NEWSLETTER

数据合规

2019 第七期 /总第七期

数据合规时事速递

北京市环球律师事务所

2019 年 9 月 3 日

目录

前 言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。据时代的机遇与挑战。

环球律师事务所
GLOBAL LAW OFFICE

团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客据合规、个人据传输、电子律咨询及相关方案设计，帮助客户迎

孟洁
合伙人律师
直线：86-10-6584-6768

一、新规速递

1. 欧盟拟立法严格限制“滥用面部识别技术”

日前，英国《金融时报》发布报道称，欧盟委员会正考虑针对面部识别的法律法规进行修改，以避免公民受到公开监视。其中，欧盟的一名官员称，新的立法会对“滥用面部识别技术”进行限制。

委员会暂没有对计划作出任何直接的评论，但其发言人表示，今年 6 月成立了一个高级别专家组，针对包括面部识别在内的跟踪和剖析，在考虑实行新的监管。

欧洲的一些民众对面部识别技术的规范讨论并不知情，在欧洲引入了一系列的公开实验之后才对相关技术进行了讨论。

英国的数据保护监管机构针对使用人脸识别技术监控伦敦国王十字路口的人群情况进行了调查。就在不久前，瑞典国家数据保护局对一所学校处以了近 20 万瑞典克朗（约合人民币 14.6 万元）的罚款，原因是因为该所学校使用了试图监控学生每日出勤率的技术。根据欧盟去年推出的 GDPR，这种技术的使用侵犯了学生的隐私权。

该委员会即将上任的新主席 Ursula von der Leyen 表示，她计划在 11 月份担任新职位时，在其上任的前 100 天内推出新的 AI 管理法规。新的法律将会成为在欧盟地区确保人工智能和相关技术符合道德标准的使命的一部分。[1]

[1] cnBeta，《报道称欧盟希望通过新立法严格限制“滥用面部识别技术”》。

2. 关键信息基础设施安全保护条例有望年内出台

2019 年 8 月 21 日，北京网络安全大会在北京国家会议中心召开，会议称，由中央网信办和公安部共同制定的《关键信息基础设施保护条例》已上报国务院，有望年内出台。

中央网信办网络安全协调局副局长李爱东称：关键信息基础设施是经济社会的神经中枢，是网络安全的重中之重，也是容易遭到重点攻击的目标。要加快建立关键信息基础设施保护制度，加快出台关键信息基础设施安全保护条例，着眼防范有组织高强度的网络攻击，切实提升安全保障能力，保障关键信息基础设施安全、稳定、连续运行。

国家关键信息基础设施包括公共通信，广播电视、能源、金融、交通、水利、卫生、社会保障等 17 个领域。《关键信息基础设施保护条例》对有关国家安全、社会公共利益等关键信息基础设施在网络安全等级保护制度的基础上，进行更有针对性的保护。工信部印发的《电信和互联网行业提升网络数据安全保护能力专项行动方案》也对网络数据安全保障体系的建立提出了相关要求，规定了 15 项以上的行业网络数据安全标准规范。在今年 10 月底之前，要求完成重点数据安全保障体系，也需要完成对所有基础电信企业，50 家重点互联网企业以及 200 款主流 App 数据的安全检查。目前，我国逐渐提升对关键信息基础设施与影者的重视，针对信息安全的漏洞的平均修复周期已经缩短到了 16 天，在 2016 年，此周期的时间为 35 天。[2]

[2] 央视网，《关键信息基础设施安全保护条例有望年内出台：防范网络攻击 提升安全保障能力》。

3. 民法典人格权编（草案）三审：电子邮箱地址和行踪信息是个人信息

8 月 22 日上午，十三届全国人大常委会第十二次会议听取全国人大宪法和法律委员会副主任委员沈春耀作关于《民法典人格权编（草案）》修改情况的汇报

三审稿明确了人格权范围

三审稿新增规定，人格权是民事主体享有的生命权、身体权、健康权、姓名权、名称权、肖像权、名誉权、荣誉权、隐私权等权利，并将该条第一款关于民事主体人格权受法律保护的规定单列一条。

草案还完善了隐私权保护的相关规定。草案二审稿明确，本法所称隐私是具有私密性的私人空间、私人活动和私人信息等。有意见提出，对隐私的定义作进一步研究修改，突出“不愿意为他人知晓”这一特点。草案三审稿将隐私的定义修改为“自然人不愿为他人知晓的私密空间、私密活动和私密信息等”，并增加规定，任何组织或者个人不得搜查、进入、窥视、拍摄他人的宾馆房间等私密空间。

电子邮箱地址和行踪信息纳入个人信息范围

三审稿还完善了个人信息保护的相关规定。

草案二审稿规定了个人信息的范围包括自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。草案三审稿将自然人的“电子邮箱地址”和“行踪信息”纳入个人信息的范围。

同时将第六章相关条文中的“使用”个人信息修改为“处理”个人信息，并增

加规定，个人信息的处理包括个人信息的使用、加工、传输、提供、公开等。[3]

[3] 北京青年报，《民法典人格权编草案三审稿：完善个人信息保护规定》。

4. 全国信息安全标准化技术委员会发布《移动互联网应用（App）收集个人信息基本规范（草案）》

为落实《网络安全法》对个人信息保护的相关要求，加快相应标准化工作，全国信息安全标准化技术委员会秘书处组织起草了《信息安全技术移动互联网应用（App）收集个人信息基本规范（草案）》（以下简称“《基本规范》”），现面向社会公开征求意见。

该《基本规范》明确了移动互联网应用收集用户个人信息时要注意和满足的基本要求，对移动互联网应用收集个人信息的行为进行规范。

《基本规范》规定了移动互联网应用的多项义务，包括履行个人信息保护义务、不得因用户拒绝提供最少信息之外的个人信息而拒绝提供该类型服务、对外共享转让个人信息前事先征得用户明示同意、不得在用户明确拒绝使用某服务类型后频繁征求用户同意使用该类型服务等。

除了管理方面的要求之外，《基本规范》还在技术方面设置标准。App 收集个人信息应满足向用户同步明示申请权限或收集信息的目的、当收集的个人信息超出服务类型的最少信息时逐项征得用户明示同意、向用户提供实时查询已收集个人信息类型的功能等要求。

除此之外，《基本规范》还对地图导航、网络约车、即时通讯、博客论坛、网络支付、新闻资讯等 21 种常用服务类型规定了可收集的最少信息。[4]

[4] 电商网，《〈互联网应用收集个人信息基本规范〉草案发布，App 收集个人信息将有标准》。

二、监管动态

1. 十部门联合印发《加强工业互联网安全工作的指导意见》

方案背景

按照《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》（以下简称《指导意见》）部署，为加快构建工业互联网安全保障体系，提升工业互联网安全保障能力，促进工业互联网高质量发展，推动现代化经济体系建设，护航制造强国和网络强国战略实施，现就加强工业互联网安全工作提出如下意见。

