立方律師

NEWSLETTER

LIFANG & PARTNERS 立方观评

关注更多精彩内容

No.122

2020.03

立方网络安全与数据合规周报

Weekly Cybersecurity and Data Protection Review

国内要闻 Domestic News

海外动态 Overseas News

国内要闻 Domestic News

《信息安全技术个人信息安全规范》等8项信息网络安全标准发布

2020年3月6日，国家市场监督管理总局（**“市场监管总局”**）和国家标准化管理委员会（**“国标委”**）联合发布了《中华人民共和国国家标准公告》（2020年第1号），据此发布了包括《信息安全技术 个人信息安全规范》等8项涉及信息网络安全的标准。8项标准中，2项为更新标准，6项为新标准，均将于2020年10月1日起正式实施。

本次发布的8项标准具体为：（查看更多）

标准编号	标准名称	实施时间
GB/T17901.1-2020	信息技术 安全技术 密钥管理 第1部分：框架	2020.10.1
GB/T35273-2020	信息安全技术 个人信息安全规范	2020.10.1
GB/T38540-2020	信息安全技术 安全电子签章密码技术规范	2020.10.1
GB/T38541-2020	信息安全技术 电子文件密码应用指南	2020.10.1
GB/T38542-2020	信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架	2020.10.1
GB/T38556-2020	信息安全技术 动态口令密码应用技术规范	2020.10.1
GB/T38558-2020	信息安全技术 办公设备安全测试方法	2020.10.1
GB/T38561-2020	信息安全技术 网络安全管理支撑系统	2020.10.1

SAMR and SAC Jointly Release 8 Standards on Personal Information and Cybersecurity

On March 6, 2020, the State Administration for Market Regulation (“**SAMR**”) and the Standardization Administration of the P.R.C (“**SAC**”) jointly released the *National Standard Announcement (2020 No.1)* (“***Announcement***”) , by which, eight standards in connection with personal information and cybersecurity were released. Among the eight standards, two are revised standards and six are new ones. All standards will come into force on October 1, 2020.

The eight standards are listed as follows: (More)

No.	Title	Effective Time
GB/T17901.1-2020	Information Technology—Security Technology—Cipher Management, Part 1: Framework	2020.10.1
GB/T35273-2020	Information Security Technology—Personal Information Security Specification	2020.10.1
GB/T38540-2020	Information Security Technology—Secure Electronic Signature Password Technical Specifications	2020.10.1
GB/T38541-2020	Information Security Technology—Guidelines of Electronic Documents Password Application	2020.10.1
GB/T38542-2020	Information Security Technology—Technical Framework of Identification of Mobile Intelligent Terminal Based on Biometrics	2020.10.1
GB/T38556-2020	Information Security Technology—Dynamic Cipher Application Technical Specifications	2020.10.1
GB/T38558-2020	Information Security Technology—Testing Method of Office Equipment Safety	2020.10.1
GB/T38561-2020	Information Security Technology—Support System of Network Security Management	2020.10.1

工信部发布《工业数据分类分级指南（试行）》

2020年3月4日，工业和信息化部（**“工信部”**）办公厅发布《工业数据分类分级指南（试行）》（**“《指南》”**）。《指南》适用于工业和信息化主管部门、工业企业、平台企业等开展工业数据分类分级工作，规定工业企业、工业互联网平台企业等作为工业数据的所有者和使用者，承担开展数据分类、加强数据管理等主体责任。《指南》按照每类工业数据遭篡改、破坏、泄露或非法利用后可能带来的潜在影响，将数据划分为三个级别，规定企业应结合行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行类别梳理，形成分类清单。（查看更多）

MIIT Publishes the *Guidelines for Classification and Grading of Industrial Data (For Trial Implementation)*

On March 4, 2020, the Ministry of Industry and Information Technology of China (“**MIIT**”) published the *Guidelines for Classification and Grading of Industrial Data (For Trial Implementation)* (“***Guideline***”). The *Guideline* is applicable to the competent departments of MIIT, industrial enterprises and platform companies. As the owner and user of industrial data, industrial enterprises and industrial internet platform enterprises shall undertake primary responsibilities to classify industrial data and strengthen data management. In addition, the *Guideline* classifies industrial data into three grades, in terms of potential impacts of tampering, destruction, disclosure or illegal use of the data. Enterprises, as required under the *Guideline,* shall sort out industrial data and form a classification list based on the actual situation of industry requirements, business scale, data complexity, etc. (More)

