LIFANG & PARTNERS
立 方 律 师 事 务 所

Data and AI Compliance Review

数据与人工智能合规观察月刊

No.3

Data and AI Compliance Review by Lifang & Partners

立方数据与人工智能合规观察月刊

2026. 11

No.3

目录

Domestic News 境内动态.....1

➢ Regulations Update 新规速递 1

Central Cyberspace Affairs Commission Issues the *National Informatization Plan for the 15th Five-Year Plan Period* 1

中央网信委发布《国家信息化“十五五”规划》 1

MIIT Issues the *Requirements for Automotive Data Security (Draft for Comment)* 2

工信部发布《汽车数据安全要求（征求意见稿）》 2

Ministry of Commerce and Ministry of Science and Technology Solicit Public Comments on the Revision of the *Catalogue of Technologies Prohibited or Restricted from Export in China* 3

商务部、科技部就修订《中国禁止出口限制出口技术目录》公开征求意见.....3

Central Committee of the Communist Party of China and the State Council issued the *Opinions on Developing New Quality Productive Forces* 4

中共中央、国务院印发《关于发展新质生产力的意见》 4

Department of Tourism, Culture, Radio, Television and Sports of Hainan Province Issues the *Guidelines on the Security of Cross-Border Data Transfers of Hainan Tourism, Culture, Radio, Television and Sports Data (Trial)* 5

海南省旅游和文化广电体育厅印发《海南旅文广体数据出境安全指引（试行）》 5

Shanghai Cyberspace Administration and Shanghai Municipal Data Bureau Issue *Several Measures on Promoting High-Level Opening Up and Facilitating Cross-Border Data Flows* 6

上海市网信办、上海市数据局发布《上海市推动高水平对外开放 促进数据跨境流动便利化的若干举措》.....6

➢ Regulatory Actions 监管行动.....7

Quality Supervision and Inspection Center for Computer Information System Security Products of the Ministry of Public Security Detects 35 Mobile Applications That Illegally Collect and Use Personal Information ..7

公安部计算机信息系统安全产品质量监督检验中心检测发现 35 款违法违规收集使用个人信息的移动应用.....7

CAC Carries Out the Determination of Internet Platform Service Providers with a Huge Number of Minor Users or with Significant Influence on the Minor Population 8

国家网信办开展未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定工作.....8

MIIT Reports 17 Apps (SDKs) with Acts Infringing Upon Users' Rights and Interests 9

工信部通报 17 款存在侵害用户权益行为的 App（SDK）.....9

Shanghai Cyberspace Administration Reports SDKs with Issues Concerning the Collection and Use of Personal Information.....10

上海市网信办通报存在个人信息收集使用问题的 SDK.....10

Hunan Cyberspace Administration Conducts Centralized Interviews with Four Large Model Operation Enterprises 10

湖南省网信办集中约谈四家大模型运营企业.....11

Overseas News 境外动态.....11

➢ Regulations Update 新规速递 11

EU: EDPS Publishes FAQ on Data Breach Notification.....11

欧盟：EDPS 发布数据泄露通知常见问题解答.....12

EU: Council Agrees Position on Simplifying Data Protection, Privacy, and Cyber Reporting Rules.....13

欧盟：欧盟理事会就简化数据保护、隐私与网络报告规则达成立场..14

Canada: Privacy Commissioner of Canada Launches the *Children's Privacy Code* 14

加拿大：加拿大隐私专员发布《儿童隐私守则》.....15

EU: EDPB Adopts Statement on the Data Protection Challenges of Smart Glasses 15
欧盟：EDPB 通过智能眼镜数据保护挑战声明 16

➢ Regulatory Actions 监管行动.....16

UK: ICO Secures Data Protection Improvements from Ten AI Developers and Launches Call for Evidence on Agentic AI 16
英国：ICO 促使十家 AI 开发商作出数据保护改进并就代理式 AI 征求意见.....17
Italy: Garante Fines IQVIA €7 Million for Unlawfully Processing Patients' Health Information.....17
意大利：Garante 因非法处理患者健康信息对 IQVIA 处以 700 万欧元罚款.....18

Domestic News 境内动态

➢ Regulations Update 新规速递

Central Cyberspace Affairs Commission Issues the *National Informatization Plan for the 15th Five-Year Plan Period*

On 23 October 2026, the Central Cyberspace Affairs Commission (Commission) issued the *National Informatization Plan for the 15th Five-Year Plan Period* (Plan). The Plan states that it is necessary to improve the agile governance mechanism for artificial intelligence and strengthen the development of the cryptographic protection system for artificial intelligence. It is necessary to optimize the filing mechanism for generative artificial intelligence, establish a security risk assessment system for the application of AI in key fields, and improve the assessment and filing of new forms such as AI agents, on-device large models, and anthropomorphic interactive services. It is necessary to advance the research, development and application of large model-based vulnerability discovery and protection technologies, strengthen the prevention of cybersecurity risks for satellite internet, and enhance the capability to respond to security risks of intelligent connected vehicles. The Plan clarifies that it is necessary to strengthen the classified and graded management of data in key industries, deepen the application of technologies such as blockchain and privacy-preserving computing in data circulation and trading, and strengthen cryptographic protection of data security. It is necessary to promote and regulate the cross-border flow of data, and efficiently implement systems such as data export security assessment, the standard contract for the cross-border transfer of personal information, and personal information protection certification. It is necessary to promote the national public service for online identity authentication, facilitate the interoperability and mutual recognition of distributed digital identities, strengthen the testing and assessment of personal information protection of smart devices, and reinforce the technical application management of biometric information. (More)