总体要求

（一）指导思想

坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中全会精神，按照《指导意见》有关要求，围绕设备、控制、网络、平台、数据安全，落实企业主体责任、政府监管责任，健全制度机制、建设技术手段、促进产业发展、强化人才培育，构建责任清晰、制度健全、技术先进的工业互联网安全保障体系，覆盖工业互联网规划、建设、运行等全生命周期，形成事前防范、事中监测、事后应急能力，全面提升工业互联网创新发展安全保障能力和服务水平。

（二）基本原则

筑牢安全，保障发展。以安全保发展，以发展促安全。严格落实《中华人民共和国网络安全法》等法律法规，按照谁运营谁负责、谁主管谁负责的原则，坚持发

展与安全并重，安全和发展同步规划、同步建设、同步运行。

统筹指导，协同推进。做好顶层设计和系统谋划，结合各地实际，突出重点，分步协同推进，加快构建工业互联网安全保障体系，确保安全工作落实到位。

分类施策，分级管理。根据行业重要性、企业规模、安全风险程度等因素，对企业实施分类分级管理，集中力量指导、监管重要行业、重点企业提升工业互联网安全保障能力，夯实企业安全主体责任。

融合创新，重点突破。基于工业互联网融合发展特性，创新安全管理机制和技术手段，鼓励推动重点领域技术突破，加快安全可靠产品的创新推广应用，有效应对新型安全挑战。

（三）总体目标

到 2020 年底，工业互联网安全保障体系初步建立。制度机制方面，建立监督检查、信息共享和通报、应急处置等工业互联网安全管理制度，构建企业安全主体责任制，制定设备、平台、数据等至少 20 项亟需的工业互联网安全标准，探索构建工业互联网安全评估体系。技术手段方面，初步建成国家工业互联网安全技术保障平台、基础资源库和安全测试验证环境。产业发展方面，在汽车、电子信息、航空航天、能源等重点领域，形成至少 20 个创新实用的安全产品、解决方案的试点示范，培育若干具有核心竞争力的工业互联网安全企业。

到 2025 年，制度机制健全完善，技术手段能力显著提升，安全产业形成规模，基本建立起较为完备可靠的工业互联网安全保障体系。

主要任务

（一）推动工业互联网安全责任落实

1. 依法落实企业主体责任。工业互联网企业明确工业互联网安全责任部门和责任人，建立健全重点设备装置和系统平台联网前后的风险评估、安全审计等制度，建立安全事件报告和问责机制，加大安全投入，部署有效安全技术防护手段，保障工业互联网安全稳定运行。由网络安全事件引发的安全生产事故，按照安全生产有关法规进行处置。

2. 政府履行监督管理责任。工业和信息化部组织开展工业互联网安全相关政策制定、标准研制等综合性工作，并对装备制造、电子信息及通信等主管行业领域的工业互联网安全开展行业指导管理。地方工业和信息化主管部门指导本行政区域内应用工业互联网的工业企业的安全工作，同步推进安全产业发展，并联合应急管理部门推进工业互联网在安全生产监管中的作用；地方通信管理局监管本行政区域内标识解析系统、公共工业互联网平台等的安全工作，并在公共互联网上对联网设备、系统等进行安全监测。生态环境、卫生健康、能源、国防科技工业等部门根据各自职责，开展本行业领域工业互联网推广应用的安全指导、监管工作。

（二）构建工业互联网安全管理体系

1. 健全安全管理制度。围绕工业互联网安全监督检查、风险评估、数据保护、信息共享和通报、应急处置等方面建立健全安全管理制度和工作机制，强化对企业的安全监管。

2. 建立分类分级管理机制。建立工业互联网行业分类指导目录、企业分级指标体系，制定工业互联网行业企业分类分级指南，形成重点企业清单，强化逐级负责的政府监管模式，实施差异化管理。

3. 建立工业互联网安全标准体系。推动工业互联网设备、控制、网络（含标

识解析系统）、平台、数据等重点领域安全标准的研究制定，建设安全技术与标准试验验证环境，支持专业机构、企业积极参与相关国际标准制定，加快标准落地实施。

（三）提升企业工业互联网安全防护水平

1. 夯实设备和控制安全。督促工业企业部署针对性防护措施，加强工业生产、主机、智能终端等设备安全接入和防护，强化控制网络协议、装置装备、工业软件等安全保障，推动设备制造商、自动化集成商与安全企业加强合作，提升设备和控制系统的本质安全。

2. 提升网络设施安全。指导工业企业、基础电信企业在网络化改造及部署 IPv6、应用 5G 的过程中，落实安全标准要求并开展安全评估，部署安全设施，提升企业内外网的安全防护能力。要求标识解析系统的建设运营单位同步加强安全防护技术能力建设，确保标识解析系统的安全运行。

3. 强化平台和工业应用程序（APP）安全。要求工业互联网平台的建设、运营单位按照相关标准开展平台建设，在平台上线前进行安全评估，针对边缘层、IaaS 层（云基础设施）、平台层（工业 PaaS）、应用层（工业 SaaS）分层部署安全防护措施。建立健全工业 APP 应用前安全检测机制，强化应用过程中用户信息和数据安全保护。

（四）强化工业互联网数据安全保护能力

1. 强化企业数据安全防护能力。明确数据收集、存储、处理、转移、删除等环节安全保护要求，指导企业完善研发设计、工业生产、运维管理、平台知识机理和数字化模型等数据的防窃密、防篡改和数据备份等安全防护措施，鼓励商用密码在工业互联网数据保护工作中的应用。

2. 建立工业互联网全产业链数据安全管理体系。依据工业门类领域、数据类型、数据价值等建立工业互联网数据分级分类管理制度，开展重要数据出境安全评估和监测，完善重大工业互联网数据泄露事件触发响应机制。

（五）建设国家工业互联网安全技术手段

1. 建设国家、省、企业三级协同的工业互联网安全技术保障平台。工业和信息化部统筹建设国家工业互联网安全技术保障平台。工业基础较好的省、自治区、直辖市先期试点建设省级技术保障平台。支持鼓励机械制造、电子信息、航空航天等重点行业企业建设企业级安全平台，强化地方、企业与国家平台之间的系统对接、数据共享、业务协作，打造整体态势感知、信息共享和应急协同能力。

2. 建立工业互联网安全基础资源库。建设工业互联网资产目录库、工业协议库、安全漏洞库、恶意代码病毒库和安全威胁信息库等基础资源库，推动研制面向典型行业工业互联网安全应急处置、安全事件现场取证等工具集，加强工业互联网安全资源储备。

3. 建设工业互联网安全测试验证环境。搭建面向机械制造、电子信息、航空航天等行业的工业互联网安全攻防演练环境，测试、验证各环节存在的网络安全风险以及相应的安全防护解决方案，提升识别安全隐患、抵御安全威胁、化解安全风险的能力。