《网络信息内容生态治理规定》3月1日生效

2020年3月1日起，国家互联网信息办公室（“**网信办**”）发布的《网络信息内容生态治理规定》（“**《网信内容规定》**”）正式实施。

《网信内容规定》对网络信息内容生产者、网络信息内容服务平台、及网络信息内容服务使用者及网络行业组织四类主体的行为进行了规范，将网络信息内容分为鼓励类、限制类和禁止类。进一步明确了网络信息内容服务平台的内容管理主体责任，要求平台建立网络信息内容生态治理机制，制定账号管理、信息发布审核、应急处置和网络谣言等信息处置等制度。要求网络信息内容服务使用者通过发帖、回复、留言、弹幕等形式参与网络活动时应遵守网络信息内容分类的要求。（查看更多）

The *Provisions on the Ecological Governance of Network Information Contents* Come into Force on March 1

On March 1, 2020, the *Provisions on the Ecological Governance of Network Information Contents* (“***Provisions***”) released by the Cyberspace Administration of China (“**CAC**”) came into force.

The *Provisions* regulates the behaviors of four groups of subjects involved in processing network information contents, i.e. the information producers, service platforms, users of service platforms, and network industrial organizations. It classifies network information contents into three types, which are encouraged, restricted, or prohibited. In addition, service platform’s responsibilities are further clarified that it shall establish a mechanism for ecological governance of network information contents, formulate detailed rules for account management, information release review, emergency response, and disposal of network rumors, etc. Users of network information content services shall conform their behavior in accordance with the requirements of the *Provisions*, and express themselves rationally when participating in network activities by way of posting, sending, replying messages and participating bullet screen comments, etc. (More)

《信息安全技术网络安全等级保护实施指南》等27项信息网络安全规范与标准3月1日起实施

2020年3月1日，市场监管总局和国标委共同发布的27项信息网络安全规范与标准正式实施。包括了网络安全等级保护、网络存储安全技术、个人信息去标识化等网络安全与数据保护的重要领域。

本次实施的27项信息网络安全规范与标准如下：（查看更多）

标准编号	标准名称
GB/T 20272-2019	信息安全技术 操作系统安全技术要求
GB/T 25058-2019	信息安全技术 网络安全等级保护实施指南
GB/T 37962-2019	信息安全技术 工业控制系统产品信息安全通用评估准则
GB/T 21050-2019	信息安全技术 网络交换机安全技术要求
GB/T 20009-2019	信息安全技术 数据库管理系统安全评估准则
GB/T 18018-2019	信息安全技术 路由器安全技术要求
GB/T 20979-2019	信息安全技术 虹膜识别系统技术要求
GB/T 37971-2019	信息安全技术 智慧城市安全体系框架
GB/T 37973-2019	信息安全技术 大数据安全管理指南
GB/T 20273-2019	信息安全技术 数据库理系统安全技术要求
GB/T37980-2019	信息安全技术 工业控制系统安全检查指南
GB/T 37931-2019	信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法
GB/T 37934-2019	信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求
GB/T 37932-2019	信息安全技术 数据交易服务安全要求
GB/T 37933-2019	信息安全技术 工业控制系统专用防火墙技术要求
GB/T 37988-2019	信息安全技术 数据安全能力成熟度模型
GB/T 37972-2019	信息安全技术 云计算服务运行监框架
GB/T 37935-2019	信息安全技术 可信计算规范 可信软件基
GB/T 37941-2019	信息安全技术 工业控制系统网络审计产品安全技术要求
GB/T 37939-2019	信息安全技术 网络存储安全技术要求
GB/T 37964-2019	信息安全技术 个人信息去标识化指南
GB/T 37950-2019	信息安全技术 桌面云安全技术要求
GB/T 37954-2019	信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法
GB/T 37952-2019	信息安全技术 移动终端安全管理平台技术要求
GB/T 37953-2019	信息安全技术 工业控制网络监测安全技术要求及测试评价方法
GB/T 37955-2019	信息安全技术 数控网络安全技术要求
GB/T 37956-2019	信息安全技术 网站安全云防护平台技术要求

27 Specifications and Standards on Information and Cyberspace Security Come into Force on March 1

On March 1, 2020, 27 specifications and standards on information and cybersecurity security jointly released by the SAMR and SAC came into force, which covered several important cybersecurity and data protection fields, including classified protection of cybersecurity, network storage and de-identifying personal information, etc.