中央网信委发布《国家信息化“十五五”规划》

2026年10月23日，中央网络安全和信息化委员会（以下简称“中央网信委”）发布了《国家信息化“十五五”规划》（以下简称《规划》）。《规划》指出，要健全人工智能敏捷治理机制，加强人工智能密码防护体系建设。优化生成式

人工智能备案机制，建立重点领域应用安全风险评估制度，完善智能体、端侧大模型、拟人化互动服务等新形态的评估备案。推进基于大模型的漏洞挖掘与防护技术研发应用。加强卫星互联网网络安全风险防范。增强智能网联汽车安全风险应对能力。《规划》明确，要加强重点行业数据分类分级管理，深化区块链、隐私保护计算等技术在数据流通交易中的应用，强化数据安全密码保护。促进和规范数据跨境流动，高效实施数据出境安全评估、个人信息出境标准合同、个人信息出境认证等制度。推广国家网络身份认证公共服务。促进分布式数字身份互通互认应用。加强智能设备个人信息保护检测评估，强化生物特征信息的技术应用管理。（查看更多）

MIIT Issues the *Requirements for Automotive Data Security (Draft for Comment)*

On 20 October 2026, the Ministry of Industry and Information Technology (MIIT) issued the mandatory national standard *Requirements for Automotive Data Security (Draft for Comment)* (Requirements) for public comment, with the deadline for feedback being 19 December 2026. The Requirements prescribe the safeguards, basic requirements, technical requirements, and same-type determination for automotive data security, and describe the corresponding inspection and test methods. The Requirements apply to M-category and N-category vehicles, and do not apply to special purpose vehicles modified from type-2 chassis or complete vehicles that have already obtained type approval. The Requirements clarify that a vehicle shall not refuse to provide functions that do not require the processing of personal information or that can be realized only by processing the vehicle identification number within the vehicle - such as starting, braking, the wiper system, and light control - on the grounds that the personal information subject does not consent to the collection of his or her personal information or withdraws consent. The Requirements state that a vehicle shall not directly transmit data overseas, except for user-initiated behaviors such as users accessing overseas websites through browsers, sending messages to overseas parties through communication software, and installing third-party applications on their own initiative that may lead to the cross-border transfer of data. (More)

工信部发布《汽车数据安全要求（征求意见稿）》

2026 年 10 月 20 日，工信部发布了强制性国家标准《汽车数据安全要求（征求意见稿）》（以下简称《要求》），向社会公开征求意见，意见反馈截止时间为 2026 年 12 月 19 日。《要求》规定了汽车数据安全保障要求、基本要求、技

术要求及同一型式判定，描述了相应检验与试验方法。《要求》适用于 M 类及 N 类车辆，不适用于基于已获得型式批准的二类底盘或整车改装的专用汽车。《要求》明确，车辆不应以个人信息主体不同意收集其个人信息或撤回同意为由，拒不提供不需处理个人信息或仅在车内处理车辆识别代号即可实现的功能，如启动、制动、雨刮系统、车灯控制等功能。《要求》指出，车辆不应直接向境外传输数据，但用户使用浏览器访问境外网站、使用通信软件向境外传递消息、自主安装可能导致数据出境的第三方应用等用户自主行为除外。（查看更多）

Ministry of Commerce and Ministry of Science and Technology Solicit Public Comments on the Revision of the *Catalogue of Technologies Prohibited or Restricted from Export in China*

On 16 October 2026, the Ministry of Commerce and the Ministry of Science and Technology solicited public comments on the revision of the *Catalogue of Technologies Prohibited or Restricted from Export in China* (Catalogue), with the deadline for feedback being 15 November 2026. The revision of the Catalogue involves 40 technologies in three fields: artificial intelligence, biomedicine, and photovoltaics. The artificial intelligence field includes 23 technologies related to large models, AI agents, computing power clusters, and information processing, which are distinguished between prohibited export technologies and restricted export technologies according to different control points. Technologies that have entered the public domain through means such as open source or publication of academic papers are not included within the scope of management. Before the Catalogue is formally revised and implemented, technology export operators shall register on the relevant platform of the Ministry of Commerce before exporting technologies listed in the Catalogue. Exports that have been commenced but not yet completed fall within the scope of registration. (More)

商务部、科技部就修订《中国禁止出口限制出口技术目录》公开征求意见

2026 年 10 月 16 日，商务部、科技部就修订《中国禁止出口限制出口技术目录》（以下简称《目录》）向社会公开征求意见，意见反馈截止时间为 2026 年 11 月 15 日。《目录》的修订涉及人工智能、生物医药、光伏三个领域 40 项技术。人工智能领域包括大模型、智能体、算力集群、信息处理相关 23 项技术，根据不同的控制要点区分禁止出口技术和限制出口技术。已通过开源、发表学术论文等方式进入公共领域的技术，不纳入管理范围。在《目录》正式修订并实施前，

技术出口经营者在出口《目录》所列技术前，应当在商务部相关平台进行登记。已经开始但尚未完成的出口，在登记范围内。（查看更多）

Central Committee of the Communist Party of China and the State Council issued the *Opinions on Developing New Quality Productive Forces*

