INNO CANYON
CONSULTING

Latest News in the Global Data Protection Space

contactus@innocanyon.com

LATEST NEWS IN THE GLOBAL DATA PROTECTION SPACE

The global data protection scene is rapidly evolving with frequent global developments. Some recent developments around the world are highlighted below.

Dutch DPA imposes a fine of 290 million Euros on Uber

The Dutch Data Protection Authority (DPA), Autoriteit Persoonsgegevens, fined Uber 290 million Euros for unlawful data transfers. Uber had transferred the personal data of its drivers to the U.S. without adequate protection, a severe violation of the General Data Protection Regulation (GDPR). The Dutch DPA found that Uber collected and stored the sensitive personal data of its drivers from the EU on US servers. The relevant sensitive personal data included account details, taxi licenses, location data, photos, payment details, identity documents, and sometimes criminal and medical data. For over two years, Uber transferred these data to its US headquarters without using proper security measures. The Court of Justice of the European Union (CJEU) had previously canceled the EU-US Privacy Shield 2020, a data transfer framework that the EU-US Privacy Framework has since replaced. However, Uber stopped using standard contractual clauses in August 2021, which led to insufficient protection of the personal data of EU drivers.

EU Standard contractual clauses are to be subject to public consultation.

The EU Commission announced its plans to open the standard contractual clauses for public consultation. The public consultation is scheduled for the fourth quarter of 2024, while the commission is expected to adopt new standard contractual clauses in the second quarter of 2025. Standard contractual clauses are a transfer mechanism that addresses the specific scenario where the data recipient, whether controller or processor, is in a third country but is directly subject to the GDPR. This will effectively complement the existing SCCs, which can be used for data transfers to third-country importers who are not subject to the GDPR.

CJEU - Joined Cases C-17/22 and C-18/22 - HTB Neunte Immobilien Portfolio

In the joined cases of HTB Neunte Immobilien Portfolio geschlossene Investment UG & Co. KG v Müller Rechtsanwaltsgesellschaft mbH (C-17/22), and Ökorenta Neue Energien Ökostabil IV geschlossene Investment GmbH & Co. KG v WealthCap Photovoltaik 1 GmbH Co. KG, WealthCap PEIA Komplementär GmbH, WealthCap Investorenbetreuung GmbH (C-18/22).

The matter pertains to investment entities endeavoring to obtain access to the names and addresses of individuals associated with indirect shareholdings in certain funds held by trust companies. However, the trust companies refused to disclose this information because some clauses prevented them from doing so. The local court of Munich noted that previous rulings usually require disclosure unless there's an abuse of rights. However, due to uncertainty about GDPR alignment, policies, and procedures, the court has referred the case to the CJEU. There was a request for a preliminary ruling from the Local Court in Munich, Germany. The CJEU (Court of Justice of the European Union) expanded the inquiry to include Article 6(1) (c) of the GDPR, which states that processing is necessary for compliance with a legal obligation to which the controller is subject, clarifying that data processing is permitted only if a legal basis exists. The court pointed out that the data subjects did not consent to sharing their identities. The court further explained that for data processing to be necessary for a contract, the contract must not prohibit identity disclosure, which it did. For the legitimate interest test, the CJEU outlined three steps. The controller must have a legitimate interest related to partners seeking contact information for negotiations. This interest must not be achievable through less intrusive means, such as asking permission to contact the other limited partners with shareholdings in the investment funds. The interests of the data subjects should not be overshadowed by the legitimate interest, especially since the contract prohibits disclosure. The CJEU emphasized that legal bases from case law must be clear, precise, and foreseeable.

The Korean Data Protection Authority (PIPC) publishes guidelines for foreign companies.

South Korea Personal Information Protection Commission (PIPC) released new guidelines to help foreign companies comply with South Korean data protection laws. These guidelines outline vital legal requirements and recent updates and aim to encourage strong data protection practices for the personal data of South Korean citizens.

DSK Publishes Guidance on Artificial Intelligence (AI) and data protection.

On the 6th of May, 2024, the German Data Protection Conference (DSK) issued guidelines on Artificial Intelligence (AI) and data protection. These guidelines provide companies with essential rules for using AI applications in compliance with data protection laws. According to the guidelines, businesses should clearly define their intended purpose and specific application areas to determine if personal data processing is necessary before implementing any AI system. The new AI regulation imposes strict conditions on specific AI systems, notably those considered high-risk, and prohibits manipulative AI systems.