（六）加强工业互联网安全公共服务能力

1. 开展工业互联网安全评估认证。构建工业互联网设备、网络、平台、工业 APP 等的安全评估体系，依托产业联盟、行业协会等第三方机构为工业互联网企业持续开展安全能力评测评估服务，推动工业互联网安全测评机构的审核认定。

2. 提升工业互联网安全服务水平。鼓励和支持专业机构、网络安全企业等提供安全诊断评估、安全咨询、数据保护、代码检查、系统加固、云端防护等服务。鼓励基础电信企业、互联网企业、系统解决方案提供商等依托专业技术优势，加强与工业互联网企业的需求对接，输出安全保障服务。

（七）推动工业互联网安全科技创新与产业发展

1. 支持工业互联网安全科技创新。加大对工业互联网安全技术研发和成果转化的支持力度，强化标识解析系统安全、平台安全、工业控制系统安全、数据安全、5G 安全等相关核心技术研究，加强攻击防护、漏洞挖掘、态势感知等安全产品研发。支持通过众测众研等创新方式，聚集社会力量，提升漏洞隐患发现技术能力。支持专业机构、高校、企业等联合建设工业互联网安全创新中心和安全实验室。探索利用人工智能、大数据、区块链等新技术提升安全防护水平。

2. 促进工业互联网安全产业发展。充分利用国家和地方网络安全产业园（基地）等形式，整合相关行业资源，打造产学研用协同创新发展平台，形成工业互联网安全对外展示和市场服务能力，培育一批核心技术水平高、市场竞争能力强、辐射带动范围广的工业互联网安全企业。在汽车、电子信息、航空航天、能源等重点领域开展试点示范，遴选优秀安全解决方案和最佳实践，并加强应用推广。

保障措施

（一）加强组织领导，健全工作机制。在工业互联网专项工作组的统一指导下，加强统筹协调，强化部门协同、部省合作，构建各负其责、紧密配合、运转高效的工作机制。各地工业和信息化、教育、人力资源社会保障、生态环境、卫生健康、应急管理、国有资产监管、市场监管、能源、国防科技工业等主管部门及地方通信管理局要加强配合，形成合力。

（二）加大支持力度，优化创新环境。各地相关部门要结合本地工业互联网发展现状，优化政府支持机制和方式，加大对工业互联网安全的支持力度，鼓励企业技术创新和安全应用，加快建设工业互联网安全技术手段，推动安全产业集聚发展。

（三）发挥市场作用，汇聚多方力量。充分发挥市场在资源配置中的决定性作用，以工业互联网企业的安全需求为着力点，形成市场需求牵引、政府支持推动的发展局面。汇聚政产学研用多方力量，逐步建立覆盖决策研究、公共研发、标准推进、联盟论坛、人才培养等的创新支撑平台，形成支持工业互联网安全发展合力。

（四）加强宣传教育，加快人才培养。深入推进产教融合、校企合作，建立安全人才联合培养机制，培养复合型、创新型高技能人才。开展工业互联网安全宣传教育，提升企业和相关从业人员网络安全意识。开展网络安全演练、安全竞赛等，培养选拔不同层次的工业互联网安全从业人员。依托国家专业机构等，打造技术领先、业界知名的工业互联网安全高端智库。[5]

[5] 工业和信息化部。

三、相关案例

1. 普华永道因处理员工个人数据缺少合法依据受到处罚

2019 年 7 月，希腊数据保护执法机构（Hellenic Data Protection Authority, “HDPA”）对其管辖区域内的普华永道（PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS SA）公司因违反欧盟数据保护条例（General Data Protection Regulation, “GDPR”）第 5 条数据处理的基本原则和第 6 条数据处理的合法依据而遭到罚款 150000 欧元。这是欧盟数据保护机构第一次针对涉及员工数据违规行为的处罚。

案件概述

普华永道是一家国际咨询公司，在处理其员工的个人数据前，要求员工签署由公司提供的《个人数据处理同意声明》，以满足依据 GDPR 第 6 条（1）（a）项规定的处理数据的合法依据。经过调查，HDPA 认为普华永道的这一行为存在以下不合规之处：

1. 所征得的员工同意不是数据主体“自由作出的”

HDPA 认为，在雇佣关系中，由于双方的权利、地位并不平等，普华永道的员工实际上不得不签署由公司提供的《个人数据处理同意声明》，给予同意，而这违背了 GDPR 第 7 条规定的“同意须为…自由作出（freely given）”这一要求，所以，普华永道所征得的同意并不符合 GDPR 规定。

2. 违反了对员工个人数据处理的透明性

HDPA 认为，在本案中，普华永道实际依据的处理依据不是 GDPR 第 6 条第（1）（a）项的“同意”，而是第（f）项“处理对于控制者所追求的正当利益是必要的”。然而在本案中，员工从未被告知普华永道处理其数据的另一合法依据，而在普华永道地误导下，错误地认为只要他们撤回了同意，普华永道就会停止处理他们的个人数据。这违反了 GDPR 第 5 条（1）（a）项规定的处理个人数据的透明性要求，对员工的告知并不充分、清晰、全面。

3. 违反了处理个人数据的可归责性（Accountability）

HDPA 认为，普华永道作为个人信息的控制者，有责任证明其处理员工个人数据的行为符合 GDPR 第 5 条（1）款所规定的透明性等基本原则。然而，普华永道一方面违反了数据处理的透明性原则，另一方面没有保存也未能提供取得数据处理合法依据过程的记录，因此普华永道违反了 GDPR 第 5 条第（2）款规定的个人数据处理的可归责性。

基于上述原因，HDPA 要求普华永道在 3 个月内进行整改，并根据 GDPR 第 83 条的规定，向普华永道做出了 150000 欧元的行政处罚。

合规提示

自 GDPR 生效一年来，欧盟各国的数据保护机构的执法活动显然都集中在公司的业务上。因此，公司在员工的数据处理方面很少投入资源来遵守隐私保护法规的要求。HDPA 对普华永道做出的处罚决定，为公司内部如何合规地处理员工个人数据敲响了警钟，同时也为中国公司进行出海业务时，是否在公司设立初期便考虑和搭建好处理员工数据的合法路径，给予了十分具体的启示。公司在进行内部数据合规时须注意以下几点：

第一，“同意”不是获得处理所有个人数据合法依据的万灵药。在“雇主-员工”这一特殊关系下，公司仅通过征得“同意”，在实践中可能会由于双方地位不平等，而被认为并不满足 GDPR 第 7 条规定的“同意须为自由作出”这一要件，进而不能取得 GDPR 第 6 条规定的处理的合法依据。

第二，如果“同意”不能成为唯一合法性依据的情况下，公司在处理员工个人数据之前，须明确并正确识别处理的合法依据是什么，并需要将该处理的合法依据充分告知员工，以保证符合 GDPR 第 5 条规定的处理个人数据的透明性要求。