On 9 October 2026, the Central Committee of the Communist Party of China and the State Council issued the *Opinions on Developing New Quality Productive Forces* (Opinions). The main contents include but are not limited to: (1) Promoting the deep integration of the real economy and the digital economy: improving the systems for the determination of data property rights attribution, market trading, distribution of rights and interests, and protection of interests; implementing pilot and demonstration projects related to data factors; and fully unleashing the potential of data factors. (2) Comprehensively implementing the "Artificial Intelligence Plus" action: advancing the transformation of traditional industries by artificial intelligence, and accelerating the scenario-based application of a new generation of smart terminals such as intelligent connected new energy vehicles, AI-enabled mobile phones and computers, and humanoid robots. (3) Improving the market regulation system: strengthening governance in fields such as artificial intelligence and biology; intensifying cross-departmental joint supervision, innovating supervision methods, reducing the number of on-site inspections, and exploring a supervision model of "decision-making with data and management with data." (4) Allocating advanced production factors globally: establishing an efficient, convenient, and secure mechanism for cross-border data flows. (More)

中共中央、国务院印发《关于发展新质生产力的意见》

2026 年 10 月 9 日，中共中央、国务院印发了《关于发展新质生产力的意见》（以下简称《意见》），主要内容包括但不限于：（1）促进实体经济和数字经济深度融合：健全数据产权归属认定、市场交易、权益分配、利益保护制度，实施数据要素相关试点示范工程，充分释放数据要素潜能。（2）全面实施“人工智能+”行动：推进人工智能对传统产业的改造，加快推进智能网联新能源汽车、人工智能手机和电脑、人形机器人等新一代智能终端场景应用。（3）完善市场监管制度：加强人工智能、生物等领域治理。强化跨部门联合监管，创新监管方式，减少现场监管次数，探索“用数据决策、用数据管理”监管模式。

（4）在全球配置先进生产要素：建立高效便利安全的数据跨境流动机制。（查看更多）

Department of Tourism, Culture, Radio, Television and Sports of Hainan Province Issues the *Guidelines on the Security of Cross-Border Data Transfers of Hainan Tourism, Culture, Radio, Television and Sports Data (Trial)*

On 21 October 2026, the Department of Tourism, Culture, Radio, Television and Sports of Hainan Province issued the *Guidelines on the Security of Cross-Border Data Transfers of Hainan Tourism, Culture, Radio, Television and Sports Data (Trial)* (Guidelines), which shall take effect from the date of issuance and remain valid for two years. Tourism, culture, radio, television and sports data processors (organizations or individuals engaged in data processing activities in the fields of tourism, culture, radio, television and sports within the administrative area of Hainan Province) shall conduct cross-border data transfer activities in accordance with the Guidelines. Hainan tourism, culture, radio, television and sports data as referred to in the Guidelines means data generated and collected in the course of providing tourism, culture, radio, television and sports services in the Hainan Free Trade Port, including personal data and important data. The Guidelines clarify that the circumstances under which a data processor may be exempted from filing a data export security assessment, filing the standard contract for the cross-border transfer of personal information, or obtaining personal information protection certification include but are not limited to: (1) personal data falling outside the scope specified under "IV. Tourism" of the Data Export Administration List (Negative List) of the Hainan Free Trade Port; (2) where, due to the needs of outbound tourism, culture, radio, television and sports project development, marketing, academic research cooperation and other activities, a data processor needs to provide Hainan tourism, culture, radio, television and sports data overseas that does not contain personal data or important data; and (3) where, as a party to a transaction, an individual, within the administrative area of Hainan Province, genuinely needs to provide personal information overseas for activities such as outbound tourism or participation in international sports events and cultural and artistic performances, for example, flight and hotel booking, visa application, and cross-border shopping. (More)

海南省旅游和文化广电体育厅印发《海南旅文广体数据出境安全指引（试行）》

2026 年 10 月 21 日，海南省旅游和文化广电体育厅发布了《海南旅文广体数据出境安全指引（试行）》（以下简称《指引》），自发布之日起施行，有效期两年。旅文广体数据处理者（在海南省行政区域内从事旅游、文化、广电、体育领域数据处理活动的组织或个人）按照《指引》引开展数据出境活动。《指引》所称的海南旅文广体数据是指海南自由贸易港旅游和文化、广电、体育服务过程中所产生、收集的数据，包括个人数据和重要数据。《指引》明确，可免予申报数据出境安全评估、个人信息出境标准合同备案、个人信息保护认证的情形包括但不限于：（1）海南自由贸易港数据出境管理清单（负面清单）中“四、旅游”规定范围以外的个人信息数据的；（2）因出境旅文广体项目开发、市场营销、学术研究合作等活动需要，数据处理者需要向境外提供海南旅文广体数据，不包含个人信息或者重要数据的；（3）个人作为一方当事人，在海南省行政区域内为出境旅游或者参加国际体育赛事、文艺表演等活动，确实需要向境外提供个人信息的，如：机票酒店预订、签证办理、跨境购物等。（查看更多）

Shanghai Cyberspace Administration and Shanghai Municipal Data Bureau Issue *Several Measures on Promoting High-Level Opening Up and Facilitating Cross-Border Data Flows*

