理、合法、安全的使用（第 37-43 条）。

### 6、法律责任更加明确，最大金额 1000 万

基于数据安全违规场景，法律更加细化了违规法律责任，并制定了直接负责的主管人员和其他直接责任人的处罚细节，最高金额提高到 1000 万（第 44-52 条）。

## 三、数据安全产业机会分析

### 1、大数据平台安全和安全监管产品迎来发展良机

安全、高效的大数据平台安全产品或套件，以及数据使用和流通共享过程中的安全监控、风控、协同响应等产品和技术方案会有很多市场机会。从战略价值看，从 IT 到 DT 的时代，未来企业之间的竞争是数据的竞争，布局大数据安全和安全运营产品，是企业快速发展抢

占战略制高点、提升核心竞争力的前提。目前数据安全厂商都在开辟新的赛道，无明显寡头出现，数据识别、数据分类分级、数据脱敏、隐私计算和数据安全运营等方向布局较多。市场主要客户包括政府、运营商、金融机构等。

**2、基于 DSMM 的数据安全治理持续推进**

数据安全能力成熟度模型（DSMM）作为业内已探索实践多年的数据安全治理抓手，无疑会迎来更好的发展机会。数据安全需要在国家统筹指导下，全社会各方共同努力，才能建立起科学的行之有效的数据安全治理体系。DSMM 相关的咨询、培训、测评、认证、审计等数据安全服务会有很大的市场空间。其战略价值是，可通过以 DSMM 为抓手的数据安全治理体系，介入客户的数据安全顶层架构设计。目前市场需求量大，企业多具备数据安全治理基础，但需要持续提升数据安全治理成熟度水平，确保安全合规运营。主要客户包括适用于有数据安全治理需求的各行各业，重点在政务、金融、电信产业和工业企业。

**3、数据安全人才培训受到广泛重视**

企业或组织不仅需要专业的数据安全管理人员去驾驭数据安全项目、解决方案和数据活动，还需要专业的数据安全技术人员去设计开发产品，以及专业的数据安全运营人员去部署产品和分析安全事件，拥有专业的数据安全管理和技术人才已经成为现代企业不可或缺的重要安全保障。《数据安全法》明确国家支持教育、科研机构和企业等开展数据安全相关教育和培训，采取多种方式培养数据开发利用技

术和数据安全专业人才，数据安全人才培训市场将迎来爆发。比如工程实验室就顺应时代潮流，推出了数据安全官和数据安全工程师的培训，为数据安全行业培养专业人才。

**4、政企级数据安全咨询地位日益重要**

过去大部分的数据安全咨询项目通常由普华永道、安永、德勤和毕马威等国外四大咨询机构获得。随着数字经济的发展，由于数据价值的凸显及其敏感性因素，更多的数据安全咨询项目机会将会转向国内数据安全机构和厂商。数据流通共享及其应用场景的复杂性提升，使得数据安全咨询地位与日俱增。咨询项目的价值是，在提供咨询过程中，识别组织的重要数据资产，提供端到端的数据安全解决方案，为数字经济发展保驾护航。目前市场需求逐年增大，通常由咨询机构提供咨询服务，各家主流安全厂商提供产品落地，方案需要结合业务场景持续优化提升数据安全治理成熟度水平。主要客户是适用于有数据安全治理需求的各行各业，重点在政务、金融、电信产业和工业领域。

**四、小结**

《数据安全法》明确提出维护国家数据主权，保护个人、机构数据权益，体现了国家对数据安全领域的高度关注，且“鼓励数据依法合理有效利用，保障数据依法有序自由流动”。值得注意的是，国家监管机构的思路逐渐由“以系统为中心的安全”转变为“以数据为中心的安全”，并反复强调这是适应现在数字经济模式的数据安全。该法为政府、产业界开展数据安全工作提供了重要的法律支撑，为企

业发展数据安全业务提供了很好的指导，利于形成全社会共同维护数据安全和促进发展的良好环境。

## 《数据安全法》指导下的数据安全发展之路

大数据协同安全技术国家工程实验室

刊登于《中国信息安全》杂志

作为我国数据安全领域的基础性法律、国家安全领域的重要法律，《数据安全法》的出台体现了当前数字经济发展对安全的关键需求，为我国数据安全的发展之路提供了指引。在数字经济发展的场景下，跨系统、跨域和跨境的数据流通共享以及多方的数据联合计算将成为常态，数据安全将不再是一个组织内部的事情，需要构建一个科学的数据安全治理体系，才能有效地保障数据安全，管控数据安全风险。而且，数字经济创新发展的关键在于数据的安全开发利用，需要数据安全和数据开发利用两者的协调发展。

### 一、建立健全数据安全治理体系

治理不同于自上而下的管理，而是基于关键抓手的、能够充分激发各相关方内驱力的多方协同共治的方式方法。数据已经成为新的生产要素，如果一种数据安全治理体系能够建立起数据与数据处理方之间的正向驱动关系，那么这种体系无疑是非常具有生命力的。

#### （1）构建基于 DSMM 的数据安全治理体系

《数据安全法》第四条提出：“维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。”

治理体系的构建对系统性提高国家的数据安全保障能力非常关键，需要找到关键抓手和基本逻辑，来调动多方力量和资源，发挥各自优势形成良性生态，建立适应当今数字时代的协同治理模式，共同提升全社会的数据安全水平。

国家标准 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》（DSMM）是我国有关数据安全治理的首个技术标准，提出了数据安全能力成熟模型。建立基于 DSMM 的数据安全治理体系，以数据为中心，能够系统性提高我国数据安全整体水平。它在数据分类分级的基础上，从组织建设、制度流程、技术工具和人员能力四个方面，对组织的数据安全能力成熟度进行测评和等级划分，从而在数据和组织间建立正向驱动的关系。根据组织的数据安全能力成熟度等级，可以决定其是否具有处理特定类型、特定等级数据的资质，以实现对数据安全风险的科学管控。这意味着，一个具有更高数据安全能力成熟度等级的组织，能获得处理更多数据资源的机会。该体系将改变过去“合规+处罚”的做法，使组织的数据安全水平成为发展的竞争力，从而激发组织主动提升其数据安全能力。

**（2）数据侧以数据分类分级为基础和前提**

《数据安全法》第二十一条明确提出“国家建立数据分类分级保护制度”，在此基础上，又专门规定了对重要数据的保护，要求各地区、各部门、各行业制定各自范围内的“重要数据目录”，并进一步指出“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”。数据分类分级保

护制度作为数据安全治理的基础与前提，将为国家开展“自上而下”的监管提供依据，推动建立重要数据与国家核心数据的统一认定标准；同时，也直接决定了组织对于不同类别与等级的数据在安全上应承担的保护义务，并对组织自身的数据安全能力提出了相应的要求。

目前，各地区、各部门正根据《数据安全法》在制定地方或行业领域的数据分类分级规范，积极推进数据分类分级保护工作。例如，贵州省率先制定发布了《政府数据 数据分类分级指南》，在全国先试先行；工业和信息化部办公厅发布了《工业数据分类分级指南（试行）》，提出对工业数据的分类和分级标准；金融行业发布了行业标准《金融数据 安全数据安全分级指南》和《证券期货业数据分类分级指引》。数据分类分级已从探索走向实践，各数据安全厂商纷纷发布创新的数据分类分级产品，敏感数据发现和分类分级管理的自动化工具正在被开发使用，极大地提升了数据安全治理的效率。

**（3）处理侧以对组织的数据安全能力成熟度测评为抓手**

在对数据进行分类分级之后，对组织的数据安全能力成熟度进行测评成为构建治理体系的关键抓手。《数据安全法》第十八条指出“国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动”，是对数据安全相关测评特别是 DSMM 测评认证最好的支持，在法律层面充分肯定了测评认证专业机构在带动数据安全合规建设和服务发展方面的积极作用。目前，我国已发展形成了多个从事 DSMM 测评认证的专业机构，包括首个获得国家认监委授权的 DSMM 认证机构贵州大数据安全工程研究中心，

正在全国范围内推广实施DSMM测评认证，并有超过百家组织通过了测评。

通过DSMM测评认证，组织能够获得全方位的数据安全建设指导性纲要，使其对自身的数据安全建设充满信心。对企业来说，能够对自身数据安全整体状况做到心中有数，并可将“数据安全能力水平”作为宣传自身品牌的差异化标签。对政府机关、事业单位来说，除了能及时发现数据安全短板、查漏补缺之外，还可掌握地方相关组织、部门的数据安全整体水平。与此同时，各地政府也逐步认识到DSMM测评认证的重要性，纷纷出台激励政策鼓励企业或组织参加DSMM测评认证，对获得证书的企业或组织进行补贴，并在一些重要数据安全项目招标中加入DSMM测评认证的控标要求。