Companies must verify whether personal data is needed to train AI models and ensure they have a valid legal basis for using that data. The guidelines emphasize that automated decisions with legal implications should involve human oversight.
The document stated that companies should choose closed systems operating within a controlled environment when selecting an AI system. Open systems pose risks, such as unauthorized access or misuse of data. Transparency is crucial, and users must be informed about how AI systems function and how their training data is utilized. Additionally, data subjects should have the option to reject the use of their data. Companies must ensure that individuals can exercise their rights, such as data rectification or erasure, through appropriate measures. The guidance also states that AI applications must comply with IT security standards outlined in Article 32 of the GDPR. Organizations must regularly review AI-related legal and technical developments and adjust their internal guidelines. Sensitive data, like health or political opinions, can only be processed with the explicit consent of data subjects, adhering to Article 9 of the GDPR. The DSK's guidance provides a comprehensive framework for companies to use AI while responsibly safeguarding data subjects' rights.

Hamburg DPA publishes a discussion paper on the relationship between the General Data Protection Regulation (GDPR) and large language models (LLMs).
The Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) released a discussion paper On the 15th of July, 2024, which focuses on the relationship between the General Data Protection Regulation (GDPR) and Large Language Models (LLMs). The discussion paper explains the technical details of LLMs to help companies and authorities address data protection concerns. It clarifies that storing an LLM does not count as data processing under the GDPR, as no personal data is retained. However, users can request information, deletion, or correction related to the inputs and outputs of these AI systems from their providers. The discussion paper also emphasizes that LLMs using personal data must comply with data protection laws, and any violations during the training process do not invalidate the model's legal use in AI applications.

Draft National Strategy on AI opened for public consultation.
On the 7th of September 2024, the Sri Lanka Ministry of Technology opened its draft national AI strategy for public consultation. The draft national strategy is open for input and support from the public, including industries and all political parties. This strategy establishes essential foundations to strengthen the nation's role in the global AI landscape, aligning closely with digital strategy 2030 and focusing on broader economic digitization efforts. The government embarked on three initiatives, including forming a multi-stakeholder committee under the presidential secretariat. The committee is empowered to draft a national AI strategy for 2024 - 2028.

The national digital strategy and its implementation plan are viewed as a dynamic framework that adapts to the ever-evolving global digital landscape and supports the country's goal of becoming a high-income economy by 2048. Key objectives include fostering sustainable economic growth and competitiveness, enhancing social inclusion, building a more substantial skills base, creating well-paying and dignified jobs, and providing trusted and inclusive services. The strategy aims to reshape and advance Sri Lanka's digital landscape, necessitating ongoing monitoring and evaluation to ensure prudent investments in digital infrastructure. A thriving private sector will be crucial for successful digital transformation with minimal reliance on public funding. Additionally, strengthening regulatory capacity, optimizing public investments and assets, and promoting social inclusion will be vital for sustainable development.

Canadian Competition Bureau Issues AI and Competition Discussion Paper.

Earlier in the year, the Canada Competition Bureau, an independent law enforcement agency that protects and promotes competition for Canadian consumers and businesses, released an AI and competition discussion paper. The discussion paper seeks to study AI, assess its effects on competition, and prepare for potential challenges. The Bureau will work with other agencies like the Office of the Privacy Commissioner and other relevant regulators to address emerging technologies, including AI, and how they affect their respective areas. The discussion paper offers an overview of how AI intersects with competition law and the technologies that can be integrated into AI products and services. The discussion paper describes the different markets involved in AI, including computational resources, AI technology development, and the creation of AI products and services. The discussion paper then examines how AI might influence market competition and be used in anti-competitive practices. Furthermore, the discussion paper outlines how AI may affect competition in the context of Canadian competition law, how it aims to foster thoughtful and informed dialogue which can help the Bureau in deepening its understanding of how competition is developing in AI markets, and how the Bureau can enforce and promote competition in these market. The discussion paper aims to gather stakeholders' feedback on its impacts on the Canadian markets.

Canada's Office of the Privacy Commissioner opens consultations on age assurance systems.

Canada's Office of the Privacy Commissioner (OPC) has initiated consultations on age assurance systems. The consultation, which started on the 10th of June, 2024, at the International Association of Privacy Professionals Privacy Symposium in Toronto, continues until the 10th of September, 2024. The consultation aims to assess various online methods for verifying user ages, including age declarations, verifications, and estimations, to protect younger users from inappropriate content.