On 16 October 2026, the Shanghai Cyberspace Administration and the Shanghai Municipal Data Bureau publicly issued the *Several Measures of Shanghai Municipality on Promoting High-Level Opening Up and Facilitating Cross-Border Data Flows*, proposing ten measures, including: (1) Strengthening the implementation and alignment of the systems for data export; (2) Deepening the negative list management model for data export; (3) Improving the management measures and operational guidelines for data export; (4) Innovating the mechanism of convenient online services; (5) Enhancing the service capability for cross-border data transfers; (6) Empowering cross-border data application scenarios in key industries; (7) Improving the infrastructure for cross-border data flows; (8) Supporting market platforms in serving cross-border data flows; (9) Cultivating a full-chain service ecosystem for cross-border data transfers; and (10) Promoting regional dialogue and standards cooperation on cross-border data flows. (More)

上海市网信办、上海市数据局发布《上海市推动高水平对外开放 促进数据跨境流动便利化的若干举措》

2026 年 10 月 16 日，上海市网信办、上海市数据局公开发布了《上海市推动高水平对外开放 促进数据跨境流动便利化的若干举措》，提出了十项举措，包括：（1）强化数据出境制度衔接落地；（2）深化数据出境负面清单管理模式；（3）完善数据出境操作指引管理举措；（4）创新线上便捷服务机制；（5）提升数据跨境服务能级；（6）赋能重点产业数据跨境应用场景；（7）完善数据跨境流动基础设施；（8）支持市场平台服务数据跨境流动；（9）培育数据跨境全链条服务生态；（10）推动数据跨境区域对话和标准合作。（查看更多）

➢ Regulatory Actions 监管行动

Quality Supervision and Inspection Center for Computer Information System Security Products of the Ministry of Public Security Detects 35 Mobile Applications That Illegally Collect and Use Personal Information

On 30 October 2026, the Quality Supervision and Inspection Center for Computer Information System Security Products of the Ministry of Public Security detected 35 mobile applications that illegally collect and use personal information. The issues identified include: (1) Collecting and using personal information without the use's consent. (2) Failing to completely and accurately inform users of the collection and use of personal information, or the stated purposes, methods, and scope of the collection and use of personal information being inconsistent with the actual collection and use. (3) Failing to specify the categories, purposes, and methods of providing personal information to third parties, as well as the names and contact information of the recipients. (4) Failing to inform users of the purposes at the same time when applying to open permissions that may collect personal information or applying to collect users' personal sensitive information such as user profiles. (5) Forcing users to consent to the collection of non-necessary personal information. (6) Collecting and using personal information beyond the necessary scope, collecting personal information such as location, contacts, and SMS messages in unrelated scenarios. (7) Failing to provide an effective function for users to cancel their accounts. (8) Failing to provide users with convenient channels to exercise their rights such as correcting, deleting, and refusing to process personal information, with the relevant functions being incomplete and unsound. (More)

公安部计算机信息系统安全产品质量监督检验中心检测发现 35 款违法违规收集使用个人信息的移动应用

2026 年 10 月 30 日，公安部计算机信息系统安全产品质量监督检验中心检测发现了 35 款违法违规收集使用个人信息的移动应用，所涉问题包括：（1）未经用户同意收集使用个人信息；（2）未完整准确告知收集使用个人信息情况，或告知收集使用个人信息目的、方式、范围与实际收集使用情况不一致。（3）未列明向第三方提供个人信息的种类、目的、方式以及接收方的名称、联系方式。（4）在申请打开可收集个人信息的权限或申请收集用户等个人敏感信息时，未同步告知用户其目的。（5）强制用户同意收集非必要个人信息。（6）超出必要范围收集使用个人信息，在无关场景收集位置、通讯录、短信等个人信息。（7）未提供有效注销用户账号功能。（8）未向用户提供行使更正、删除、拒绝处理个人信息等权利的便捷渠道，相关功能不完善不健全。（查看更多）

CAC Carries Out the Determination of Internet Platform Service Providers with a Huge Number of Minor Users or with Significant Influence on the Minor Population

On 19 October 2026, the Cyberspace Administration of China (CAC) announced that it would carry out the determination of internet platform service providers with a huge number of minor users or with significant influence on the minor population, and concurrently issued relevant work guidelines. The work guidelines clarify that internet platform service providers shall, in accordance with the *Measures for the Determination of Internet Platform Service Providers with a Huge Number of Minor Users or with Significant Influence on the Minor Population*, determine whether they fall within the category of internet platform service providers with a huge number of minor users or internet platform service providers with significant influence on the minor population. Where the corresponding conditions are met, the internet platform service provider shall proactively and promptly submit its determination application materials, by way of delivering written materials accompanied by an electronic version, within 20 working days from the date of issuance of the notice. The work guidelines prescribe the application materials to be submitted by internet platform service providers and the requirements for such application materials. (More)

国家网信办开展未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定工作

2026 年 10 月 19 日，国家网信办宣布开展开展未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定工作，并同步发布相关工作

指南。工作指南明确，网络平台服务提供者根据《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法》判断其是否属于未成年人用户数量巨大的网络平台服务提供者或对未成年人群体具有显著影响的网络平台服务提供者；若符合相应条件，网络平台服务提供者应当主动、及时在通知发布之日起 20 个工作日内，通过送达书面材料并附带电子版的方式提交认定申报材料。工作指南对网络平台服务提供者应提交的申报材料、申报材料的要求作出了规定。（查看更多）

MIIT Reports 17 Apps (SDKs) with Acts Infringing Upon Users' Rights and Interests