## 二、保障数据安全与数据开发利用的协调发展

数字经济已成为支撑我国经济发展的重要引擎，数据开发利用则是数字经济创新发展的关键，需将保障数据安全贯穿于数据开发利用的全过程，防范和化解影响我国数字经济发展过程中的安全风险，同步提升数据安全和数据开发利用水平。

### （1）在数据安全与发展之间取得平衡

《数据安全法》第二章的主题是数据安全与发展，并于第十三条提出：“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”。可见，该法的目的是取得数据安全与发展之间的平衡，保障数据安全与促进数据开发利用和产业发展是相辅相成的，既不能以发展之名忽略安全，也

不能以安全之名阻碍发展。数字经济需要充分挖掘数据的价值，将数据作为生产要素进行开发利用，同时，在数据开发利用的过程中，又需要充分保障数据的安全。

数据的开发利用为数据安全提供了技术支持和概念革新，数据安全为数据的开发利用提供了基础的保障和稳固的底盘。数字经济时代与过去不同，在很多场景下会先有数据再有应用，基于数据的数字创新应用开发将成为常态。数据安全影响国家发展与安全，关系公众利益和公民个人权益，应建立数据全生命周期安全的概念，关注数据的流通共享，确保以安全为前提进行数据的开发利用。

**（2）推进政务数据安全开发利用**

《数据安全法》第五章聚焦的政务数据安全与开放，是数据安全开发利用的一个特定应用场景。它在保障政务数据安全方面，对国家机关收集、使用数据的行为和能力提出了要求，严格监督可能涉及的第三方；在推动政务数据开发利用方面，明确了以及时、准确公开为原则，要求“国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台”，这为政府各部门迈开步子安全开放数据提供了法律支持和行动指导，为我国数字政府和智慧城市建设铺平了道路。

国家在“十四五”规划进程中将大力推进电子政务建设，政务数据开放将进一步提升政府工作效能，政务数据在采集、存储、加工过程中的安全非常关键，需要被合理、合法、安全地使用。在智慧城市应用场景下，跨域数据的流通共享与联合计算需求日益增多，政务数

据开放平台和基于隐私计算技术的数据协同应用平台将得到广泛应用。利用可信执行环境、联邦学习、安全多方计算、同态加密和差分隐私等技术搭建隐私计算平台，可实现多方数据的协同安全计算，它与政务数据开放平台一起，能够打破数据孤岛，联通政务数据和各行业领域数据，从而促进政务数据的安全开发利用，充分挖掘政务数据的价值。

**（3）为数据安全开发利用培养足够的专业人才**

数据安全开发利用离不开相关专业人才的支撑，《数据安全法》第二十条明确提出“国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。”这体现了国家对培养数据安全专业人才的重视，鼓励企业与高等院校联合，从多个渠道培养数据开发利用和安全人才。企业也能够从教育培训等领域寻找自身商业机会，带动数字产业的发展与创新。通过专业的培训，能够提高组织人员的数据安全技能，为数据安全产业发展和数字经济发展注入强大的人才动力。

经过多年的发展，我国在网络安全领域已建立起较为完善的人才培养体系，网络安全也成为一级学科。在数据安全领域，人才的培养还没有上升到数字经济所要求的高度，相关的培训内容还不够完善。对于数据安全，既需要拥有了解组织数据安全战略规划的数据安全管理专家，也需要懂具体业务场景，掌握相关数据安全技术的数据安全工程师。因此，为支持组织良性发展，提高组织人才的数据安全意识，

大数据协同安全技术国家工程实验室推出了注册数据安全官、注册数据安全工程师、DSMM 测评师的培训，服务于数据安全治理体系的构建，为业界培养专业的数据安全管理人才和技术人才。

## 三、对数据跨境流动进行严格安全审查

《数据安全法》第二十四条明确提出：“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”，包含对数据跨境流动的安全审查。第三十一条规定了关键信息基础设施运营者重要数据的出境安全管理，适用《网络安全法》的规定，其他主体重要数据的出境则适用于国家网信部门会同国务院制定的管理办法。通过区分主体的监管思路，进一步明确补充了对重要数据出境的规定，也使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，法案第三十六条针对外国司法或执法机构调取我国数据的情况进行了规定，即非经主管机关批准，境内组织、个人不得擅自提供境内的数据，此举是依法应对域外“长臂管辖”所作出的防御性措施。

在当前全球尚未形成共识的数据安全治理体系框架条件下，数据的跨境流动带来了敏感数据泄露、授权管理、数据权属、流向追踪和法律风险等系列问题，并难以对数据接收方的数据处理活动进行监控和审计。因此，对于涉及国家、公民的敏感数据，要严格遵守“非必要不出境”原则，尽量做到数据在本地存储、分析和利用。确需出境的数据，需经过匿名化、去标识化和脱敏处理，并对跨境数据进行严格的安全审查，杜绝敏感信息外泄。对于关系国家安全、国民经济命

脉、重要民生、重大公共利益的国家核心数据，应严禁跨境流动并防范潜在数据跨境风险，防止滴滴美国上市类似事件的发生。

## 对汽车数据安全的几点认识与思考

大数据协同安全技术国家工程实验室

刊登于《中国信息安全》杂志

为加强个人信息和重要数据保护，规范汽车数据处理活动，根据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同有关部门起草了《汽车数据安全管理若干规定（征求意见稿）》（以下简称《规定》），向社会公开征求意见。这是我国首个汽车行业数据安全管理的规章制度，是针对目前智能网联汽车在发展过程中引发公众关注的数据安全问题的监管回应。我们基于大数据协同安全技术国家工程实验室多年来在数据安全治理方面的研究和实践工作，在梳理与解读该规定重点内容的基础上，谈一谈汽车数据安全的几点认识和思考。

### 一、汽车数据利用与数据安全应达成平衡

#### （1）数字经济时代需鼓励数字创新应用

随着人工智能、物联网和大数据分析等技术的广泛应用，经济社会发展日益呈现数据驱动的新态势，各类个人信息的处理活动不断拓展，数据安全与发展的动态平衡已成为数字经济领域各类新业态、新产业、新模式创新发展的关键。刚发布的《数据安全法》明确提出，“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安

全，以数据安全保障数据开发利用和产业发展”，其明确了国家鼓励数据依法合理有效利用，以促进数字经济发展。

从现在低级别的辅助驾驶，到未来高级别的自动驾驶，为了应对复杂多样的路况和行车场景，数据的收集与分析利用是汽车智能驾驶在发展道路上不可或缺的动力源泉。而且，汽车作为人们的一个重要的生活空间，也将发展成为一个智能综合体，汽车拥有的数字创新应用会成为一个品牌汽车能否取得市场成功的关键因素。因此，汽车产业需要鼓励汽车数据的开发利用，鼓励数字创新应用的发展，不能单纯为了保障数据安全而遏制了数据的合法合规收集与数据开发利用，需要在两者之间根据数字经济时代的发展特点取得恰当的平衡。

**（2）需正确把握汽车数据采集的度**

在汽车智能网联化的大潮中，很多行车安全功能的实现离不开数据的采集，自动驾驶所需的感知、决策、控制都依赖于大数据采集的各种场景，保障车主人身安全也需要行车路线和位置数据的采集，只有收集了这些数据才能使人车配合得更加紧密。我们知道，疫情时期健康宝的使用虽然收集了大量个人敏感信息，但同时方便了大家的出行，维护了公共安全，这需要我们在个人隐私信息上有所让渡。同样地，汽车收集的数据，虽然也会涉及个人隐私信息，但它会提高驾驶者的人身安全和行车安全。如果要获得汽车智能化的一些功能，确实需要汽车去收集必要的数据。

根据《个人信息保护法（草案）》和相关标准规范，充分告知与授权同意是个人信息采集的基础性合规框架。具体到汽车数据的业务

场景，我们认为也必须要满足个人隐私合规的法规标准要求。因为汽车和智能手机一样，都属于个人的物品，所以汽车数据安全的重点应放在对外交互数据特别是车企云服务平台数据的安全管控上，不宜过度限制汽车数据的采集。对于《规定》的第六条（五）项中提出了“默认不收集原则”，要求“除非确有必要，每次驾驶时默认为不收集状态，驾驶人的同意授权只对本次驾驶有效”，以及在第八条（二）项中规定驾驶结束（驾驶人离开驾驶席）后本次授权自动失效等条款，这在实践中对于车主来说可能难以做到。我们建议对这些条款进行修改完善，车主只要有选择的权利即可，从而可使车主更关注于车辆安全驾驶本身。