第三，在无论何种情况下，公司须对处理个人数据的各个环节做“记录”并且需要保留所有相关记录，以证明其履行了 GDPR 第 5 条规定的个人数据处理的基本原则和可归责性的要求。[6]

[6] 作者：孟洁、张淑怡，孟洁律师团队，《普华永道因处理员工个人数据缺少合法依据受到处罚》。

2. 瑞典 GDPR 处罚第一案：聚焦人脸识别技术，探讨企业合规方案

2019 年 8 月 21 日，瑞典数据保护机构对瑞典 Anderstorps 中学因违反通用数据保护条例（General Data Protection Regulation, “GDPR”）第 5 条规定的数据处理的最小必要性原则和第 6 条规定的数据处理的合法依据而判处 2 万欧元罚款。这是瑞典数据保护机构针对违反 GDPR 规定的行为做出的第一笔处罚。

案件概述

该学校位于瑞典的 Skellefteå 市，学校的工作人员在一个教室里面安装了一部人脸识别相机作为实验，以检测采用此种方式登记学生考勤是否更为迅速。该实验持续了 3 周，共影响 22 名学生。瑞典数据保护机构认为，学校采用人脸识别技术收集、处理生物可识别数据的行为违反了 GDPR 的相关规定，具体体现在以下两个方面：

1. 该学校征得的同意不是“自由作出的” 。

在该案中，学校辩称实验的进行已征得了学生及其家长的同意。但瑞典数据保护机构认为，因为学生需要在学校接受教育，因而在本案中学校与学生及其监护人实际的地位明显不平等，在此情况下学校征得的同意违背了 GDPR 第 7 条规定的“同意须为…自由作出（freely given）”这一要求。

2. 学校收集的数据类别不符合最小必要性原则。

瑞典数据保护机构认为，该学校利用人脸识别技术并收集生物性识别数据的目的是监控学生的出勤，但为实现这一目的，本可以采取其他更为保护学生个人数据的方式进行，且学校所采取的人脸识别技术和收集学生的生物性识别数据并不

是 GDPR 第 5 条第（1）（c）项要求的“为了实现数据处理目的而适当的、相关的和必要的”，故该学校的个人数据收集违反了 GDPR 所要求的最小必要性原则。

基于该案件的严重性以及涉及的生物性识别数据的敏感性，但考虑到实验进行的时间很短且涉及的学生较少，瑞典数据保护机构最终对该学校做出了约 20000 欧元的处罚。

合规提示

人脸识别技术一直是当下的热点话题，人脸识别技术的使用，为各行业带来了诸多便利。然而，伴随而之的，是它对数据主体隐私权和个人数据的侵犯，这些问题不容小觑。瑞典数据保护机构，在 GDPR 生效后 1 年多的时间，终于做出了第一笔处罚，其象征意义是极其深刻的：一方面体现了瑞典数据保护机构对涉及个人数据的新兴科技的关注，警示采用人脸技术的相关企业在进行数据收集、处理前须自行确认是否取得了正当的合法处理依据; 另一方面本案中瑞典数据保护机构在作出处罚时委婉地表示，2 万欧元的处罚是因为考虑到本案涉及人员较少、时间较短而做出的结果，暗示着该机构对未来违反 GDPR 行为的处罚力度上，不会手软。

正确使用人脸识别技术，不仅为企业降低数据合规风险，还可以赢得用户的信任。我们建议国内相关企业，在使用人脸识别技术和人的面部特征数据时，应当充分告知，保证信息收集、处理的透明性、征得用户的明示同意、开展个人信息安全评估、保障数据安全、人员与业务管理能力。

1. 充分告知，保证信息收集、处理的透明性

企业应制定并发布《隐私政策》，以清晰、明确、易懂的方式告知其使用人脸识别系统以及收集面部特征信息目的、该等信息是否会被分享和分享的第三方清

单、该等信息的保存期限、删除和去标识化手段、报告反馈问题的途径、发生重大变更的措施、拒绝自动化决策的方式等，以及个人信息主体审查其面部特征信息的方法、信息有误时如何进行更正修改等行使其权利的方法。

2. 征得用户的明示同意

不论是欧盟的 GDPR、美国的《生物信息隐私法案》还是中国的《信息安全技术个人信息安全规范》，均要求企业在收集面部特征信息前，履行告知义务并征得信息主体的授权同意。因此，企业在收集前应向个人信息主体告知收集、使用面部特征信息的目的、方式和范围，以及征得个人信息主体的明示同意(通过肯定性动作进行表示)，并确保个人信息主体的明示同意是其在完全知情的基础上给出自主的、具体的、清晰明确的意思表示。

3. 开展个人信息安全影响评估

企业在应用人脸识别技术收集面部特征信息前，应当评估使用人脸识别技术收集相应的信息是否遵循了个人信息安全基本原则，以及处理活动对个人信息主体合法权益是否会造成影响。具体而言，评估内容主要包括：

（1）个人信息收集环节是否能够遵循目的限定、选择同意、最少必要、透明性等原则；

（2）个人信息处理环节是否可能对个人信息主体的合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致歧视性差别待遇等；

（3）个人信息安全措施的有效性与可靠性，是否会进行漏洞检测、渗透性测试和病毒防护等措施；

（4）采用去标识化处理后的数据集能够重新识别出个人信息主体或与其他数据集汇聚后重新识别出个人信息主体的风险；

（5）共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响；

（6）发生安全事件时，对个人信息主体合法权益可能产生的不利影响，以及拟采取的应急预案准备情况。

4. 保障数据安全能力

企业在应用人脸识别技术，收集、处理面部特征信息时，应当保证自身的数据安全能力，并确保足以保护该等信息。企业可采取的措施包括但不限于: 收集的面部特征信息后，宜做去标识化处理；存储面部特征信息时，应采用加密和其他技术措施确保信息安全，例如将个人生物识别信息的原始信息和摘要分开存储，或仅存储摘要信息，设定访问权限；对面部特征信息的处理活动进行记录；当面部特征信息已过保存的最小期限后，建议立即对该等信息进行删除或匿名化处置。如果涉及有收集经授权的儿童脸部信息的，更应该谨慎使用，并且建议分类存储并对脸部部分位置打码处理，尽量少做主动识别动作，不做画像和精准推送。

5. 保障人员与业务管理能力

隐私和个人信息保护的概念应当贯穿企业收集和处理的全过程。企业应当任命专门的人员负责监督面部特征信息的收集和使用、培训员工相关知识并定期进行考核；同时，企业应当定期对隐私政策、相关规程和安全措施的有效性进行审计，及时处理审计过程中发现的面部特征信息违规使用、滥用等情况。[7]