On 15 October 2026, following spot checks organized with third-party testing institutions, the MIIT reported 17 Apps (SDKs) with acts infringing upon users' rights and interests. The issues identified include: (1) information windows that cannot be closed; (2) random redirection upon clicking information windows; (3) redirection upon sliding information windows; (4) illegal collection of personal information; (5) collection of personal information beyond the permitted scope; (6) illegal use of personal information; (7) inadequate disclosure of SDK information; (8) Apps frequently self-starting and associated-starting; (9) Apps forcibly, frequently, and excessively requesting permissions; (10) forcing users to use targeted push notification functions; and (11) inadequate display of App information on application distribution platforms. The aforementioned Apps (SDKs) shall carry out rectification in accordance with the relevant provisions. Where rectification is not properly implemented, the MIIT will, in accordance with laws and regulations, organize and carry out relevant disposition work. (More)

工信部通报 17 款存在侵害用户权益行为的 App（SDK）

2026 年 10 月 15 日，经组织第三方检测机构进行抽查，工信部通报了 17 款存在侵害用户权益行为的 App（SDK），所涉问题包括：（1）信息窗口无法关闭；（2）信息窗口点击乱跳转；（3）信息窗口滑动跳转；（4）违规收集个人信息；（5）超范围收集个人信息；（5）违规使用个人信息；（6）SDK 信息公示不到位；（7）App 频繁自启动和关联启动；（8）App 强制、频繁、过度索取权限；（9）强制用户使用定向推送功能；（10）应用分发平台上的 App 信息明示不到位。所涉 App（SDK）应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。（查看更多）

Shanghai Cyberspace Administration Reports SDKs with Issues Concerning the Collection and Use of Personal Information

On 10 October 2026, the Shanghai Cyberspace Administration reported local Apps with issues concerning the collection and use of personal information. The issues identified include: (1) the stated purposes, methods, and scope of the collection and use of personal information being inconsistent with the actual collection and use; (2) continuing to collect personal information after the user has explicitly expressed non-consent; (3) failing to provide an opt-out function for personalized push notifications; (4) collecting and using personal information beyond the necessary scope; and (5) the committed time limit for responding to complaints and reports exceeding the statutory ceiling. The relevant operators shall complete rectification within 15 working days from the date of issuance of the report, and report the rectification status to the Shanghai Cyberspace Administration, which will, together with the relevant departments, carry out verification and, in light of the rectification status, conduct disposition and penalties in accordance with laws and regulations. (More)

上海市网信办通报存在个人信息收集使用问题的 SDK

2026 年 10 月 10 日，上海市网信办通报了存在个人信息收集使用问题的属地 App，所涉问题包括：（1）告知收集使用个人信息目的、方式、范围与实际收集使用情况不一致；（2）用户明确表示不同意后仍收集个人信息；（3）未提供个性化推送退出功能；（4）超出必要范围收集使用个人信息；（5）承诺的投诉、举报反馈时限超法定上限。相关运营者应当于通报发布之日起的 15 个工作日内完成整改，并将整改情况报上海市网信办，其将会同有关部门进行核查，并结合整改情况依法依规开展处置处罚。（查看更多）

Hunan Cyberspace Administration Conducts Centralized Interviews with Four Large Model Operation Enterprises

On 9 October 2026, the Hunan Cyberspace Administration issued an announcement stating that, in response to the failure of certain large model operation entities to fully perform their responsibilities, it had conducted centralized interviews with four large model operation enterprises within Hunan Province. The interviews pointed out that the interviewed enterprises failed to comprehensively fulfill their primary responsibilities, with weak links in the algorithm design of large models, training data management, and the security prevention and control of generated content, and that their technical

measures for cybersecurity and data security were not properly implemented, posing hidden risks such as information content security, AI attacks, and data poisoning. In response to the issues identified, the Hunan Cyberspace Administration put forward clear rectification requirements: (1) Comprehensively investigate vulnerabilities and hidden dangers, focusing on the three dimensions of institutions, technology, and management, sort out the weak links one by one, establish a problem ledger, and achieve closed-loop rectification. (2) Improve the security prevention and control system, upgrade technical capabilities such as AI content identification, risk interception, and anomaly monitoring, and carry out routine self-inspection and self-correction of risks. (3) Operate strictly in compliance with laws and regulations, complete the procedures for the filing of generative artificial intelligence services and algorithm filing in accordance with the law, standardize service operation practices, and ensure complete qualifications and standardized operations. (More)

湖南省网信办集中约谈四家大模型运营企业

2026 年 10 月 9 日，湖南省网信办发布公告称，其针对部分大模型运营主体履责不到位问题，集中约谈了四家湖南省内大模型运营企业。约谈指出，被约谈企业未能全面履行主体责任，在大模型算法设计、训练数据管理、生成内容安全防控等方面存在薄弱环节，网络安全、数据安全技术措施落实不到位，存在信息内容安全、AI 攻击、数据投毒等风险隐患。针对发现的问题，湖南省网信办提出明确整改要求：（1）全面排查漏洞隐患，聚焦制度、技术、管理三个维度，逐条梳理薄弱环节，建立问题台账，实现闭环整改。（2）健全安全防控体系，升级 AI 内容识别、风险拦截、异常监测等技术能力，常态化开展风险自查自纠。（3）严格依法合规经营，依法完成生成式人工智能服务备案、算法备案等手续，规范服务运营行为，确保资质完备、运营规范。（查看更多）