**（3）区分车内数据和车外交互数据**

《规定》第六条（一）项提出的“车内处理原则”，除非确有必要不向车外提供个人信息和重要数据。我们认为这是非常有必要的，也是科学进行汽车数据安全治理的关键。一方面，汽车属于私人物品，必然会采集处理大量的个人隐私数据，只要这些数据在车内就没有问题；另一方面，基于安全驾驶的需要，汽车也会采集大量的环境、路况、位置和地理信息，其中可能会涉及敏感数据。如果这些数据只是在车内由行车电脑进行处理，并不对外交互，可以认为不涉及数据安全和个人隐私保护问题。因此，“车内处理原则”实质上是区分了车内数据和车外交互数据，对于车内数据，其数据权属于车主，应重点关注如何利用和安全保护；而对于车外交互数据，比如云服务平台，其数据管理权属于车企，则重点关注数据泄露风险，只有这样才能更

好地治理汽车数据，达到保障汽车数据安全的目的。

目前，行车电脑的性能已能满足相关数据安全处理的要求。关键的一部分内容是车路协同所需的车外交互数据的处理，包括车车互联、人车互联、车辆与路侧基础设施以及云服务平台的交互数据的处理。这需要区分不同的情况来将车外交互数据进行安全处理，以防止产生数据泄露和隐私侵犯等安全风险。例如，就像《规定》第六条条款所描述的，如果收集的车外行人个人信息经过了数据匿名化和脱敏处理，就无需征得其授权同意。具体而言，就要求行车电脑能够删除可识别自然人的画面或对画面中的人脸进行局部轮廓化处理，以及防止数据滥用或未经授权的第三方访问。这是车企在数据处理方面的实践中通常会采用的方法，体现了官方对此种处理方式的认可。

## 二、全周期全方位保障汽车数据安全

数智时代的到来让汽车迎来新一轮的变革，汽车智能化在带来便利的同时也极易引发数据安全问题。据英特尔公司预测，一辆联网的自动驾驶汽车每运行 8 小时将产生 4TB 的数据。这主要是因为汽车上安装了越来越多的传感器，汽车收集的数据种类和数量不断上升。在数智时代，所有的业务都将是数据驱动的，一旦敏感数据被破坏或泄露，将会造成重大经济损失或生产瘫痪。因此，需要建立起数据全生命周期保护的理念，保障数据活动在每一个环节的数据安全。

### （1）数据采集安全

汽车依赖其传感器进行数据采集，通过网络获得来自云服务平台或其他设备的交互数据。对于任何一个云服务平台来说，汽车是主要

的数据采集工具。因此，在某种程度上说，做好汽车数据采集安全，汽车数据安全就成功了大半。我们认为，汽车数据采集安全需要做到：1）在知情同意原则下进行数据采集，能够获得支撑汽车智能化发展所必须的数据；2）对采集的数据进行分类分级，至少区分车内数据和车外交互数据，并采取相对应的安全保护措施；3）对外发的车外交互数据进行匿名化、去标识化和脱敏等处理，防止敏感数据泄露；4）严禁汽车装配超出地理信息测绘精度的部件，杜绝敏感测绘数据的采集；5）严禁采集相关法律法规禁止采集的数据。

**（2）数据传输安全**

汽车数据传输主要是针对车外交互数据，这存在很多潜在的攻击入口和路径，比如车内 Wi-Fi、蓝牙和移动通信网络等，需防止数据遭到嗅探、篡改和其他攻击。因此，数据传输安全需要做到：1）对传输实体进行双向身份鉴别，确保数据被正确的对象发送和接收；2）采取加密保护措施，防止传输过程中的数据劫持，防止恶意汽车控制交互；3）建立车与人、车与车、车与路、车与云协同的攻击防御和无线通信安全防护机制；4）严禁汽车装配卫星通信部件，直接与境外服务器进行数据传输。

**（3）数据存储安全**

数据存储安全需要关注两个点：一是数据在汽车内的存储安全，二是汽车数据在云服务平台上的存储安全。对于车内数据，应该有基本的访问控制措施，防止未授权的访问，且不需要长时间保存，例如，行车安全相关的数据可以用后即删，或者根本不需要存储。而对于云

服务平台上的数据，需要有数据库安全防护和大数据平台安全防护相关措施，并在管理上满足相关法规标准要求。

**（4）数据处理安全**

汽车数据处理过程包括数据的使用和加工，应注意防范数据滥用和数据泄露问题。根据《规定》中提出的汽车数据运营者处理个人信息和重要数据应坚持 “车内处理”、“匿名化处理”、“精度范围适用”原则，大量汽车数据在加工、分析处理前应对重要数据进行脱敏，保证数据可用性和安全性的平衡，在数据处理过程中应采取适当的安全控制措施，防止数据挖掘、分析过程中有价值数据和个人信息泄露的风险。对于需要商业合作伙伴进行数据开发利用的场景，比如进行某种汽车智能化功能的开发，汽车数据运营者需审核其数据安全能力，以有效降低数据应用开发过程中因提供数据带来的数据泄露风险。

**（5）数据交换安全**

汽车数据运营者应严格控制汽车数据的交换，建议采用两种方式：1）采用隐私计算技术，在确需多方汽车数据联合计算的需求场景，通过隐私计算平台来可控、安全地交换数据的使用权，保证自己的数据不离开本地，实现“数据可用不可见”模式下的汽车数据价值挖掘；2）对必须转移或出售数据的需求场景，应严格按照相关法律规范，对数据进行去标识化、匿名化和脱敏后方可实施。同时，对数据交换过程应进行监控与审计，共享的数据不能超出数据共享使用授权范围。

**（6）数据销毁安全**

数据销毁安全体现在汽车数据存储介质上的数据销毁和云服务平台上的数据销毁两个地方。汽车应提供数据擦除功能，以支持原车主在汽车转移登记之前将所有数据清除。而对于云服务平台上的数据，云服务平台应提供数据安全清除的功能。

**（7）从“云、管、端”落实汽车数据安全保障措施**

典型的车联网结构分为“端”、“管”、“云”三层，汽车数据安全包括数据在这三个层面的安全保障。“端”主要指汽车，是属于车主的个人物品；“管”指的是“云”和“端”之间连接的网络通道，通常会通过移动通信网络进行连接；“云”则是车企建立的云服务平台，会从“端”获取汽车相关的数据，为“端”提供相关服务。从“端”、“管”、“云”三个层面，更易于看清汽车数据安全保障措施的落地。汽车在出厂时就应具备基本的数据安全防护能力，例如安全策略设置、身份鉴别、数据加密、访问控制和安全审计等功能，并可以通过行车电脑进行持续升级。同时，建议逐步增加数据分类分级、去标识化、匿名化和数据脱敏等功能，确保上传给“云”的数据不含与服务无关的个人信息。通过在汽车和“云”上装载数据加密模块，确保“管”的数据通信是受到加密保护的。“云”数据安全是大数据平台的数据安全，既需要身份鉴别、授权管理、访问控制和安全审计等基础安全功能，也需要数据库安全、数据脱敏、数据接口和数据销毁等涉及数据全生命周期安全的功能组件或模块，并要求在中国境内建立云服务平台。

## 三、加强汽车数据安全管理

除了采用上述数据安全的技术措施之外，还应该从管理角度采取措施来有效管控数据安全风险。

**（1）限制汽车驶入的场所**

就像手机不能带入涉密场所一样，应该对汽车驶入敏感场所进行严格限制，比如军事管理区、国防科工等涉及国家秘密的区域，这是最直接简单有效的管理办法，可以在数据采集源头上就根本杜绝数据非法采集和泄露的风险。

**（2）限制汽车测绘精度**

精准的自身位置定位和周边环境感知是汽车自动驾驶的基础，这涉及到对周边道路环境和地理信息的测绘，也关系到国家安全。应按照测绘地理信息相关法规标准的要求，禁止采集超出满足汽车自动驾驶功能需求的地理环境数据，严禁汽车装配超精度测绘的零部件，对涉及国家安全的地理信息数据加强监管力度。而对于非自动驾驶汽车，则无需高精度测绘定位，相关零部件的测绘指标参数应进一步降低。

**（3）管控汽车数据流动的安全风险**

《意见稿》第十六条“科研和商业合作伙伴需要查询利用境内存储的个人信息和重要数据的，运营者应当采取有效措施保证数据安全，防止流失”。这是一个典型的涉及数据安全治理的问题，即在数据的流通共享中，如何确保数据的安全，它需要的是一个科学合理的数据安全治理体系。对于车企来说，采集上来的数据需要进行利用，很多科研和商业合作伙伴将会看到和利用这些数据，全量或部分数据将会流动到这些合作伙伴中。这需要汽车数据相关的车企、零部件供应商、

应用软件提供商、网约车企业、保险公司和科研机构等，在相同的数据安全治理体系框架下运行，持续不断地提升自己的数据安全能力，才能有效管控数据流动的安全风险。建议采用基于数据安全能力成熟模型的数据安全治理体系，由专门的测评认证机构对汽车数据相关企业或组织进行数据安全能力评价，只有具备一定数据安全能力的企业或组织，才能获得相应等级的汽车数据。