[7] 作者：孟洁、张淑怡，《瑞典 GDPR 处罚第一案：聚焦人脸识别技术，探讨企业合规方案》。

3. 谷歌与 FTC 达成和解，因侵犯儿童隐私被重罚 2 亿美金

据外媒报道，Alphabet 公司旗下谷歌同意支付约 2 亿美元的和解费，以了结美国联邦贸易委员会（FTC）对其视频平台 YouTube 涉嫌违反儿童隐私法的调查，同时可能会在近期宣布和解协议。这将是有史以来，因违反了《儿童在线隐私保护条例》而被监管机构处罚的金额最大的一笔罚款，不过谷歌对此拒绝置评。

案件概述

据公开信息，谷歌推出的 YouTube Kids，这是谷歌旗下视频网站 YouTube 专门为儿童和青少年设计的应用，专注于儿童友好型内容。该网站的创建是为了给孩子们创造一个更安全的环境，让他们探索自己的兴趣和培养好奇心，同时为父母提供为孩子定制体验的工具。YouTubeKids 面向的用户群是基于三个不同年龄段，分别为：学前班、5-7 岁和 8-12 岁，家长可以从中选择适合自己孩子年龄的内容。

然而，有知情人士曾向 FTC 投诉称，YouTube 涉嫌收集未成年人的个人信息，未经父母同意就使用这些信息投放广告，违反了《儿童在线隐私保护法》（Children‘s Online Privacy Protection Act）。

事发后，部分孩子的家长对此表示不敢相信，甚至是感到愤怒。同时，FTC 对该事件表示高度重视，以涉嫌违反儿童隐私法向谷歌进行处罚，后经双方磋商达成了和解，谷歌方面同意支付 2 亿美金的罚金。

民主党参议员埃德·马基（EdMarkey）表示，“联邦贸易委员之所以会对 YouTube 进行处罚，因为它侵犯了用户的在线隐私。在这个案例里，谷歌侵犯了孩子们的个人信息，我们必须严厉打击侵犯儿童隐私的公司。”

FTC 是以 3 票赞成、2 票反对的投票结果通过了和解协议，并作为审查过程的一部分，已将该和解协议送至美国司法部。更早的时候，华盛顿邮报曾在 7 月份报道称这一和解协议已达成，但当时没有详细说明和解协议所涉及金额。

尽管这是有史以来，因违反了《儿童在线隐私保护条例》而处罚的金额最大的一笔罚款，但仍然有行业人士表示，这个处罚太轻。广告评论机构 Center for Digital Democracy 副主任凯瑟琳·柯普（Katharina Kopp）表示："考虑到谷歌违法行为的恶劣性质和从违法行为中的获利程度，结合谷歌的规模和收入情况，约 2 亿美元的罚金这个数额简直是低得可怜。"

案件启示

近年来，无论是国内还是国外，儿童数据隐私问题频发，比如日前轰动一时的 Facebook 用户数据泄漏事件，以及 Musical.ly 隐私数据的泄露等。

去年 10 月，多家儿童和消费者保护组织表示，Facebook 通过 Messenger Kids 应用非法收集儿童/少年数据。为此，美国 17 家个人隐私保护组织向 FTC 提交了投诉信，要求该机构对 Facebook 展开彻底调查。参加此次投诉的隐私权益组织包括"电子隐私信息中心"和"美国消费者联盟"等。

而今年 2 月，FTC 对音乐短视频 App Musical.ly 持续三年的调查告一段落。FTC 宣布，被调查企业 Musical.ly 同意支付 570 万美金的和解金，双方正式达成和解。Musical.ly 现在的实际运营者 TikTok 发言人表示，随着与 FTC 和解的达成，公司将在美国更大范围地推进商业化探索。这意味着在北美困扰 TikTok 一年多的 FTC 调查结束了。

当枪口对准儿童的时候，事情就变得可怕了，尽管此次谷歌被重罚 2 亿美金，

远高于 Musical.ly 的 570 万美金，但难保后面不会有此类事件的重演。[8]

[8] 雷锋网，《谷歌与 FTC 达成和解 因侵犯儿童隐私被重罚 2 亿美金》。

4. 珠海市公安局破获 50 万个人信息泄露案

今年 8 月，珠海市公安局网警支队与高新分局网安大队通过网络大数据情报研判，成功侦破一起房产中介人员私自出售业主信息的侵犯公民个人信息案。

案件概述

今年 7 月，一位房地产中介因大量出售各小区业主的相关信息，且购买者众多被群众向高新分局网安大队举报。警方在接到举报后立即展开了调查，并抓获了主要的犯罪嫌疑人赵某。经调查，赵某将其通过房地产公司工作所掌握的公民个人信息和通过其他渠道购买到的相关信息进行转卖，并从中获利。

从 2018 年年底开始，赵某就陆陆续续多次向他人出售房地产业主的信息，违法赚取相关利益。除此之外，警方根据调查的线索进行追踪，将向赵某出售业主信息的装修公司员工王某抓获。王某对其出售个人信息的行为供认不讳。

截止到目前，已有 4 名犯罪嫌疑人被警方抓获，涉及非法获取公民个人信息的数量达到 50 多万条。目前案件仍在具体的审理过程中。

近段时间以来，珠海网警自主侦办并破获大量案件，涉及网络黑客、侵犯公民个人信息、网络水军、组织考试作弊等案件 12 宗，其中被刑拘的人数达到 50 人，被逮捕的人数达到 43 人。除此之外，还协助刑侦、经侦、治安和禁毒等部门侦破涉黑，涉黄，盗窃抢劫等案件 700 多宗，抓获相关犯罪嫌疑人约 1400 人。

案件启示

刑法第二百五十三条之一：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。

根据《最高人民法院、最高人民检察院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》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。

业主的房产信息，电话和姓名等都属于其公民个人信息，房地产中介向他人提供此类信息，无论其是否从中获利，都属于违法行为。[9]

[9] 珠海网警巡查执法，《50 多万条公民个人信息泄露，是谁如此猖獗》。

5. 安徽破获跨省侵犯公民信息案，查获个人信息 1000 余万条

今年 8 月，安徽省阜阳市公安局破获一跨省侵犯公民信息案件，查获公民个人信息 1000 余万条。

2018 年 12 月初，阜阳市公安局颍泉分局接群众举报称：当地一小区内有一违法公司，非法买卖大量公民个人信息。警方成立专案组，在查清犯罪团伙的组织架构、违法犯罪事实后，进一步查明并锁定了 5 处犯罪窝点。2018 年 12 月 24 日，警方统一收网，一举抓获涉嫌侵犯公民个人信息的违法犯罪人员 49 名。

警方顺藤摸瓜，2019 年 5 月至 7 月，先后赴河北、山东等地，相继抓获杨某、朱某等 2 名非法出售采集公民个人信息软件的犯罪嫌疑人。至此，本案主要涉案成员全部落网。

经查，该犯罪团伙利用非法采集软件网上批量导出求职网站的个人信息，并通过购买、交换等方式非法获取个人姓名、电话号码等信息，再提供给阜阳多家互联网服务公司，用于业务推广，从而达到非法牟利的目的。