The 27 specifications and standards are listed as follows: (More)

No.	Title
GB/T 20272-2019	Information security technology—Security technical requirements for operating system
GB/T 25058-2019	Information security technology—Implementation guide for classified protection of cybersecurity
GB/T 37962-2019	Information security technology—Common criteria for industrial control system products security
GB/T 21050-2019	Information security technology—Security requirements for network switch
GB/T 20009-2019	Information security technology—Security evaluation criteria for database management system
GB/T 18018-2019	Information security technology—Technical requirement for router security
GB/T 20979-2019	Information security technology—Technical requirements for iris recognition system
GB/T 37971-2019	Information security technology—Framework of smart city security system
GB/T 37973-2019	Information security technology—Big data security management guide
GB/T 20273-2019	Information security technology—Security technical requirements for database management system
GB/T37980-2019	Information security technology—Guide for security inspection of industrial control systems
GB/T 37931-2019	Information security technology—Security technology requirements and testing and evaluation approaches for Web application security detection system
GB/T 37934-2019	Information security technology—Security technical requirements of industrial control system security isolation and information ferry system
GB/T 37932-2019	Information security technology—Security requirements for data transaction service
GB/T 37933-2019	Information security technology—Technical requirements of industrial control system dedicated firewall
GB/T 37988-2019	Information security technology—Data security capability maturity model
GB/T 37972-2019	Information security technology—Operation supervision framework of cloud computing service
GB/T 37935-2019	Information security technology—Trusted computing specification—Trusted software base
GB/T 37941-2019	Information security technology—Security technical requirements of industrial control system network audit products
GB/T 37939-2019	Information security technology—Security techniques requirement for network storage
GB/T 37964-2019	Information security technology—Guide for de-identifying personal information
GB/T 37950-2019	Information security technology—Security technical requirements for desktop cloud
GB/T 37954-2019	Information security technology—Technique requirements and testing and evaluation approaches for industrial control system vulnerability detection products
GB/T 37952-2019	Information security technology—Technical requirements of mobile terminal security management platform
GB/T 37953-2019	Information security technology—Security requirements and evaluation approaches for industrial control network monitor
GB/T 37955-2019	Information security technology—Security technique requirements for numerical control network
GB/T 37956-2019	Information security technology—Technology requirement for website security cloud protection platform

中国信通院发布《“互联网+行业”个人信息保护研究报告（2020年）》

2020年3月，中国信息通信研究院（“**中国信通院**”）发布了《“互联网+行业”个人信息保护研究报告（2020年）》（“**《报告》**”）。该《报告》研究了“互联网+”服务收集、使用个人信息的范围和特点，梳理归纳了当前国内个人信息保护法规和监管现状并对当前面临的问题和挑战进行剖析，从立法完善、政府治理、企业自治、行业自律等方面对个人信息保护提出建议。（查看更多）

CAICT Publishes the *Report of 2020 on Personal Information Protection in “Internet + Industry”*

In Early March, 2020, the China Academy of Information and Communications Technology (“**CAICT**”) published the *Report of 2020 on Personal Information Protection in “Internet + Industry”* (“***Report***”). The *Report* conducted detailed researches on the ranges and patterns for collecting and using of personal information by “Internet + Industry” services and summarized the existing legislations on the protection and supervision of personal information in China and analyzed nowadays problems and challenges. The *Report* also provides several advices on personal information protection, from the perspectives of legislation improvement, government action and participants self-discipline. (More)

安徽2月份依法关闭12家违法违规网站和4个公众账号

2020年3月3日，网信办发布新闻称，2020年2月，安徽省网信办会同省通信管理局，依法关停12家违法违规网站，协调有关平台依照其用户服务协议关闭4个违法违规公众账号。关停原因主要涉及发布涉新冠肺炎疫情不实信息、传播违法信息，发布误导网民的虚假政务信息、破坏网上舆论生态等。（查看更多）