**（4）对汽车数据出境严格管理**

按照《网络安全法》和《数据安全法》的要求，如《规定》第十二条明确规定的“个人信息或者重要数据应当依法在境内存储，确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估”，我们认为，汽车数据应原则上不出境。这一方面是要求所有在国内有销售的汽车品牌，其车企应该在国内建立云服务平台，数据在国内存储、分析和利用；另一方面是汽车数据出境不是行车安全和使用汽车的必要条件。只有汽车设计、行车安全、重大事故等相关的数据，在经过匿名化、去标识化和脱敏处理，以及有关部门的安全审查之后，才能出境。

**（5）严控大规模数据集的流动**

《规定》中第十七条提出“处理个人信息涉及个人信息主体超过10万人、或者处理重要数据的运营者，应当在每年十二月十五日前将年度数据安全管理情况报省级网信部门和有关部门”。这一条非常重要，通常对每一个品牌的车企来说，其云服务平台收集处理的数据都将超过百万级用户，涉及联系方式、位置、身份证号码等大量用户

隐私数据。而对车企来说，这些大规模数据集都很有可能交给科研和商业合作伙伴去处理。因此，对这些有大规模数据处理需求的云服务平台应进行严格监管，特别是要通过限制流动的数据量级来管控数据处理时的安全风险，并对其严格做好管理登记，要求数据流动所涉及的科研和商业合作伙伴应具备相应的数据安全能力。

**（6）明确汽车数据分类分级规范**

建议在交通领域数据分类分级标准规范的基础上，尽快制定汽车数据分类分级规范，针对不同类别、不同级别的汽车数据，制定针对性的收集、存储、传输和应用技术要求，确保用户信息、车辆信息、测绘地理信息等数据受到恰当的保护，其相关数据活动处于安全可控的状态。

**（7）严禁汽车装配卫星通信部件**

为防止汽车采集的数据非法跨境传输，应严禁汽车出厂装载卫星通信的零部件和软件。

**小结**

本文站在数据安全治理的视角，在数据开发利用和保障数据安全相互促进与协调发展的基础上，从技术层面和管理层面提出了保障汽车数据安全的具体方法。

# 数据安全合规：企业数据安全治理的红线

大数据协同安全技术国家工程实验室

2021 年 7 月 4 日，网信办网站通报滴滴出行 app 下线，引起社会各界巨大的反响。作为移动出行领域最大的服务提供商，滴滴通过互联网+技术引领了行业变革，彻底改变了民众的出行习惯。因为滴滴的业务涉及全国城市交通，并且收集有大量的关系到国家安全的测绘数据和公民个人信息，使得滴滴成为一家关键信息基础设施的运营者（CIIO），事件说明滴滴在海外上市的过程中没有完全符合《中华人民共和国国家安全法》《中华人民共和国网络安全法》，《中华人民共和国数据安全法》等相关法律法规要求，才导致了事件的发生。

## 一、“滴滴出行”数据安全事件背景

- 2021 年 6 月 11 日滴滴出行正式向美国证券交易委员会递交了 IPO 招股书。
- 2021 年 6 月 30 日滴滴出行低调地登录美国纳斯达克。
- 2021 年 7 月 2 日，**网络安全审查办公室**发布公告，对滴滴启动安全审查，原文如下：

*为防范国家数据安全风险，维护国家安全，保障公共利益，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对“滴滴出行”实施网络安全审查。为配合网络安全审查工作，防范风险扩大，审查期间“滴滴出行”**停止新用户注册**。*

- 2021 年 7 月 4 日，**国家互联网信息办公室**通报滴滴出行 App 下架，

原文如下：

*根据举报，经检测核实，“滴滴出行”App 存在**严重违法违规收集使用个人信息**问题。国家互联网信息办公室依据《中华人民共和国网络安全法》相关规定，通知应用商店**下架**“滴滴出行”App，要求滴滴出行科技有限公司严格按照法律要求，参照国家有关标准，认真整改存在的问题，切实保障广大用户个人信息安全。*

- 2021 年 7 月 5 日，**网络安全审查办公室**发布公告，原文如下：

*为防范国家数据安全风险，维护国家安全，保障公共利益，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对“运满满”“货车帮”“BOSS 直聘”实施网络安全审查。为配合网络安全审查工作，防范风险扩大，审查期间“运满满”“货车帮”“BOSS 直聘”**停止新用户注册**。*

- 2021 年 7 月 6 日，**中共中央办公厅、国务院办公厅**，印发了《关于依法从严打击证券违法活动的意见》的通知。
- 2021 年 7 月 8 日，Keep、喜马拉雅、零氪科技取消赴美 IPO 计划。

## 二、事件分析：上市之路

滴滴的 VIE 上市之路主要依据的是国家 1994 年发布的关于股份有限公司境外募集股份及上市的特别规定，要求境内公司向境外投资人募集股份并在境外上市时，向国务院证券主管部门报批。这一规定并未就持股或控制境内业务的境外实体海外上市做出明确规定，因此大量中概股公司得以通过在开曼群岛等地注册离岸实体发行股票。离

岸实体通过持股或协议控制，绕过中国证监会核准程序实现境内业务境外上市。新浪 2000 年通过一系列控制及利润分配协议形成的 VIE 架构，成功登陆美国资本市场，此后几乎所有海外上市的中国互联网企业都采取了这一模式。滴滴无疑也想以此模式登录纳斯达克，但是因滴滴特殊的行业属性，以及国内外的数据安全大环境的变化，导致了这次事件。

## 三、事件分析：为什么是滴滴

滴滴作为国内第一大出行平台在中国坐拥数亿活跃用户，业务范围已经渗透到各行各业，作为一家快速发展的互联网公司，滴滴近年大力投入信息化建设，通过大数据，云计算，人工智能等技术开出的 app 已经获得广大民众的认可，从产品功能的快速迭代和用户体验看，滴滴 app 产品功能涵盖面广，包括租车，代价，约车，导航等核心功能，相对国内其他平台有明显的技术优势，终端用户体量大，粘度强，几乎每个有出行需求的人都会在手机上下载并使用滴滴 app。

2017 年滴滴拿到了全国高精地图甲级测绘牌照，这意味着滴滴可以合法采集收集和处理国家地图测绘信息，这些信息包含敏感的街景信息，地理坐标信息，道路建筑信息等，这些都是非常敏感的重要信息，是关系到国家安全和社会安全的重要信息。

近年，滴滴大力拓展业务范围，把服务从 C 端拓展到了 B 端，使得滴滴可以获得更多的用户数据，包括企业和政府的用户数据和出行信息，利用大数据技术，滴滴可以帮我们快速推送目的地位置信息，

车辆信息，路况信息，但同时也可以分析终端用户行为，包括政府和企业高管的活动规律。

自 2018 年滴滴平台发生几起安全事故后，滴滴在每一个终端上都开启了视频采集和录音功能，这个功能很大程度上保证了女性乘客的安全，但对于滴滴平台来说，默认强制开启的摄像头和录音功能采集的敏感个人信息是否能确保被合理合法的使用，滴滴作为重要数据的控制者和处理者面临的不仅仅是技术挑战，而是更复杂场景的合规挑战。

另外，随着车联网，自动驾驶技术的发展，在未来智能交通的业务场景中，大数据，云计算，人工智能都需要滴滴在现有的平台上进行安全的设计，因为在滴滴的业务场景下的数据安全不仅仅关系到信息系统安全，还关系到每一个驾驶者的人身安全。

综上所述，根据滴滴出行的行业属性和《网安法》第三十一条描述 *“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，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、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定”*。滴滴的行业属性非常重要与敏感，滴滴应属于公路水路运输行业领域的关键信息基础设施的运营者。

## 四、事件分析：执法依据

滴滴出行被审查的主要依据是根据上位法《中华人民共和国国家安全法》《中华人民共和国网络安全法》，滴滴出行属于公路水路运输行业领域的关键信息基础设施的运营者。因此需要启动网络安全审查，审查的主要内容是针对其采购网络产品和服务的行为，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。而滴滴并没有在上市进程中按要求完成这些工作。

2021 年 6 月发布的《中华人民共和国数据安全法》明确了由中央国家安全领导机构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。第三十一条明确了重要数据出境安全管理制度，*“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。”*

另外，《数安法》还严格规制面向境外司法或者执法机构的数据出境活动。第三十六条规定，*“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”*。滴滴在 6 月 11 日提交 IPO 申请，且在 6 月 30 日成功上市说明滴滴一定是通过了美国证监会 SEC 的审查，按要求提交了相关数据，根据四大会计师事务所的审计准则和相关标准，审计底稿一定包括核心财务系统的相关信息以及与之相关的信息系统数