Overseas News 境外动态

➢ Regulations Update 新规速递

EU: EDPS Publishes FAQ on Data Breach Notification

On 28 October 2026, the European Data Protection Supervisor (EDPS) published a FAQ on data breach notification, clarifying 12 key operational issues concerning the performance of notification obligations by data controllers. With respect to risk

assessment, the EDPS clarifies that a controller shall commence the assessment as soon as it becomes aware, with a reasonable degree of certainty, that a personal data breach has occurred. The assessment shall consider factors such as the type and sensitivity of the data, the quality of the data, the categories of affected data subjects, the processing activities involved, the volume of data, the breach-specific characteristics, and the security measures in place, and shall comprehensively evaluate the likelihood and severity of adverse effects, with results classified into three tiers: unlikely risk, risk, and high risk. Where the risk falls below the notification threshold, no notification to the EDPS is required, but the breach must still be documented internally. With respect to notification operations, phased notifications and supplementary information shall in all cases be submitted through the dedicated notification form, and informal emails are not accepted. Where new information becomes available after a conclusive notification has been submitted, the controller shall reassess the breach and, where necessary, submit a new conclusive notification. Where a single incident affects multiple processing operations, the controller may either group them into a single notification or submit individual notifications; a grouped notification shall specify item by item the data controller, the data processor, the affected data subjects, and the data categories, and shall still include a risk analysis for each combination. With respect to the "residual number," data subjects who could not be reached through direct communication shall be ensured to become aware of the breach through fallback solutions such as public notices on websites. In addition, where a subsequent investigation confirms that the incident does not constitute a breach, the controller may withdraw the original notification by submitting a comprehensive conclusive notification stating the reasons. (More)

欧盟：EDPS 发布数据泄露通知常见问题解答

2026 年 10 月 28 日，欧洲数据保护监督员（EDPS）发布了数据泄露通知常见问题解答，就数据控制者履行通知义务中的 12 个关键操作问题作出澄清。关于风险评估，EDPS 明确：控制者以合理确定性知悉泄露发生后即应启动评估。评估应结合数据类型与敏感性、数据质量、受影响主体类别、处理活动、数据规模、泄露特征及既有安全措施等因素，综合判断不利影响的可能性与严重性，并按照不太可能风险、风险、高风险三档认定结果。若风险低于通知门槛，无需向 EDPS 通知，但仍须内部记录。关于通知操作，分阶段通知及补充信息一律须使

用专用通知表格，非正式邮件不被接受。最终通知提交后若出现新信息，须重新评估并视情况提交新的最终通知。单一事件影响多个处理操作时，可合并为一份通知或分别提交，合并通知须逐项列明数据控制者、数据处理者、受影响主体及数据类别，并仍须逐组合进行风险分析。关于“剩余数量”，针对直接沟通失败未能触达的数据主体，须通过网站公告等兜底方式确保其知悉。此外，若后续调查证实事件不构成泄露，数据控制者可通过提交说明理由的综合最终通知撤回原通知。（查看更多）

EU: Council Agrees Position on Simplifying Data Protection, Privacy, and Cyber Reporting Rules

On 21 October 2026, the Council of the EU recently agreed its negotiating position on the proposal to simplify rules on data protection, privacy, and cybersecurity, aiming to make the EU’s digital rulebook clearer and easier to apply for businesses, public administrations, and citizens, so as to support competitiveness, while maintaining strong levels of protection for personal data. With respect to the GDPR: the current definition of personal data is maintained, and a new provision on pseudonymization and the identification of a natural person is introduced; compliance obligations are simplified in relation to unfounded or excessive requests and specific low-risk circumstances; a principle-based definition of “scientific research” is introduced, with targeted exemptions granted to research organizations; safeguards are added to the newly proposed derogation allowing for the processing of sensitive data for the purpose of biometric verification and in the context of the development and operation of AI systems; the extension of the deadline for the notification of personal data breaches is supported, and a single list at EU level of categories of processing likely to result in a high risk for individuals, as well as common templates, are established. With respect to the consolidation of data rules: the rules on data altruism and data intermediation services are streamlined; public sector bodies are allowed to set different conditions and charge higher fees for the re-use by very large enterprises and, in particular, undertakings designated as gatekeepers; and safeguards against the risk of trade secret leaks are strengthened, requiring that trade secrets be disclosed only once the data holder and the user have taken all necessary measures to preserve their confidentiality. With respect to cookies: the rules under the e-Privacy Directive are maintained, with clearer and additional purposes for which consent will not be required (such as

necessary for the provision of a service, audience measurement, and ensuring the security of the user's device), thereby reducing cookie banners. With respect to incident reporting: the proposed single entry point at EU level is replaced by the establishment of a national entry point in each Member State, and the establishment of an incident reporting information point at EU level, as well as a harmonized framework for incident notification and cross-border incident notifications, is proposed. (More)