The OPC will then utilize all the information obtained from the consultations to formulate policies and regulations, leading to the creation of a guidance document and further consultations. Additionally, the OPC intends to release a joint international statement of principles on age assurance later this year, focusing on enhancing online safety for youth while upholding privacy rights.

The Office of the Privacy Commissioner issues guidance on data anonymization.

On 17th of September, 2024, the New Zealand Privacy Commissioner issued guidance to agencies regarding data anonymization. The guidance provides that agencies using data anonymization and de-identification techniques must protect people's privacy. The Privacy Act allows for sharing information as long as it does not reveal personal details about identifiable individuals. It states that it is essential to handle information carefully, as accidental re-identification could result in serious harm. A privacy impact assessment (PIA) must be conducted to protect privacy, especially for any significant projects involving personal data. To minimize the risk of re-identification, any information that could potentially lead to the re-identification of individuals in the data-sharing process must be removed.

Brazil's National Data Protection Authority publishes data protection report.

On the 13th of September 2024, the Brazilian National Data Protection Authority (ANPD) published a report tagged "Navigating Data Protection in the G20 Digital Economy Agenda". The report highlights the significance of safeguarding personal data as a primary focus within the working group's four priorities: meaningful connections, public digital infrastructure, information integrity, and Artificial Intelligence (AI). The 3rd G20 Digital Economy Working Group Meeting took place on the 12th of June 2024 in Brazil, and one of the significant challenges highlighted in the report is the proliferation of disinformation, hate speech, and cyber threats targeting vulnerable groups, such as children, adolescents, and older people. The goal of the meeting was to promote the protection of personal data and discuss the role of data protection in the digital economy.

UNITED KINGDOM (UK)

Meta to make use of User Data to train AI: ICO responds

Meta stated that it will start training AI in the coming months by using public content from adults on Facebook and Instagram in the UK. According to Meta, this will help build AI to capture British history, culture, and language.

In response to the above, the Information Commissioner's Office (ICO) said it will monitor Meta's activities in the coming weeks. The ICO has emphasized that any organization using user data to train generative AI models must be transparent about how the data is used. It further stated that organizations should implement appropriate safeguards before using personal data for model training. Users must also be provided with a clear and straightforward way to object.

Meta had earlier paused its plans to use Facebook and Instagram user data for training generative AI following the ICO's request. Meta has since updated its approach by making it easier for users to object to data processing. Meta will now proceed with its plans with ICO monitoring the situation. The ICO also emphasized the importance of transparency in deploying user data to train generative AI models. Organizations should implement strong safeguards before using personal data for model training and provide a clear and straightforward way for users to object. The ICO has not approved this processing activity, so it is Meta's responsibility to ensure and demonstrate ongoing compliance.

UNITED STATES OF AMERICA

Senators urge the DOJ to Investigate Generative AI Products for Potential Antitrust Violations.

On September 10, 2024, some US senators issued a statement urging the Department of Justice (DOJ) Antitrust Division and the Federal Trade Commission to investigate whether the designs of some generative AI features recently launched by some online platforms constitute a form of exclusionary conduct or an unfair method of competition in violation of the antitrust laws.

This request concerns major online platforms launching new generative AI features that address user queries by summarizing or, in some cases, simply repeating content from other sources or platforms. These new AI features further jeopardize the ability of journalists and content creators to earn fair compensation for their essential work. Unlike traditional search results or news feed links, which direct users to the publisher's website, AI-generated summaries keep users on the original search platform, where the platform alone benefits from user engagement through advertising and data collection. The Senators urged the DOJ's Antitrust Division and the Federal Trade Commission to investigate whether the design of some generative AI features introduced by already dominant platforms is a form of exclusionary conduct or an unfair method of competition in violation of the antitrust laws.

Switzerland Issues US Adequacy Decision.

For the Swiss-U.S. DPF, organizations can receive personal data from Switzerland from 15th September 2024, when Switzerland recognizes adequacy. Although the Swiss-U.S. DPF Principles became effective on 17th July 2023, concerning the Swiss-US Data protection framework, US entities can receive personal data from Switzerland following the adequacy decision granted to the US by Switzerland. Data transfers could only commence after adequacy was recognized in compliance with Swiss law. The Data Privacy Framework (DPF) program, managed by the International Trade Administration (ITA) in the U.S. Department of Commerce, allows eligible U.S. organizations to self-certify compliance with the EU-U.S. DPF, the UK Extension, and the Swiss-U.S. DPF. Those under the Swiss-U.S. Privacy Shield must adhere to the Swiss-U.S. DPF Principles to benefit from the new framework.