据，这些都属于关键信息基础设施的重要敏感数据，这无疑与网安法和数安法的要求不符也是最终导致滴滴违规，下线 app 事件的发生。2021 年 7 月 6 日，中共中央办公厅、国务院办公厅，印发的《关于依法从严打击证券违法活动的意见》中第十九条指出，*“加强跨境监管合作。完善数据安全、跨境数据流动、涉密信息管理等相关法律法规，压实境外上市公司信息安全主体责任”*。该意见的提出说明国家将规范海外上市公司的审批流程，滴滴无疑成为该规范执行的第一个企业。

## 五、事件总结

毋庸置疑，数据已经成为关键生产要素决定企业的发展，数据不仅仅是企业的更是国家的，人民的。数据安全在大数据时代需要在新的框架下得到安全合规的治理。企业在海外 IPO 进程中不仅要考虑传统的数据安全还要考虑数据安全的合规使用，尤其在日益复杂的数据使用场景下的国际环境下的数据交换。

数据安全治理不仅仅是技术问题，更是管理与治理的问题，企业需要自上而下的数据安全治理，高层领导者和核心业务决策者的深入参与至关重要，企业只有在合规运营的基础上结合数据安全技术与产品，才能在日趋复杂的地缘政治因素影响下顺利发展。

DSMM 作为数据安全治理的最佳实践工具可以很好地帮助企业开展数据安全治理工作，配合数据安全官 DSO 专业课程培训可以帮助企业高管了解最新的数据安全治理理念与技术方案，为企业出海保驾护航。

# 《个人信息保护法》解读

大数据协同安全技术国家工程实验室

## 一、背景

2021 年 8 月 20 日十三届全国人大常委会第三十次会议在第一项表决中批准了《中华人民共和国个人信息保护》（以下简称“个保法”）（第 91 号主席令），该法案将在 2021 年 11 月 1 日起实施。个保法将与《数据安全法》（以下简称“数安法”）和《网络安全法》（以下简称“网安法”）一起分别从不同的角度相辅相成构建出中国的网络安全法律框架。

个人信息保护法全文共 8 章 74 条，是我国首部根据宪法制定的专门规定个人信息保护的法律，它为监管机构和司法机关提供了明确的执法抓手，为企业和组织提供了落实个人信息保护责任的法律依据，明确了个人信息处理和利用的合规要求，为公民个人提供了个人信息权益保护的法律保障。

## 二、重点解读

### 解读 1：明确了个人信息、敏感个人信息的定义

（1）个人信息：以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息（第 4 条）；

（2）敏感个人信息：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（第 28 条）；

（3）匿名化信息：个人信息经过处理无法识别特定自然人且不能复原的信息（第 4，73 条）。

处理者可以根据定义对现有个人信息进行盘点，完成个人信息的分类工作，对于个人信息和敏感个人信息要实施不同严格程度的数据安全保护措施，值得注意的是匿名化信息不在个保法管控范围。

**解读 2：境外处理境内自然人个人信息的活动要遵守个保法**

（1）境外以向境内自然人提供产品或者服务为目的（第 3 条）；

（2）境外分析、评估境内自然人的行为（第 3 条）。

类似 GDPR，个保法的适用场景包括境外处理境内自然人个人信息的情况。

**解读 3：遵循个人信息收集最小原则**

（1）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 5 条）；

（2）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（第 6 条）。

杜绝应用程序（APP）过度收集个人信息的情况，应采取对个人权益影响最小的方式收集个人信息。

**解读 4：将未成年人个人信息作为敏感个人信息予以严格保护**

明确 14 岁以下未成年人个人信息属于敏感个人信息，处理该类数据时需要得到监护人的授权同意（第 15 条）。

**解读 5：个人信息的可携带权**

个人请求将其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22，45 条）。

类似 GDPR、CCPA 等国外隐私法规中规定的数据可携带权，赋予用户对个人信息更多的控制权，有利于数据流动，防止数据垄断。

**解读 6：对个人图像的管理要求**

出于维护公共安全目的，在公共场所安装图像采集、个人身份识别设备的，应显著标识以进行告知；收集的个人图像、身份识别信息不能用于除维护公共安全以外的目的，除非取得个人单独的同意（第26 条）杜绝了默认同意采集个人图像信息情况的发生，在收集个人信息的过程中，需要设计相应的隐私控制功能。

**解读 7：强调自动化决策的公平透明，避免算法歧视**

企业应保证决策的透明度和结果的公平、公正性，不得利用算法实行价格歧视等差别性待遇（第 7，17，24 条）。这一要求从立法层面禁止了“大数据杀熟”。

**解读 8：扩充个人信息出境的合法依据，限制境外司法调取个人信息**

境外司法调取境内存储的个人信息应在获得中华人民共和国主管机关批准后，处理者方能提供（第 38，41 条）。

在国内公司海外上市的过程中需要获得主管机关的批准，完成相应的网络安全审查工作。

**解读 9：完成个人信息保护影响评估**

个人信息处理者应开展“事前”的个人信息保护影响评估，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 55，56，61 条）。

履行个人信息保护职责的部门（网信，公安，政府部门等）会组织对应用程序 APP 进行个人信息保护影响评估并根据评估的结果进行处理，包括强制 APP 下架、停止注册型用户等措施。

**解读 10：明确法律责任和处罚，最大处罚金额达“五千万元或上年营业额百分之五”**

明确了个人信息处理者的法律责任和义务，个人信息处理违规行为可能会导致企业业务中断、对企业和个人同时进行财务处罚（第 66 条）。

## 三、企业的主要应对方案

首先，企业应尽快落实个人信息安全管理职责，在现有网安法，数安法的安全管理体系基础上开展个人信息安全合规工作，主要包括以下重点任务：

（1）个人信息分类分级

（2）个人信息资产盘点

（3）指定个人信息安全管理负责人

（4）开展个人信息保护影响评估

第二，对于收集个人信息的应用系统进行整改，完善用户权力的功能设计，包括以下重点内容：

知情权：对个人数据使用的用途，数据生命周期的安全保护措施有全面的了解。

删除权：对个人数据的使用时效，删除技术有全面的了解，并能决定删除。

决定权：对个人数据资产具有主体物权。

查阅复制权：对个人数据具有按需查阅和复制的权力。

转移权：对个人数据具有按需转移和复制的权力。

更正补充权：对个人数据的修改有更正和补充的权力。

第三，完善 App 应用收集个人信息的功能设计，参考个保法和《常见类型移动互联网应用程序必要个人信息范围规定》的要求对个人信息的收集范围采用最小原则重新设计并实施相应的安全保护控制措施。

数字经济时代，企业的发展可能始于数据价值，也可能止于数据泄漏。数据安全与个人信息安全是企业的命脉，只有在安全与合规的双轮驱动下，企业才能在新时期扬帆破浪，创造辉煌。

# （二）大咖观点

## 关于数据安全与隐私保护的认识

中国工程院院士 冯登国

关于数据安全与隐私保护的几点认识：一是要深刻认识大数据时代数据安全的内涵。大数据时代的数据安全不仅包括传统的可用性、机密性、完整性、不可否认性和可互性等，也包括隐私保护，不仅包括防止数据泄露的隐私保护，也包括数据分析意义下的隐私保护。二是要加强数据安全法律法规研究与制定。通过法律法规政策和管理手段规范市场、强化监管、合理平衡数据管制与自由流动，营造良好的法制环境。三是要紧跟国际数据安全技术发展趋势。应充分借鉴国际先进成果，不能闭关自守。通过交流、合作、开源等手段推动数据安全技术的发展与应用。四是要高度重视使用中的数据安全。数据的生命周期包括数据产生、采集、传输、交换、存储、分析、使用、共享、销毁等诸多环节，每个环节都面临着不同的安全威胁，需要进行全链条创新研究。五是要紧密结合产业和应用实际。我们要自主研发一批核心关键技术和产品，并能够可控利用国际上的关键核心技术和产品，推出切实可行的安全解决方案和标准规范，为保障数据开发利用和产业健康稳定发展保驾护航。

（来源：ISC 2021）

# 保护数据安全需要新一代安全能力框架

360 集团创始人、董事长 周鸿祎

传统安全无法应对数据安全新挑战，对数据安全的保护，重点应在于构建事前防护能力，而不是事后应对。数字化时代有三个明显特征，即一切皆可编程，未来所有产业、行业、生活都将架构在软件之上，我们身边的一切皆可编程；其次是万物均要互联，未来联网设备将以百亿、千亿计算，如今我们看到的所有设施、终端、设备都将变成内置类似手机的方式，万物将连接在一起；第三是大数据驱动业务，未来所有业务核心都将变成大数据平台，通过数据计算来实现对业务的判断。360 政企安全集团基于 16 年实网攻防经验和 230 亿研发投入，形成了“国家级服务能力+新战法+新一代能力框架”。 其中，国家级服务能力涵盖安全数据、算力、知识、专家、情报等多方面的网络安全技术、产品和能力；新战法是指在实践能力基础上，360 总结出一套适应数字化转型和大安全挑战的新战法：顶层设计、数据制胜、安全基建、攻防兼备、以人为本、运营为王、服务赋能、生态共建；最终，基于这套新战法，以体系化思路将安全体系与数字体系融合、攻防能力与管控能力融合，构建出真正面向数字化的新一代能力框架。