欧盟：欧盟理事会就简化数据保护、隐私与网络报告规则达成立场

2026 年 10 月 21 日，欧盟理事会近日就其简化数据保护、隐私与网络安全规则提案达成谈判立场，在维持高水平个人数据保护的同时，使欧盟数字规则更清晰、更易适用，以支持竞争力。GDPR 方面，保留现行个人数据定义，新增关于假名化与自然人识别的条款；简化无根据或过度请求及低风险情形下的合规义务；引入基于原则的“科学研究”定义并给予研究机构定向豁免；为生物识别验证及 AI 系统开发运营中处理敏感数据的拟议克减增设保障措施；支持延长个人数据泄露通知期限，并建立欧盟层面高风险处理类别单一清单及通用模板。数据规则整合方面，精简数据利他与数据中介服务规则，允许公共部门对超大型企业（尤其守门人企业）设定不同复用条件和更高费用；强化商业秘密防护，要求商业秘密仅在数据持有者和用户采取一切必要保密措施后方可披露。cookies 方面，保留 e-privacy 指令下相关规则，新增无需同意的清晰目的（如服务必需、受众测量、设备安全），以减少 cookie 横幅。事件报告方面，将拟议的欧盟单一入口改为各成员国国家入口点，并拟建立欧盟层面事件报告信息点及跨境事件通知协调框架。（查看更多）

Canada: Privacy Commissioner of Canada Launches the *Children's Privacy Code*

On 20 October 2026, the Privacy Commissioner of Canada announced the launch of Canada's first *Children's Privacy Code* (Code), aimed at creating a safer and more transparent online environment for children and teens. The Code establishes clear, practical compliance expectations for organizations that handle children's personal information, including: (1) obtaining meaningful consent for the collection, use, and disclosure of children's personal information (with parental consent required for those under 13), and adopting an opt-in mechanism for non-essential data uses; (2) communicating privacy information in a clear, accessible, and age-appropriate manner; (3) providing children with a means of correcting inaccurate or incomplete personal information and the option to delete their personal information entirely, so as to

accommodate changes in their views as they grow and evolve; (4) avoiding profiling children for marketing purposes (including targeted or behavioral advertising) or for the purposes of AI-driven decision-making; and (5) promoting privacy by default, with settings such as location tracking, profile visibility, and third-party data sharing turned off by default. The Code also clarifies improper data use practices that are fundamentally incompatible with children's best interests: websites and mobile applications shall not use deceptive design practices to influence, manipulate, or coerce children into providing more personal information than necessary, nor use children's information to exploit their vulnerabilities. (More)

加拿大：加拿大隐私专员发布《儿童隐私守则》

2026年10月20日，加拿大隐私专员宣布启动加拿大首部《儿童隐私守则》（以下简称《守则》），旨在为儿童和青少年创造更安全、更透明的在线环境。《守则》为处理儿童个人信息的组织确立了清晰、务实的合规预期，包括：（1）就儿童个人信息的收集、使用和披露取得有意义的同意（13岁以下儿童须取得家长同意），非必要数据使用须采取选择加入（opt-in）机制。（2）以清晰、可访问且适合年龄的方式告知隐私信息。（3）为儿童提供纠正不准确或不完整个人信息的途径及完全删除个人信息的选项，以适应其成长中观念的变化。（4）避免为营销目的（包括定向或行为广告）及AI驱动决策目的对儿童进行画像。（5）推行默认隐私，位置跟踪、个人资料可见性、第三方数据共享等设置默认关闭。《守则》同时明确了与儿童最大利益根本不符的不当数据使用方式：网站和移动应用不得利用欺骗性设计影响、操纵或胁迫儿童提供超出必要范围的个人信息，也不得利用儿童信息利用其弱点。（查看更多）

EU: EDPB Adopts Statement on the Data Protection Challenges of Smart Glasses

On 13 October 2026, the European Data Protection Board (EDPB) adopted a statement on smart glasses and published a related expert report. The statement points out that, although smart glasses create opportunities for communication, assistance, and innovation, their increasing prevalence poses significant challenges to the protection of personal data and to individuals' rights and freedoms. The statement provides preliminary guidance to users, manufacturers, and service providers. With respect to the allocation of responsibility, whether a user constitutes a data controller under the GDPR depends on the manner of use. For example, if a user shares photos or videos on a public social media account, or uses the device for official, professional, or political

activities, the user will be considered a data controller. However, if the use is limited to personal activities such as filming family members or friends, or using the device for translation in a private context, the household exemption applies and the GDPR does not apply, although the user may still be subject to criminal, civil, and labor law, as well as other sector-specific rules. Manufacturers and the providers of linked applications or services, as data controllers, shall not transfer their obligations to users; they must comply with data protection law and ensure that any new processing remains compatible with the original purpose of collection. The EDPB emphasizes that smart glasses should make their recording obvious through bright LED lights, audio signals, voice activation cues, privacy-friendly smartphone notifications, or unique designs, and that such warnings need to be reliable, hard to ignore, and always up to date. The statement also encourages the development of industry standards and the implementation of awareness-raising measures. (More)

欧盟：EDPB 通过智能眼镜数据保护挑战声明

2026 年 10 月 13 日，欧洲数据保护委员会（EDPB）在通过了关于智能眼镜的声明，并发布相关专家报告。声明指出，智能眼镜虽创造沟通、辅助与创新机遇，但其普及对个人数据保护及权利自由构成重大挑战。声明为使用者、制造商和服务提供者提供初步指导。关于责任划分，用户是否构成 GDPR 项下的数据控制者取决于使用方式。如在公开社交媒体账户分享照片视频，或用于公务、职业、政治活动，用户将被视为数据控制者；不过，若仅用于拍摄家人朋友或私人场景翻译等个人活动，则适用家庭豁免，GDPR 不适用，但仍可能受刑事、民事、劳动法及其他行业规则约束。制造商及关联应用或服务提供者作为数据控制者不得将义务转嫁给用户，其须遵守数据保护法规并确保新处理行为与原收集目的相符。EDPB 强调，智能眼镜应通过明亮的 LED 灯、音频信号、语音激活提示、隐私友好的手机通知或独特设计使录制行为显而易见，且这些提示须可靠、难以忽视、始终更新。声明还鼓励制定行业标准并开展提高认识措施。（查看更多）