House Committee Prepares to Discuss Kids Safety Online Act.

On 18th September 2024, the House Committee on Energy and Commerce convened to deliberate on the Kids Safety Online Act (KOSA) bill. Some senators, alongside some parents who tragically lost their children due to online hazards, advocated for legislative action to safeguard children's online well-being. It was reported that a group of parents were scheduled to visit Capitol Hill to confer with legislators in anticipation of the Energy and Commerce House Committee's forthcoming review of the bill. However, the bill's passage is anticipated to encounter challenges, as certain Republican members have expressed reservations regarding its constitutionality, the broad authority conferred upon the Federal Trade Commission, and the potential for censoring conservative perspectives. Notably, the committee's markup is slated to occur just ahead of the House's autumn recess, which is expected to extend beyond the November election. Advocates are optimistic that this timing may facilitate a House vote on the bill by year-end.

Pennsylvania

Pennsylvania AG launches an online portal for data breach reporting.

The Pennsylvania Attorney General has launched an online portal to simplify the reporting process for data breaches. The AG stated that starting from the 26th of September 2024, companies must report breaches affecting over 500 residents as mandated by state law. He further noted that credit reporting agencies and other organizations that handle personal data must inform the Office of the Attorney General about such breaches under the new Breach of Personal Information Notification Act (BPINA). The new law will enhance protections for Pennsylvanians by ensuring prompt notifications when sensitive information is compromised. The recently launched portal aims to simplify the reporting process for businesses required to notify affected individuals.

Montana

Montana's Consumer Data Privacy Act (MTCDPA)

The Montana Consumer Data Privacy Act (SB 384) was signed in May 2023 and became effective on 1st October 2024, making Montana the 12th state to implement privacy legislation. The Act applies to organizations based in Montana, those providing goods/services to Montana residents, and entities managing data for large numbers of residents or earning significant revenue from data sales.

The Act requires data processors and controllers to provide a detailed privacy notice, process personal data only when necessary, allow consumers to exercise their privacy rights securely, obtain consent for processing sensitive data, contract with data processors, and conduct protection assessments for high-risk activities.

Tennessee

Tennessee's Information Protection Act (TIPA)

The Tennessee Information Protection Act (TIPA) was signed into law in May 2023 and will become effective from the 1st of July 2025. TIPA is designed to be business-friendly, with less strict criteria for applicability. Key consumer protection provisions include the ability for consumers to confirm, modify, or delete their personal data. TIPA also provides that data controllers must adhere to best practices for data handling. It provides for a two-year onboarding period, giving all businesses ample time to comply and supporting businesses with existing privacy programs aligned with frameworks like the National Institute of Standards and Technology (NIST), which can use an affirmative defense to protect against potential violations.

Texas

Deadline for compliance with the Texas' Data Privacy and Security Act (TDPSA) draws near.

The Texas Data Privacy and Security Act (TDPSA) was signed on the 18th of June, 2023, and took effect on the 1st of July, 2024, with entities required to comply by the 1st of January, 2025. TDPSA aims to establish data privacy requirements based on industry best practices, similar to laws in California and other proactive states. The Act applies to businesses operating in Texas or offering products or services to Texas residents. The Act exempts small businesses, as defined by the Small Business Administration, from compliance. Some notable features of the TDPSA include the requirement that companies must disclose sales of sensitive information, the provision of a universal opt-out mechanism for consumers, etc.

The Hong Kong Monetary Authority publishes a circular on using AI

The Hong Kong Monetary Authority (HKMA) issued a circular to industries on 9th September 2024, informing them about the potential of AI in reducing risks related to money laundering and terrorist financing. The circular emphasized HKMA's commitment to supporting and promoting the use of AI in authorized institutions, given the increasing complexity of money laundering and terrorist financing risks, including global cases and the use of mule accounts. Authorized institutions are to enhance their monitoring and risk management by adopting technologies that will help improve monitoring systems, allocate resources to higher-risk activities, and facilitate more effective intelligence sharing within the industry.

To promote the use of AI in monitoring suspicious activities, HKMA announced several initiatives, including an upcoming forum in November 2024, which will feature industry and technology speakers discussing AI applications in suspicious activity monitoring. Additionally, HKMA is set to provide targeted guidance and support through a dedicated team and external consultants, who will offer feedback and technical guidance to help authorized institutions improve their monitoring processes. This support will be provided through the Fintech Supervisory Sandbox and Chatroom. HKMA assured authorized institutions of its commitment to supporting their anti-money laundering and counter-terrorist financing efforts.