对此，公安机关启动“一案双查”工作机制，即在对网络违法犯罪案件开展侦查调查工作时，同步启动对涉案网络服务提供者法定网络安全义务履行情况的监督检查。经查，涉案的 5 家互联网服务公司均存在未建立健全用户信息保护制度、违规收集公民个人信息、未经被收集者同意向他人提供公民个人信息等违法行为。阜阳公安机关依法对 5 家公司进行行政处罚，并责令其关闭非法网络平台、停业整顿。[10]

[10] 新华网，《安徽破获跨省侵犯公民信息案 查获个人信息 1000 余万条》。

6. 网上贩卖上万条个人信息获刑 10 月

为挣快钱，23 岁的男青年陈某通过网上联络，当上了售卖公民个人信息的“中间商”，成为非法产业链中的一环。23 日，记者从江夏区人民检察院获悉，经该院依法提起公诉，陈某因犯侵犯公民个人信息罪被法院判处有期徒刑 10 个月，缓刑 1 年，并处罚金人民币 2 万元。

案件概述

1996 年出生的陈某还是一名在校生。2018 年 8 月，陈某在与网友聊天时得知倒卖个人信息可以赚钱。此后，陈某在上网时对此类信息格外留意，希望能够挣点快钱。当年底，陈某在一“催收”主题贴吧内结识了网友“颜如玉”，在其邀请下，陈某迅速“入坑”，开始帮助“颜如玉”从事倒卖公民个人信息的“生意”。

“颜如玉”声称能够凭姓名和身份证号从移动或联通公司获取他人手机号，只要陈某提供姓名和身份证号，通过“颜如玉”查询，再将包含手机号的公民个人信息卖出去，就能赚到差价。

面对“商机”，陈某很快在网上联系到持有大量公民身份证号和姓名的“客户”，“颜如玉”用“客户”提供的身份证号和姓名查询手机号后，以每条人民币 2.7-4 元的价格打包卖给陈某，陈某再以每条人民币 3-4.5 元的价格卖回给“客户”，从中赚取差价。

从今年 1 月至 5 月，陈某在其学校宿舍内，通过上述方式共赚得赃款人民币 15000 余元。今年 5 月 8 日 15 时许，公安机关接获线索后，在陈某宿舍内将其抓获，并从其身上查获作案工具手机 2 部。

经鉴定，陈某手机中共存有包含姓名、身份证号和电话号码信息的公民个人信息记录共计 11134 条。目前，陈某的上线“颜如玉”，以及其他参与获取、出售公民个人信息的犯罪嫌疑人还在追抓当中。

案件启示

检察官审查认为，陈某违反国家有关规定，向他人出售公民个人信息，情节严重，其行为触犯了《中华人民共和国刑法》第二百五十三条之一第一款的规定，应当以侵犯公民个人信息罪追究刑事责任。其法定刑为三年以下有期徒刑或者拘役，并处或者单处罚金。后经依法公诉，陈某被判有罪并获刑，为自己对法律的无知付出了沉重的代价。

检察官提醒，违反国家规定，出售或者非法提供、获取公民个人信息都是违法犯罪行为，必将受到法律的严惩。此外，公民个人在日常生活中要注意提高个人信息保护意识，做好相关防护措施，掌握相应的证据，在必要时及时报警以维护自身权益。[11]

[11] 武汉晨报，《“网上倒爷”卖上万条个人信息获刑 10 月》。

7. 个人简历售卖产业链曝光 国内某知名招聘公司销售员等五人获刑

8 月 30 日，北京朝阳法院对此案作出一审判决，五人因侵犯公民个人信息罪，分别被判处徒刑四至四年九个月，并处罚金人民币五万至三十万元不等。

案件概述

1. 指控丨五人买卖个人信息数十万条

淘宝店主郑某主要以售卖个人信息为营，他不单从解某处购买黄某偷来的数十万份个人简历，还从国内某知名招聘公司销售员卢某、王某处购买，后两人则是明知郑某无合法手续，还向其出售数十万条个人简历。

公诉机关指控，黄某于 2016 年 10 月至 2018 年 6 月间，非法进入国内某知名招聘公司账号内，盗取个人简历信息出售给解某，违法所得 20 余万元。解某于 2016 年 10 月至 2018 年 8 月间，将从黄某处非法获取的个人简历信息出售给郑某，违法所得 60 余万元。

2018 年 3 月至 6 月，国内某知名招聘公司上海分公司员工卢某和王某将公司企业客户账号非法出售给郑某，分别涉及个人简历信息 12 万余条和 4 万余条。此外，王某还在 2018 年 6 月至 7 月，非法出售个人简历信息给郑某，违法所得 3 万余元。

公诉机关认为，卢某、王某向他人出售公民个人信息；黄某、解某、郑某窃取或者以其他方法非法获取公民个人信息，并向他人出售公民个人信息，应当以侵犯公民个人信息罪追究五人刑事责任。

2. 庭审丨个人简历售卖链条层层加价

出生于 1982 年的郑某曾在淘宝开店卖日用品，从 2016 年开始转而买卖个人信息。

郑某在庭审时供述称，其从解某处购买了十余万份国内某知名招聘公司的个人信息，“一份是 2.5 至 5 元，看下载量，偏远地区的简历便宜点，一线城市的贵些，全国区域的就更贵些。”在淘宝出售时，郑某在每份简历的价格上加价 1 元至 1.5 元不等。

郑某称，解某自称上家是国内某知名招聘公司的内部人员，信息也是内部销售的。而据解某在庭审中的供述，他本人也只是“二道贩子”，涉案简历是其从黄某处购买的。

“区域的 2 元，一线城市 3.5 元，全国 4 元，我加五毛到一块给郑某，他支付宝给我钱。”解某在庭审中交代，他从黄某处购买了约 10 万份简历，均转卖给了郑某。

黄某手中的简历又从何处来呢？黄某自称此前从事互联网推广业，与国内某知名招聘公司并无联系。黄某发现一些企业的会员名在网上公开，自己便尝试破解密码，最终取得了 200 多个账号。

在这个链条中还有“售后服务”。黄某卖给解某的账户中约有 20%不能用，出现这种情况他便会退款给解某，再由解某退款给郑某。

3. 国内某知名招聘公司员工协助造假 批量出售简历

2018 年，郑某经朋友介绍结识了在国内某知名招聘公司从事招聘工作的卢某和王某，开始从二人处购买简历。“他们有便宜的套餐，一份简历 4.5 元，一个账号 2800 份简历。”郑某称。

但按照国内某知名招聘公司的正常信息销售流程，企业需要与国内某知名招聘公司签订正式合同，待审批生效后再以企业账号的形式获得信息。

卢某称，郑某自称是猎头公司的，需要大量简历。于是卢某通过公司内部获取了超过 60 个企业名称，还协助郑某用 PS 伪造虚假的企业营业执照蒙混过关。郑某将钱款转至卢某的个人微信或支付宝账户，再由卢某转至公司的银行账户。