➢ Regulatory Actions 监管行动

UK: ICO Secures Data Protection Improvements from Ten AI Developers and Launches Call for Evidence on Agentic AI

On 8 October 2026, the Information Commissioner's Office (ICO) published a new report announcing that it had secured or secured commitments to data protection

improvements from ten of the world's largest AI foundation model developers operating in the UK. The improvements include providing clearer transparency information, strengthening mechanisms for individuals to exercise their rights, and conducting stricter assessments of safeguards. The report also sets out the ICO's regulatory positions on key issues, including the lawful use of special category data and whether foundation models themselves may contain personal data, and acknowledges that current model training practices present technical challenges when it comes to complying with UK data protection law and the principle of data protection by design. As foundation models underpin a new wave of AI agents capable of autonomously completing tasks, using tools, and interacting with websites, data protection risks are extending from the training stage to their independent behavior once deployed. The ICO has launched a six-week call for evidence, seeking views from developers, deployers, and others on the governance of risks posed by agentic AI, and has recently made enquiries with OpenAI and others concerning recent agentic AI testing and deployment. (More)

英国：ICO 促使十家 AI 开发商作出数据保护改进并就代理式 AI 征求意见

2026 年 10 月 8 日，英国信息专员办公室（ICO）发布新报告，宣布已促使在英国运营的十家全球最大 AI 基础模型开发商作出或承诺作出数据保护改进。改进措施涵盖提供更清晰的透明度信息、强化个人行使权利机制，以及更严格的安全保障评估。报告同时阐明 ICO 对特殊类别数据合法使用、基础模型本身是否包含个人数据等关键问题的监管立场，并承认当前模型训练实践在遵守英国数据保护法及“数据保护设计”原则方面存在技术挑战。随着基础模型支撑起新一代可自主完成任务、调用工具并交互网站的 AI 智能体，数据保护风险正从训练环节延伸至部署后的独立行为。ICO 已启动为期六周的证据征询，面向开发者、部署者等征求代理式 AI 风险治理意见，并已就近期智能体测试与部署向 OpenAI 等提出问询。（查看更多）

Italy: Garante Fines IQVIA €7 Million for Unlawfully Processing Patients' Health Information

On 2 October 2026, the Italian data protection authority (Garante) imposed a fine of €7 million on IQVIA for unlawfully processing the health data of approximately one million patients, rejecting the company's claim that the relevant records had been anonymized. The database at issue aggregated information provided by approximately

800 general practitioners and was used for research on medical treatments and related health outcomes, including studies commissioned by pharmaceutical companies. The Garante found that each patient was assigned a persistent code that allowed their successive records to be linked over time, and that the database simultaneously contained detailed information such as year of birth, sex, diagnoses, symptoms, prescriptions, medical tests, vaccinations, and location data. This combination was sufficient to single out and re-identify patients using reasonably available means, and therefore the records could not be treated as anonymous simply because conventional identifiers had been replaced with codes. The Garante found that IQVIA bore responsibility as the data controller from the point at which it collected information from doctors. Its violations included: processing health data without an appropriate legal basis, failing to adequately inform patients about how their data was used, failing to set defined retention periods (with records dating back to 2001), failing to complete a data protection impact assessment, and failing to implement adequate security measures. IQVIA must satisfy the rectification requirements within 120 days of notification if it intends to continue the processing activity. Alternatively, doctors must independently anonymize the information before providing it. (More)

意大利：Garante 因非法处理患者健康信息对 IQVIA 处以 700 万欧元罚款

2026 年 10 月 2 日，意大利数据保护机构（Garante），对 IQVIA 处以 700 万欧元罚款，原因是其非法处理约 100 万名患者的健康数据，并驳回该公司声称相关记录已匿名的抗辩。涉事数据库汇集了约 800 名全科医生提供的信息，用于医学治疗及相关健康结果研究，包括制药公司委托的研究。Garante 认定，每名患者被分配持久代码，可随时间关联其先后记录，数据库同时包含出生年份、性别、诊断、症状、处方、检验、疫苗接种及位置数据等详细信息，该组合足以通过合理可用手段识别并重新识别患者，因此不能仅因传统标识符被代码替代而视为匿名数据。Garante 认定 IQVIA 自向医生收集信息起即作为数据控制者承担责任，其违规包括：处理健康数据缺乏适当法律依据、未充分告知患者数据使用情况、未设定明确保留期限（记录可追溯至 2001 年）、未完成数据保护影响评估、未实施充分安全措施。IQVIA 须在收到通知后 120 天内满足整改要求方可继续处理活动。或者，医生须在提供信息前独立完成匿名化。（查看更多）

立方律师事务所编写本刊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. 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.

北京 | 上海 | 武汉 | 广州 | 深圳 | 海口 | 首尔

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Haikou | Seoul

www.lifanglaw.com
Email: info@lifanglaw.com
Tel: +86 10 64096099
Fax: +86 10 64096260/64096261