Irish DPC fumes as X trained its AI with user posts without informing them

X (formerly known as Twitter) has trained its Artificial Intelligence (AI) system, Grok, on users' posts without informing them. The Data Protection Commission (DPC) made significant efforts to address concerns about the processing of personal data in the public posts of X's European Union /European Economic Area users to train its AI 'Grok'. Consequently, legal action was taken against X in the Irish High Court on the 8th of August 2024. The Norwegian data protection authority, through the office of the Data Protection Commission (DPC), alleged that social media company X uses user personal data to train its AI. The DPC emphasized that the company must handle personal data legally and transparently under the EU's General Data Protection Regulation (GDPR). This means that social media company X users have the right to know how their data is used and the legal basis for that use. There is uncertainty about whether X has obtained consent to process user data to train Grok, its AI model.

The Irish Data Protection Commission (DPC), in its capacity as X's supervisory authority in the EU, agreed with X to pause data processing for AI training. Users who do not want their information used for such AI training have been advised to adjust their settings and turn off the pre-ticked option for AI training. The investigation into the legality of this AI model will continue in collaboration with the DPC and other EU authorities. European Digital Rights activist NOYB has also filed lawsuits in nine EU countries regarding the legality of X's data processing for AI training.

Court upholds the Austrian Data Protection Authority's decision on cookie banners.

In this case, a data subject visited a media company's website and encountered a cookie banner with the reject option hidden in a second layer. They complained to the Austrian DPA, claiming violations of GDPR due to this design. The controller argued their actions were for journalistic purposes and not under the DPA's jurisdiction. They later improved the banner by adding a visible reject button but removed it again. The DPA ordered the controller to ensure the reject option was as prominent as the accept button. On the 31st of July, 2024, the Federal Administrative Court in Austria gave its final verdict in the matter W108 2284491-1/15E, in which a cookie banner's first layer was hidden in the second layer. The court agreed with the Data Protection Authority that the controller must ensure that the reject option contains a visually equivalent option to reject cookies and must be prominent, just like the accept button. The court dismissed the appeal of the controller as unfounded.

Romania's Data Protection Authority fines Fundația Pro Economica

In August 2024, the National Supervisory Authority for Personal Data found the Pro Economica Foundation violated GDPR Article 32 and fined them 4,976.70 lei (about 1,000 euros). The investigation was prompted by a report of a data security breach resulting from a cyberattack that deleted personal data from the Foundation's server, impacting data availability. The supervisory authority stated that the Foundation failed to implement adequate security measures, leading to unauthorized access to personal data, including names, contact details, and financial information. The Authority also ordered the Foundation to review and enhance its technical and organizational security measures for data protection.

PORTUGAL

National Data Protection Authority Portugal. (CNPD) Portugal - Deliberação 2019/207

The Portuguese Data Protection Authority (CNPD) issues fine In Portugal, during a routine inspection by the Public Security Police at a commercial establishment on the 18th of June, 2018, the data protection authority stated that it discovered that there was no visible informational notice about the operation of an active CCTV system. The situation was reported to the CNPD. The CCTV system had been installed to protect people and property. The business owner, who had recently acquired signage after a similar issue at another store, argued that an informative sign was always present but obscured by furniture. The controller also highlighted her financial hardships and ongoing negotiations with creditors. The CNPD imposed a €2,000 fine on a controller for not informing data subjects about video surveillance by failing to install signs in the monitored area, which violated Article 13 of the GDPR.

References

1. Autoriteit Persoonsgegeven, 'Dutch DPA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US (August 2024) https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us.
2. European Commission(EU) Standard contractual clauses for the transfer of data to third-country controllers and processors subject to the GDPR, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14404-Standard-contractual-clauses-for-the-transfer-of-data-to-third-country-controllers-and-processors-subject-to-the-GDPR_en
3. EUR-Lex Access to European Union law, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0017
4. South Korea Personal Data Protection Commission,' PIPC Releases "Guidelines on Applying the Personal Information Protection Act to Foreign Business Operators" https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2488
5. Dr. Hans Markus Wulf and Antje Munch,' Data protection compliant use of artificial intelligence – Data protection authorities publish guidance,' Heuking, https://www.heuking.de/en/news-events/newsletter-articles/detail/data-protection-compliant-use-of-artificial-intelligence-data-pro.tection-authorities-publish-guidance.html accessed 25th September 2024
6. The Hamburg Commissioner for Data Protection and Freedom of Information, 'Hamburg Theses on Person Reference in Large Language Models,' (15th July 2024), https://datenschutz-hamburg.de/news/hamburger-thesen-zum-personenbezug-in-large-language-models accessed 25th September 2024.
7. DFG Publishes Position Paper on the Future EU Framework Programme (FP10) (May 2024), https://www.dfg.de/en/service/press/press-releases/2024/press-release-no-22
8. Ministry of Technology, Digital Sri Lanka 2030 (A National Digital Strategy for Sri Lanka), https://mot.gov.lk/assets/files/National%20Digital%20Economy%20Strategy%202030%20Sri%20Lanka-bc77184e0b6035d235cd0bb1ebf75707.pdf