当公诉人当庭询问其做法是否符合国内某知名招聘公司制度要求时，卢某称，“领导跟我说客户给钱就行”。但他同时称自己并未从中获益。

而另一位国内某知名招聘公司的销售员王某则称，其在一开始并不知道郑某营业执照的假的，“我到后来才知道是他 PS 的”。面对公诉人“你提供企业名称，郑某就提供营业执照”是否符合常理的疑问，王某称其未考虑太多。

4. 判决|侵犯公民个人信息罪 情节严重

经过 5 月 6 日和 7 月 5 日两次开庭审理，2019 年 8 月 30 日，朝阳法院对此案作出一审判决。

法院认为，黄某违反国家有关规定，窃取公民个人信息并出售；解某违反国家有关规定，非法出售公民个人信息；卢某、王某身为国内某知名招聘公司职员，将在履行职责或提供服务过程中获得的公民个人信息非法出售给他人；被告人郑某违反国家有关规定，长期通过多人非法购买公民个人信息并利用互联网进行转卖。

法院认为，上述五人均属情节特别严重，触犯了刑法，构成侵犯公民个人信息罪，分别判处五人有期徒刑四至四年九个月，并处罚金人民币 5 万元至 30 万元不

等，同时，追缴其违法所得的钱款。[12]

[12] 北京青年报，《个人简历售卖产业链曝光 国内某知名招聘公司销售员等五人获刑》。

四、环球解读

1. 新规解读——《儿童个人信息网络保护规定》

经两个多月征求意见，国家互联网信息办公室对《儿童个人信息网络保护规定（征求意见稿）》（以下简称“《征求意见稿》”）进行了部分修改，于 2019 年 8 月 23 日正式发布了《儿童个人信息网络保护规定》（以下简称“《正式稿》”），《正式稿》将在 10 月 1 日生效。

六大重要修改

除调整体例和统一措辞外，相较于《征求意见稿》，《正式稿》有六大重要修改

1. 禁止侵害儿童信息安全

《正式稿》新增了第四条，规定任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。此条款从内容上对儿童个人信息进行了保护。

2. 增加监护人义务

《征求意见稿》仅规定了企业的责任和义务，并鼓励互联网行业加强行业自律，履行社会责任。《正式稿》新增了监护人的义务，要求监护人正确履行监护职责，教育并引导儿童增强个人信息保护的能力和意识。这意味着在儿童个人信息保护方面，需要运营者、互联网行业以及监护人的共同努力，仅靠一方是远远不够的。

3. 降低监护人表达同意的难度

根据《征求意见稿》，在收集使用儿童个人信息时，应当征得监护人“明示同意”，

《正式稿》则删除了“明示”二字，降低了监护人表达同意的难度。根据《个人信息安全规范》，“明示”是指通过书面主动声明或自主作出肯定性动作，肯定性动作包括主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”、主动填写或提供等。而此次《正式稿》则删除了“明示”二字，意味着同意隐私政策的方式即代表授权同意，不需要通过额外的肯定性动作表明同意。实际上可能也是一定程度上想避免通过过多收集信息来验证谁是家长谁是儿童，因为这确实是一个难题，有待于继续探讨和研究。也有可能需要与后面会生效的《数据安全管理办法（征求意见稿）》的思路和表述保持一致。但是不要求监护人通过明示授权，是否会对未成年人的个人信息保护造成影响，可能这也是 case by case 的问题。

此外，《征求意见稿》第十四条规定，与第三方共同使用儿童个人信息的，应当征得监护人的明示同意。《正式稿》并未提及此条。《征求意见稿》第十五条要求，在向第三方转移儿童个人信息时，应当进行安全评估并征得监护人的明示同意。而《正式稿》仅要求进行安全评估。

4. 删除同意的例外

根据《征求意见稿》，在收集、使用、转移、披露儿童个人信息时，不需要经过监护人明示同意的三种情况包括：维护国家安全或公共利益；为消除儿童人身或者财产上的紧急危险；法律法规规定的其他情形。此次《正式稿》删除了此条内容。

5. 增加监管主体

此次《正式稿》还将监管部门由原来的国家互联网信息办公室变更为了网信部门。这表明地方网信部门也将负责儿童个人信息相关问题的监管工作。

6. 扩大罚则依据

《征求意见稿》在行政罚则部分仅引述了《网络安全法》第六十四条。而《正式稿》对罚则的依据进行了增加，删除了第六十四条的引述。这意味着，一旦违反《正式稿》的规定，则可能面临《网络安全法》第六章（第五十九条到第七十五条）的罚则以及《互联网信息服务管理办法》等相关法律法规的罚则。《正式稿》第四条规定，企业不得制作、发布、传播侵害儿童个人信息安全的信息。而《互联网信息服务管理办法》第十五条第九款则设置了兜底条款，规定互联网信息服务提供者不得制作、复制、发布、传播含有法律法规禁止内容的信息。根据《互联网信息服务管理办法》第二十条，一旦企业制作、复制、发布、传播第十五条所列内容之一的信息，可能会受到相应的处罚。这就意味着，企业如制作、发布、传播侵害儿童个人信息安全的信息，监管部门可能会根据《互联网信息服务管理办法》第二十条的规定，对经营性互联网信息服务提供者处以责令停业整顿至吊销经营许可证的处罚，或对非经营性互联网信息服务提供者处以责令暂时关闭网站至关闭网站的处罚。

除上述六大主要变更外，《正式稿》还新增了第二十八条，即通过计算机系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，依照其他有关规定执行。

其他重点规范

尽管有上述六大重要变化，在其他条款上，《正式稿》沿袭了《征求意见稿》的相关内容，未做出实质性变化，建议企业重点关注并提前准备，包括《正式稿》第八条、第十三条、第十五条以及第十七条。

1. 专门的规则和专门的负责人

第八条要求网络运营者设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。《征求意见稿》第五条规定，适用于儿童的用户协议应当简洁、易懂，《正式稿》并未提及此项要求，但保留了设置专门的个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护的要求。从这一点上讲，对于儿童专属类产品，根据《正式稿》要求，需要起草单独的隐私政策和用户协议。但是，对于可能会收集儿童个人信息的全年龄段产品，企业可以根据自身实际情况，考虑制定专门的儿童隐私政策和用户协议。《正式稿》第十条还增加了隐私政策中应当包括的内容，即更正、删除儿童个人信息的途径和方法，这也是需要在起草隐私政策时需要特别注意的内容。

另外，《正式稿》还要求设置专人负责儿童个人信息保护，删除了“个人信息保护专员”的表述，可能是考虑到企业的成本，目前要求的是有专人负责儿童个人信息保护工作，企业可视情况自主决定是否设置“专员”这一岗位。

2. 存储的技术措施

第十三条要求在存储儿童个人信息时采取技术措施。企业可参考《个人信息安全规范》中关于保存个人信息或个人敏感信息的要求，规范内部制度，例如，在传输和存储时进行加密处理，在收集后进行去标识化处理，或将儿童个人信息与非儿童个人信息分开存储等。