（来源：ISC 2021）

# 建立健全数据安全治理体系、提高数据安全保障能力

公安部十一局原局长、中国安全防范产品行业协会理事长 顾建国

随着数字经济的蓬勃发展，数字安全特别是数据安全摆上了更加重要的位置，这对于我们技术和产业的发展是很好的机遇，将会带来新的技术进步，新的发展空间和新的发展动力。但我们同时也应清醒地看到，面对新技术、新应用的发展和复杂的国际环境，我们将面向临更多的新挑战。这需要建立健全数据安全治理体系、提高数据安全保障能力。为此，我谈三点认识：

## 一、要坚持问题导向

目前突出问题有三个方向：一是数据主权问题，特别是从国家安全层面审视数据安全问题以及个人信息保护，重要数据保护以及如何对数据安全的风险评估、报告、信息共享、检测预警等；二是相应的法律法规和标准还没有得到很好的贯彻落实，违法违规问题还比较普遍；三是技术保障能力不强，特别是自主创新技术方面比较薄弱。需要我们在工作重点、法治建设和能力建设上形成共识，不断加强。

## 二、要坚持依法治理

随着《网络安全法》、《数据安全法》和《个人信息保护法》的陆续颁布实施，相应的一批行政法规也已发布和正在制定，已发布和正在研制的有关数据安全和个人信息保护的相应国家标准也有近30部，这些都是我们依法治理的重要基础和保障。要下大力气抓好这些法律规范的落地执行，抓好法律规范和标准的宣传贯彻，做到学法、知法、懂法、守法，坚决查处违法违规行为。

### 三、要坚持自主创新

目前，我们在数字技术方面容易被卡脖子的问题还很突出，原则性、基础性、关键性、引领性的创新十分稀缺，在不少技术领域还在邯郸学步、亦步亦趋。这是我们网络安全和数据安全最大的隐患之一，必须要下大力气改变现状，加强攻关有所突破。企业是创新的主体，要增强使命担当，努力自主创新。也希望政府有关部门加强组织协调、统筹安排，对基础性、关键性的重大项目“揭榜挂帅”，重点支持，让创新从量的积累迈向质的飞跃，从点的突破迈向系统能力提升。

（来源：ISC 2021）

## 每个企业都要有数据安全官

360 集团首席安全官、大数据协同安全技术国家工程实验室常务副主任 杜跃进

数据安全，是当前最恐慌、最混乱的新问题。传统的数据安全概念和方案已经不适用于数字经济时代的数据安全，需要新理念和新框架。技术上，要跳出传统 IT 安全的限制，从“以系统为中心”转到“以数据为中心”；管理上，要改变原来自上而下的单一模式，从特定行业的强化“管理”方式，转到面对普遍问题的多方“治理”模式，建立多方参与的数据安全治理生态；机制上，要调整只会处罚的一刀切做法，从“处罚一招鲜”，转到有处罚有激励有帮助，充分调动积极性。

数据安全不是传统数据文件保密、数据版权保护、数据库安全等，更不是大数据平台安全、云计算安全和传统网络信息系统安全，而是

大数据和智能化时代下，从不同视角关注的数据防窃取/破坏、防滥用和防误用。在此背景下，数据安全专业人员将成为保障企业或组织数据安全与依法合规的关键因素。数据安全当前最紧迫的问题是人才不足，一个组织的数据安全能力也离不开组织中人员的能力，在企业内设计数据安全岗位势在必行，国家法律也提出了相应的要求。每个企业都需要数据安全官，以提升企业数据安全整体能力，并以达到保障数据安全效果为最终目标。数据安全官相当于“数据风险的治理者”，要负责统筹规划数据安全战略目标，协调各部门共同协作进行体系化建设。

（来源：ISC 2021）

## 数据安全面临的新挑战与建议

国家信息中心首席工程师/研究员、《信息安全研究》杂志社社长 李新友

新形势下，数据安全面临新的严重挑战，一是数据确权问题。二是数据安全管理问题。三是数据跨境流动安全问题。四是数据全生命周期的安全技术问题。为此，提出以下几点建议：（1）组建国家数据管理局。适时组建国家数据管理局，统领地方大数据管理局（中心）、地方大数据产业发展局等，指导实施国家数据安全战略，研究制定数据安全重大方针政策，统筹协调网络数据安全和相关安全检查、测评、监管等工作。（2）建设“数据海关”。“数据海关”负责网络数据跨境流动的审核和安全监管，出入境数据交易的关税，打击网络数据走私，防止危及国家安全的网络数据非法出入境。（3）建设“天下

数仓”。在国家四大基础库的基础上，整合存量资源，建设“天下数仓”。（4）建设“数据交易市场”。为网络数据交易提供一个安全、公开、公平的环境。（5）建设“网络数据安全监控平台”。实时监测和有效控制重要或敏感数据全生命周期的安全状况。

（来源：ISC 2021）

## 加速推进数据分类分级保护工作

大数据协同安全技术国家工程实验室副主任 钟力

在数字经济时代，跨组织、跨平台和跨境的数据流通共享以及多方的数据协同计算将成为常态，数据安全将不再是一个企业或组织内部的事情，而是需要构建一个国家级的乃至全球的数据安全治理体系，才能有效管控数据安全风险，保障数据的安全开发利用。这其中，数据的分类分级是数据安全治理的关键性、基础性工作。《数据安全法》第二十一条明确提出国家建立数据分类分级保护制度，我认为这是抓住了数据安全治理的牛鼻子，为此特建议：

（1）在《网络安全法》和《数据安全法》指导下，尽快制定各行业、各地区的数据分类分级实施规范，明确需分类分级的数据对象、重要数据具体目录和分类分级依据等主要内容，给出可操作性强的落地操作指南，并在典型行业领域或地区进行试点示范应用。

（2）以数据流通共享和数据交易需求为牵引，进行数据对象的分割确定，在此基础上再进行该数据对象的分类分级。在工作开始能

力经验不足时避免一刀切，抓住重点，能够大幅度降低数据分类分级工作的复杂性，抓住数据开发利用的关键环节进行安全治理。

（3）建立数据分类分级指标体系，依据行业领域进行数据分类，根据数据类别、数据对象规模、敏感信息内容和重要程度等因素进行数据分级，《数据安全法》提出了重要数据、核心数据两类关键数据，可以在此基础上进一步细化。

（4）加快数据分类分级自动化支撑工具的开发应用，减少人工参与，提高工作效率。目前，不少安全厂商已发布创新的数据分类分级相关产品，使敏感数据发现、分类分级和数据质量管理得到较好的支撑，这极大地提升了数据安全治理的能力和效率。

## 《数据安全法》合规要求下的数据安全解决方案

全知科技创始人兼 CEO 方兴

《数据安全法》对监管单位、一般数据保护单位、政务数据的责任保护单位三个核心的实体提出了具体要求。从技术角度上看，监管层面最核心的是两件事，第一件是要去制定重要数据的保护目录，推进数据分类分级，落地制度的体系；第二件是监管机构要建立一整套数据风险感知体系，收集相应的数据风险，然后感知研判预警风险，并做出响应。

因此，要落地数安法，需**以数据分类分级为纲，以风险为领**，核心包括两条路径：一是在数据流转过程当中，做好数据分类分级；二

是在数据处理活动当中实施数据风险评估、数据风险监测、数据安全事件响应。（来源：ISC 2021）

## 《数据安全法》划定数据安全风险基本“红线”

国家工业信息安全发展研究中心副总工程师兼信息政策所所长 黄鹏

在第三章“数据安全制度”中，《数据安全法》明确建立数据分类分级保护制度，对关系到国家安全、国民经济命脉、重要民生、重大公共利益等数据实行更为严格的管理制度；对外国司法、执法机构调取我国数据的情况进行了规定；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活动进行国家安全审查。《数据安全法》增加了对违反国家核心数据管理制度的处罚力度，对危害国家主权、安全和发展利益的，非法向境外提供重要数据的，处以最高 1000 万元罚款。《数据安全法》对数据安全风险设置了基本“红线”，一旦数据泄露事件危及国家安全，将面临巨额罚款。

（来源：人民网）

## 《数据安全法》为全球数据安全治理贡献中国智慧和中国方案

中国信息通信研究院互联网法律研究中心主任 方禹

**作为我国数据安全领域的基础性法律，《数据安全法》主要有以下三个特点：一是坚持安全与发展并重。**设专章对支持促进数据安全与发展的措施作了规定，保护个人、组织与数据有关的权益，提升数据安全治理和数据开发利用水平，促进以数据为关键生产要素的数字