9. Artificial Intelligence and Competition, Discussion Paper, https://competition-bureau.canada.ca/sites/default/files/documents/AICompetition-Discussion-Paper-240320-ver3-e.pdf
10. Office of the Privacy Commissioner Canada,' exploratory consultation on age assurance Systems', https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/nr-c_240610/
11. Privacy Commissioner,' Care is needed with Data Anonymisation', https://privacy.org.nz/publications/statements-media-releases/care-is-needed-with-data-anonymisation/
12. ANPD holds side-event to the 3rd G20 Digital Economy Working Group Meeting, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-holds-parallel-event-to-the-3rd-g20-digital-economy-working-group-meeting
13. Meta,' Building AI Technology for the UK in a Responsible and Transparent Way',(September 2024), https://about.fb.com/news/2024/09/building-ai-technology-for-the-uk-in-a-responsible-and-transparent-way/
14. Information Commissioner Office (ICO) statement in response to Meta's announcement on user data to train AI, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/09/ico-statement-in-response-to-metas-announcement-on-user-data-to-train-ai/
15. Suzanne Smalley, 'UK regulator stops LinkedIn from training AI models with British users' content', (20th September 2024), https://therecord.media/uk-regulator-stops-linkedin-ai-models accessed 25th September 2024.
16. Klobuchar, Colleagues Urge Justice Department, Federal Trade Commission to Investigate Generative AI Products for Potential Antitrust Violations, https://www.klobuchar.senate.gov/public/_cache/files/2/8/28792e8d-9f57-4f82-84eb-810103e85084/2E67A60C5FD8132EB31EBCDFD9DFF9078BEDD557974D621951B43B0597175096.final-letter-to-doj-ftc---competition-issues-with-generative-ai-and-content---9.10.24.pdf
17. Data Privacy Framework (DPF) Program, https://www.dataprivacyframework.gov/Program-Overview
18. Miranda Nazzaro, The Hill,' Senators, parents ramp up pressure on House to pass Kids Online Safety Act'(September 2024), https://thehill.com/policy/technology/4884489-senate-pressure-house-kids-online-safety-act/
19. AG Henry Launches Online Portal for Companies Required to Report Data Breaches that Impact Pennsylvanians, https://www.attorneygeneral.gov/taking-action/ag-henry-launches-online-portal-for-companies-required-to-report-data-breaches-that-impact-pennsylvanians/
20. Osman Husain, Enzuzo, 'Data Privacy Laws', https://www.enzuzo.com/blog/data-privacy-laws
21. Ibid.
22. Use of Artificial Intelligence for Monitoring of Suspicious Activities, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240909e1.pdf
23. On Protection of Personal Data During The Fight Against COVID-19, https://www.kvkk.gov.tr/Icerik/6731/On-Protection-of-Personal-Data-During-The-Fight-Against-COVID-19
24. Datatilsynet, X trains AI on user data', https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2024/x-trener-ki-pa-brukerdata/
25. Datatilsynet (Norway) - 23/03206, Datatilsynet (Norway) - 23/03206 - GDPRhub
26. Federal Administrative Court, Rdb.manz 'BVwG W108 2284491-1 - Decision', https://gdprhub.eu/index.php?title=BVwG_-_W_108_2284491-1
27. The National Supervisory Authority for the Processing of Personal Data, https://www.dataprotection.ro/?page=Comunicat_Presa_10.09.2024&lang=ro
28. GDPRhub, CNPD (Portugal) - Deliberação 2019/207, https://gdprhub.eu/index.php?title=CNPD_(Portugal)_-_Delibera%C3%A7%C3%A3o_2019/207

Sign up for the Inno Canyon newsletter!
We keep you updated about the latest news and developments as they occur.

https://innocanyon.com/newsletter-2/

INNO CANYON
CONSULTING

contactus@innocanyon.com