3. 严格的访问和审批

根据第十五条，网络运营者应当严格设定访问儿童个人信息的权限；工作人员访问儿童个人信息的，应当经儿童个人信息保护负责人或其授权人员审批，并进行记录。这与《个人信息安全规范》的要求基本一致。《正式稿》生效后，其效力层级比《个人信息安全规范》更高。因此，建议相关企业尽快建立内部制度：（1）严

格控制对儿童个人信息的访问，对访问儿童个人信息的员工设立权限，使其只能访问职责所需的最少够用的信息；（2）设立相应的审批机制；（3）对访问情况及时记录，防止无权限的员工越权访问和复制儿童个人信息。

4. 安全评估

根据第十七条，在转移儿童个人信息时，网络运营者可自行或委托第三方机构进行安全评估。此处的安全评估可参考个人信息安全影响评估的规则。在相关企业有足够能力支持的情况下，可自行进行安全评估；如需要，可委托律师事务所等第三方机构协助开展安全评估。[13]

[13] 作者：孟洁、殷坤、张淑仪， 孟洁律师团队，《【新规】<儿童个人信息网络保护规定>正式发布》。

2. 儿童个人信息保护实证调研篇（一）

2019 年 8 月 23 日，国家互联网信息办公室正式发布《儿童个人信息网络保护规定》（以下简称“《规定》”），我们团队也对该《规定》的各重要条款和与征求意见稿有变化的条款进行了第一时间的解读，请详见【新规】《儿童个人信息网络保护规定》正式发布。其中，《规定》第九条、第十条和第十四条第一款规定了收集、使用儿童信息必须经过监护人同意制度，并在第五条规定了监护人应当履行监护职责的义务。但对于如何落地实施监护人同意，是企业更为关心的问题，也是难题所在。故本文章将挑选国外较为典型的儿童产品实践，尝试为企业提供相应的参考。

注册阶段识别儿童身份

由于 App 运营商在用户下载时无法得知下载者的年龄是否属于受特殊保护的儿童，故用户的身份判断主要通过注册或使用时输入出生年份的方式验证。如果出生年份所对应的年龄在受保护儿童给的范围之内，App 一般采取以下两种方式：（i）禁止操作者的后续操作；或（ii）要求操作者输入监护人的邮箱，要求监护人代替儿童进行后续操作。以下将分别进行说明、举例。

1. 禁止操作者的后续操作

采取此种方式的 App 有 Facebook、Spotify 等 App。通常的做法是，在创建账户时首先为用户提供选择出生日期的选项，当用户选择的年份对应的年龄为 13 岁或其他相应法域规定的年龄线以下时，则提示“不满足年龄要求”并无法进行下一步操作。

2. 要求操作者输入监护人的联系方式，要求监护人进行后续操作

采取此种方式的 App 有 BBC iPlayer、Youtube Kids 等 App。根据对 BBC iPlayer 的调研，在注册时用户首先需要选择年龄是 13 岁以下还是以上，如果选择在十三岁以下，则要求提供监护人的邮箱，然后由监护人根据邮箱提示进行操作。在监护人邮箱受到特定邮件后，由监护人进行相应操作。

如何征得监护人同意

就如何征得监护人同意而言，在调研范围内的产品中，主流的方式有两种，包括：在产品界面展示监护人同意书、为监护人发送邮件征得同意。

1. 在产品界面展示监护人同意书

在用户登录账户后并为儿童创建简历前，Youtube Kids 会通过向用户展示完整的监护人同意书，来征求监护人同意。监护人同意书的内容包括收集的信息类型、如何使用、如何分享、监护人如何控制儿童信息或撤回同意，并通过最终再次输入账户密码的方式表示已阅读隐私政策并授予监护人同意。

2. 通过监护人邮箱征得监护人同意

根据对 BBC iPlayer 的调研，监护人填写邮箱后，会收到一封用于验证的邮件。在填写儿童的相关信息时，系统会逐项告知填写的各项信息收集的目的，如果监护人填写了相关信息并点击“继续”，则视为已征求监护人的同意。

如何保障监护人控制

经调研，针对使用环节的个别功能，例如设置、充值等，App 通常也会要求验证监护人身份，防止儿童错误操作，保障监护人能够控制儿童的使用。此时验证监护人的方式一般包括：请监护人进行数学运算、根据提示识别相应的小写字母、完

成特定手势等。而 App 可能会在多个功能方面实现监护人控制：（1）向监护人提供访问、更改、删除儿童个人信息的方式；（2）控制可能被收集的儿童个人信息类型；以及（3）控制儿童可观看内容。

1. 向监护人提供访问、更改、删除儿童个人信息的方式

根据调研，在访问、更改、删除儿童个人信息方面，目前 App 的验证模式大体相同，均要求通过特定验证方式，保证操作者为监护人而非儿童。以 Youtube Kids 为例，当用户点击页面的设置并通过数学计算验证年龄，则可以看到儿童的个人信息页面，如需访问儿童个人信息，则要求再次输入账户密码，输入密码后方可实现对儿童个人信息的访问、更改、删除等操作。根据调研，相似的验证监护人的方式还包括根据提示识别相应的小写字母、完成特定手势等。

2. 控制可能被收集的儿童个人信息类型

BBC iPlayer 在注册阶段便要求监护人为选择儿童可以使用的产品功能，包括个性化推送、评论、上传功能、通知功能，在源头上为监护人提供相应的渠道和方式，实现控制可能被收集儿童个人信息的效果。

3. 控制儿童可观看内容

从内容保护和防沉迷的角度，Youtube Kids 还从观看内容和观看时间两个角度加强对儿童的保护。例如，在监护人为儿童创建角色之后，要求监护人根据儿童的年龄选择儿童可以观看的视频范围，或者针对某一视频采取屏蔽的措施。

同时，Youtube Kids 还为监护人提供了控制儿童观看时间的功能，从而有效地控制儿童使用 App 的时间，起到防沉迷的作用。

结语

《儿童个人信息网络保护规定》虽然经历二个月征求意见后已经正式发布，但就具体的“同意”实施方式，还需要配套可落地的相关标准。企业可以借鉴国外相关实践，以破只是简单点击隐私政策就代表了是由监护人陪同阅读并同意的“假命题”。毕竟国内外隐私保护的环境与基础不同，在国内，我们更需要各方予以关注和思考，尽快设计出一套行之有效，既保护到儿童的个人信息不被滥收集，真正是由家长起到监督管理作用，又能够管住企业不因验证儿童与家长的年龄而多收集个人信息主体的个人信息，这确实需要进一步在实践中进行回答。[14]

[14] 作者：孟洁、殷坤、张淑怡，孟洁律师团队，《儿童个人信息保护实证调研篇（一）》。

中国首家律师事务所

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

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987