经济发展；**二是加强具体制度与整体治理框架的衔接。**从基础定义、数据安全管理、数据分类分级、重要数据出境等方面，进一步加强与《网络安全法》等法律的衔接，完善我国数据治理法律制度建设；**三是回应社会关切。**加大数据处理违法行为处罚力度，建设重要数据管理、行业自律管理、数据交易管理等制度，回应实践问题及社会关切。

（来源：中国网信网）

# （三）政策形势

## 关注1：《数据安全法》表决通过，9月1日起正式施行

关键词： 数据安全法 十三届全国人大常委会

2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议表决通过数据安全法。这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于 2021 年 9 月 1 日起施行。《数据安全法》共七章五十五条，涉及数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任等内容。

作为我国数据安全领域的基础性立法，《数据安全法》确立数据分类分级管理，数据安全审查，数据安全风险评估、监测预警和应急处置等基本制度；同时明确相关主体依法依规开展数据活动，建立健全数据安全管理制度，加强风险监测和及时处置数据安全事件等义务和责任，通过严格规范数据处理活动，切实加强数据安全保护。

同时，《数据安全法》坚持安全与发展并重，在规范数据活动的同时，对支持促进数据安全与发展的措施、推进政务数据开放利用等作出相应规定，通过促进数据依法合理有效利用，充分发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济，更好服务我国经济社会发展。

（来源：中国人大网）

## 关注2：《个人信息保护法》获通过，11月1日起施行

关键词： 个人信息保护 十三届全国人大常委会

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》。个人信息保护法自 2021 年 11 月 1 日起施行。其中明确：①通过自动化决策方式向个人进行信息推送、商业营销，应提供不针对其个人特征的选项或提供便捷的拒绝方式②处理生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息，应取得个人的单独同意③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。

（来源：新华网）

## 关注3：《关键信息基础设施安全保护条例》9月1日起施行

关键词： 关键信息基础设施保护 国务院

2021 年 8 月 17 日，国务院总理李克强日前签署国务院令，公布《关键信息基础设施安全保护条例》（以下简称《条例》），自 2021 年 9 月 1 日起施行。

《条例》建立专门保护制度，明确各方责任，提出保障促进措施，有利于进一步健全关键信息基础设施安全保护法律制度体系。

《条例》明确，重点行业和领域重要网络设施、信息系统属于关键信息基础设施，国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治违法犯罪活动。

（来源：新华社）

## 关注4：国家互联网信息办公室等五部门发布《汽车数据安全管理若干规定（试行）》

关键词： 汽车数据安全管理 个人信息保护

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《汽车数据安全管理若干规定（试行）》（以下简称《规定》），自 2021 年 10 月 1 日起施行。国家互联网信息办公室有关负责人表示，出台《规定》旨在规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用。

《规定》倡导，汽车数据处理者在开展汽车数据处理活动中坚持“车内处理”、“默认不收集”、“精度范围适用”、“脱敏处理”等数据处理原则，减少对汽车数据的无序收集和违规滥用。

《规定》明确，汽车数据处理者应当履行个人信息保护责任，充分保护个人信息安全和合法权益。开展个人信息处理活动，汽车数据处理者应当通过显著方式告知个人相关信息，取得个人同意或者符合法律、行政法规规定的其他情形。处理敏感个人信息，汽车数据处理者还应当取得个人单独同意，满足限定处理目的、提示收集状态、终止收集等具体要求或者符合法律、行政法规和强制性国家标准等其他要求。汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

（来源：中国网信网）

## 关注5：中办、国办：加强中概股监管 完善数据安全相关法律法规

关键词：数据安全 监管 跨境数据

2021 年 7 月 6 日，中共中央办公厅、国务院办公厅印发《关于依法从严打击证券违法活动的意见》。意见提出，加强中概股监管。切实采取措施做好中概股公司风险及突发情况应对，推进相关监管制度体系建设。修改国务院关于股份有限公司境外募集股份及上市的特别规定，明确境内行业主管和监管部门职责，加强跨部门监管协同。

意见提出，完善数据安全、跨境数据流动、涉密信息管理等相关法律法规。抓紧修订关于加强在境外发行证券与上市相关保密和档案管理工作的规定，压实境外上市公司信息安全主体责任。

（来源：cnbeta）

## 关注6：国家网信办等七部门进驻滴滴，开展网络安全审查

关键词：网信办 滴滴 网络安全审查 个人信息

2021 年 7 月 16 日，网络安全审查办公室有关负责同志表示，按照网络安全审查工作安排，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、市场监管总局等部门联合进驻滴滴出行科技有限公司，开展网络安全审查。

这是上市两周后，滴滴第五次出现在监管的处罚名单上。7 月 2 日，网络安全审查办公室发布公告称，对“滴滴出行”实施网络安全

审查，期间“滴滴出行”停止新用户注册。7 月 4 日，国家网信办因“滴滴出行”App 存在严重违法违规收集使用个人信息问题将其下架。7 月 9 日晚，因存在严重违法违规收集使用个人信息问题，网信办再次下架滴滴旗下 25 款应用，包括内部社交软件、车队管理软件等。

（来源：cac.gov）

## 关注7：国内数据领域首部综合性立法《深圳经济特区数据条例》正式颁布

关键词： 数据领域 深圳市七届人大常委会

2021 年 6 月 29 日，《深圳经济特区数据条例》（《条例》）获深圳市七届人大常委会第二次会议表决通过，拟自 2022 年 1 月 1 日起实施。《条例》内容涵盖了个人数据、公共数据、数据要素市场、数据安全等方面，是国内数据领域首部基础性、综合性立法。长期以来，一些 APP 过度收集个人信息、强制索要用户授权等行为令人深恶痛绝。针对这一问题，《条例》率先在立法中提出“数据权益”，明确自然人对个人数据依法享有人格权益，包括知情同意、补充更正、删除、查阅复制等权益；自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益，可以依法自主使用，取得收益，进行处分。

（来源：深圳晚报）

## 关注8：美国两州颁布法律加强网络安全和数据隐私保护

关键词： 美国 网络安全 隐私保护

康涅狄格州颁布了一项《网络安全标准法》，旨在为遵守网络安全框架的企业提供某些法律保护，规定禁止在数据泄露后对已实施“合理”安全控制的组织进行惩罚性赔偿。而科罗拉多州的一项新的数据隐私法赋予居民拒绝对个人数据的收集的权利，科罗拉多州因此与加利福尼亚州、弗吉尼亚州一起成为美国唯一拥有全面隐私措施的州。

（来源：inforisktoday.com）

## 关注9：欧盟宣布正式通过针对英国数据保护的充分性决定

关键词：欧盟 英国 数据保护

据欧盟委员会官网 6 月 28 日消息，欧盟宣布正式通过基于《通用数据保护条例》（GDPR）和《执法指令》（LED）的针对英国数据保护的充分性决定，这意味着至少未来 4 年内，个人数据可以自由地在欧盟和英国之间流动，并确保享有与欧盟法律所保证的基本相同的保护水平。相关各方认为，充分性决定将有助于维持欧盟与英国紧密的贸易联系，并且对联合开展反网络犯罪行动至关重要。

（来源：europa）

## 关注10：德国通过电信行业数据和隐私保护新法

关键词：巴西 数据保护

2021 年 5 月，德国议会通过了一项关于电信和电信媒体的数据保护和隐私的法律（简称 TTDSG），这是立法者首次将欧盟关于 Cookies 的要求从电子隐私指令中移植过来。通过该法律，德国的数

据保护规定将得到统一，并与欧盟的《通用数据保护条例》（GDPR）保持一致。不过，该法律可能会被其他欧洲法律所取代，因为欧盟当时正在就此事进行讨论的新问题，该规定将规范整个欧洲的数据保护。

（来源：EURACTIV）

# （四）安全事件

## 关注1：石油巨头沙特阿美数据泄露，面临5000万美元勒索

关键词：数据泄露 勒索攻击 石油 能源

7 月 22 日消息，世界上最有价值的石油生产商沙特阿美向 BBC 证实，公司数据已从其第三方承包商泄露。作为世界上规模最大的石油与天然气上市企业之一，这家石油巨头拥有 66000 多名员工，年收入近 2300 亿美元。

美联社报道称，勒索者掌握了 1TB 沙特阿美的专有数据，并在暗网上提出 5000 万美元的加密货币作为赎金，以换取删除数据，但尚不清楚谁是赎金阴谋的幕后黑手。沙特阿美已经将此次数据泄露归因于第三方承包商，并在采访中强调，事件本身并未对公司的日常运营造成影响。