Anhui Shuts Down 12 Websites and 4 Public Accounts in February

On March 3, 2020, the CAC announced on its website that the Anhui CAC and the Communications Administration of Anhui Province jointly shut down 12 websites and 4 public internet accounts in accordance with relevant laws and platforms’ user services agreements. The shutting down was caused by the account owners’ release of false information relating to the outbreak of Covid-19 coronavirus, the spread of illegal information, the publication of misleading false governmental information and the disruption of internet ecology. (More)

海外动态 Overseas News

国泰航空因客户数据泄露被英数据监管机构处罚50万英镑

2020年3月4日，英国信息专员办公室（Information Commissioner’s Office，“**ICO**”）发布新闻称，因国泰航空公司的乘客数据意外泄露，对其处以50万英镑的罚款。据悉，2014年10月至2018年5月期间，国泰航空的计算机系统缺乏适当的安全措施，导致全球约 940万客户的个人信息被泄露，包括乘客姓名、护照号、出生日期、电子邮件地址、电话号码、以及旅行历史等敏

感信息。ICO调查称国泰航空的系统被植入了恶意数据收集软件，并发现其系统在安全性方面的不足，包括未进行密码保护的备份文件、未打补丁的Web服务器、不再由开发者更新的操作系统和缺乏防病毒保护等。鉴于案件发生时间，根据英国1998年《数据保护法》该案最终被处以最高额50万英镑的罚款。（查看更多）

Cathay Pacific Airways Fined GBP 500,000 for the Leakage of Customer's Personal Data

On March 4, 2020, the Information Commissioner's Office ("**ICO**") fined Cathay Pacific Airways Limited GBP 500,000 for failing to protect the security of its customers' personal data. Between October 2014 and May 2018, Cathay Pacific's computer systems lacked appropriate security measures which led to 9.4 million worldwide customers' personal information being exposed, including customers' names, passport and identity details, dates of birth, postal and email addresses, phone numbers and historical travel information. The ICO found Cathay Pacific's systems were entered via a server connected to the internet and malware was installed to harvest data. A catalogue of errors was found during the ICO's investigation including back-up files that were not password protected; unpatched internet-facing servers; use of operating systems that were no longer supported by the developer and inadequate anti-virus protection. Due to the timing of these incidents the ICO investigated this case under the *Data Protection Act 1998*, a maximum financial penalty was imposed upon Cathay Pacific. (More)

荷兰皇家网球协会因违法出售数据被荷兰数据保护局处以52.5万欧元罚款

2020年3月3日，荷兰数据保护局（Dutch Data Protection Authority，"**DDPA**"）依据《通用数据保护条例》（General Data Protection Regulation，"**GDPR**"）第五章和第六章的规定，对荷兰皇家网球协会违法出售数据的行为处罚52.5万欧元。据悉，荷兰皇家网球协会将会员的姓名、性别、地址等个人信息未经所有人许可的情况下出售给具有利益关系的第三方机构。DDPA认为出售个人信息数据的行为是没有法律依据的。（查看更多）

KNLTB Fined EUR 525,000 for Selling Personal Data

On March 3, 2020, the Dutch Data Protection Authority fined the Royal Dutch Tennis Association ("**KNLTB**") with EUR 525,000 for selling the personal data of more than 350,000 of its members to third parties in accordance with Article 5 and Article 6 of *General Data Protection Regulation* ("***GDPR***"). It was found that the KNLTB sold personal data such as name, gender and address to third parties without obtaining the consent of the data subjects. The data protection authority also rejected the existence of a legitimate interest for the sale of the data and therefore decided that there was no legal basis for the transfer of the personal data to third parties. (More)

立方律师事务所编写《立方观评》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

This Newsletter has been prepared for clients and professional associates of Lifang & Partners. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

Subscribe to our WeChat community

扫码关注公众号“立方律师事务所”和“竞争法视界”

北京 ｜ 上海 ｜ 武汉 ｜ 广州 ｜ 深圳 ｜ 韩国

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

www.lifanglaw.com
Email：info@lifanglaw.com

Tel：+8610 64096099
Fax：+8610 64096260/64096261