（来源：BBC）

## 关注2：亚马逊因违反欧盟数据保护条例遭重罚8.87亿美元

关键词：GDPR 亚马逊 罚单 个人数据保护

7 月 31 日消息，根据亚马逊周五向美国证券交易委员会（SEC）提交的文件显示，因该公司欧洲核心部门对个人数据的处理不符合《欧盟通用数据保护条例》（GDPR），违反了欧盟的数据保护法，卢森堡数据保护委员会（CNPD）在 7 月 16 日对该公司开出了 7.46 亿欧元（约合 8.87 亿美元，57.29 亿元人民币）的罚单。这是欧盟有史以来最大的数据隐私泄露罚款。

此前因违反 GDPR 而被罚款最高的记录保持者是谷歌，该公司被处罚 5000 万欧元（约合 5700 万美元）。随着亚马逊此次 7.46 亿欧

元处罚事件，表明随着时间的推移，违反欧盟隐私规则的代价越来越大。

（来源：secrss.com）

## 关注3：奥迪、大众数据泄露影响 330 万客户

关键词：数据泄露 奥迪 大众 供应商

6 月 12 日消息，一家提供销售与营销服务的第三方供应商遭遇数据泄露事件，导致超过 330 万奥迪和大众汽车车主的个人信息意外流出。在提交给美国缅因州总检察长的函件中，大众汽车确认此次违规事件发生在 2019 年 8 月至 2021 年 5 月之间。

3 月 20 日，大众曾接到供应商通知，称有未经授权的人访问了数据，并可能获取了奥迪、大众和部分授权经销商的客户信息。大众表示，暴露的数据因客户而异，对于 97%以上的客户，此次事件泄露的信息包括了车主姓名、邮寄地址、邮箱或电话号码，少部分受影响较大的还泄露了购买车辆相关信息、购买凭证信息、驾照及个人身份识别信息等。

（来源：BleepingComputer）

## 关注4：全球IT咨询巨头埃森哲遭 LockBit 2.0 勒索病毒攻击

关键词：埃森哲 勒索攻击 数据泄露 LockBit

8 月 11 日消息，勒索软件团伙 Lockbit 在其数据泄露网站上发布了关于全球 IT 咨询巨头埃森哲已遭受 LockBit2.0 勒索病毒攻击的相关公告。据威胁情报公司 Cyble 称，该团伙从内网中窃取了包含超过 6TB 数据的数据库，要求在指定时间内支付 5000 万美元（约 3.2 亿人民币）的赎金，并宣称一位公司内部人员应对此次攻击负责。

随后，埃森哲发表声明称攻击未造成影响："企业环境中发现了不正常的活动。我们立即控制了事态，隔离了受影响的服务器。我们从备份中完全恢复了受影响的系统。此事未对埃森哲的运营或我们客户的系统造成影响。"Lockbit 随后开始在暗网发布 2384 个文件，表明埃森哲可能未尝试购买被盗数据，目前尚不清楚数据的敏感程度。

（来源：securityaffairs）

## 关注5：硬件厂商技嘉遭受勒索软件团伙RansomExx攻击

关键词：技嘉 勒索攻击 数据泄露 RansomExx

8 月 7 日消息，硬件厂商技嘉（Gigabyte）遭到勒索软件团伙 RansomExx 攻击。攻击者威胁称如果公司不支付赎金，将公开 112GB 的公司内部数据,其中包括技嘉和 Intel、AMD 和 American Megatrends 的机密通信。技嘉在公告中证实了此次攻击事件，但表示攻击没有对生产系统产生影响，因为攻击的目标是位于总部的少量内部服务器。

这并不是 RansomExx 团队发起的首次攻击，在 2018 年前该团队以“Defray”的名称运营，并攻击了包括佳明、宏碁、仁宝、广达和研华等公司。上个月，它还攻击了意大利和厄瓜多尔国营电信公司 CNT 的 Covid-19 疫苗接种预订系统。

（来源：cnbeta）

## 关注6：东京奥运会购票信息在网上泄露：疑似恶意软件窃取

关键词：东京奥运会 数据泄露

一位日本政府官员在 7 月 21 日表示，日本东京奥运会和残奥会购票用户、东京奥运会志愿者网站注册用户的登录账号和密码在互联网上被泄露，攻击者可据此获取购票者和志愿者的姓名、地址、银行

账户等个人信息。据透露，泄露数据疑似通过未经授权访问电脑或智能手机盗取。有专家认为，可能是恶意软件窃取。

在这起事件前，东京奥运会已遭遇过多起网络安全事件。2020年4月底，日本奥委会遭到疑似勒索软件攻击，被迫暂停业务；2021年6月初，东京奥组委受到富士通ProjectWEB系统供应链攻击事件影响，工作人员信息外泄。东京奥运会之所以特别吸引恶意攻击者的“关注”，是因为在新冠疫情的影响下，这是全球首届专门以数字平台或电视广播为载体的体育盛会。

（来源：secrss.com）

## 关注7：数据泄露后北爱尔兰暂停疫苗护照系统

关键词：数据泄露 新冠疫情 疫苗认证

在发生数据泄露事件后，北爱尔兰卫生部（DoH）暂时停止了COVID-19 疫苗接种认证在线服务。

COVIDCert系统使北爱尔兰的完全接种疫苗的个人能够获得数字证书，确认其COVID-19疫苗接种状态，类似“疫苗护照”式服务。北爱尔兰卫生部表示，由于在某些情况下，COVIDCert NI服务的一些用户可能会接触到其他用户的数据，因此暂时停止了COVIDCert在线疫苗接种认证服务。在新闻发出时，Web服务和移动应用功能都不可访问。

此外，北爱尔兰卫生部指出，某些已经申请数字证书或正在等待身份检查的个人不会受到影响。一旦恢复运营，用户可以继续正常使用服务。

（来源： bleepingcomputer）

## 关注8：美国电信巨头T-Mobile遭遇重大安全事件，超1亿用户数据泄露

关键词：电信运营商 数据泄露 基础设施

8月15日消息，美国电信巨头T-Mobile遭遇了一起重大安全事件，攻击者声称入侵了T-Mobile的生产、部署和开发服务器，窃取了多个数据库，总计106GB的数据，超过1亿用户的个人信息被泄露售卖，被盗数据包括用户的社保号码、电话号码、姓名、居住地址、国际移动电话识别码（IMEI）以及驾照信息。

威胁情报公司Hudson Rock的CTO Alon Gal表示，攻击者的这次行动是为了进行打击报复，破坏美国的基础设施。

8月20日，调查更新显示，T-Mobile已确认黑客窃取了超过5400万用户的个人数据，未来几周内，我们可能会看到受影响的T-Mobile客户不断增加。

（来源：BleepingComputer）

## 关注9：近12亿条电商用户信息被泄露，黑客非法获利34万元

关键词：数据泄露 数据爬取

河南省商丘市睢阳区人民法院公布的一起案件显示，犯罪分子通过自己开发软件爬取到了淘宝客户的数字ID、淘宝昵称、手机号码等信息近12亿条，用于从事淘宝客推广业务，共获利34万余元，最终被判处侵犯公民个人信息罪。

裁判文书显示，淘宝网安全风控员在工作中发现，在2020年7月6日到2020年7月13日之间，有黑产通过淘宝无线开放平台订单评价接口绕过平台风控批量爬取加密数据，爬取字段量巨大，平均每

天爬取数量为 500 万，爬取内容包括买家用户昵称、用户评价内容、昵称等敏感字段。爬取的客户信息被用于在微信群里进行淘宝商品的推广，从而获得淘宝网佣金和商家服务费。法院最终认为，其违反了国家规定，非法获取公民个人信息，情节特别严重，均已构成了侵犯公民个人信息罪。

（来源：sohu）

## 关注10：黑客抓取 7 亿份 LinkedIn 个人资料，并再次在线出售数据

关键词：数据泄露 数据爬取 LinkedIn

7 月 12 日消息，继领英（LinkedIn）5 亿用户信息被出售的两个月后，7 亿条领英用户信息再次出现在黑客论坛上，目前正在以未公开的价格出售，这是领英史上最大规模的数据泄露事件。

该论坛帖子的作者提供了 100 万条用户信息样本作为证明，共享的样本中包括用户全名、邮箱、电话号码、用户社交媒体账户的链接以及从 LinkedIn 个人资料中收集的各种公开可用的专业信息等。

LinkedIn 拒绝将恶意抓取视为安全问题，这可能使网络犯罪分子能够不受惩罚地收集有关新受害者的数据，大规模收集公开可用的信息仍然会使用户面临垃圾邮件和网络钓鱼攻击的风险。

（来源：securityaffairs）

**《安全观察》版块**

每周动态/政策解读/行业洞察/技术前瞻/事件分析

策略建议/国际智库精编/信创专刊/数据安全专刊/国防专刊

**总编辑：**杜跃进

**执行编辑：**韩李云 张义荣

**编委会：**张义荣 钟力 许蔓舒 闫斐 姚珊 赵旭 高昕 李晗 刘福军

**排版校对：**唐会芳 韩露荻

内部文件 如需对外使用

邮件请至 dipperresearch@360.cn