NEWSLETTER

AZURE DATA PROTECTION CONSULTANTS LLP

JANUARY 2023

Your privacy digest is filled with the latest developments in the field of privacy and data protection across the globe.

There has been never been a better time to strengthen privacy compliance, We wish you all a happy and privacy compliant New Year!!

Data Breaches

Password manager company breached
December 1, 2022

An investigation was announced on LastPass, password manager company into a security incident in which customers' personal data, stored in a third-party cloud storage provider, shared by LastPass and its parent company, GoTo was accessed by an unauthorized party. This is the second time, the systems were compromised.

US ICE discloses identities of vulnerable immigrants
December 1, 2022

US Immigration Customs Enforcement accidentally posted the identities and detention locations of more than 6,000 immigrants fleeing "torture and persecution" on its website. The document was posted on the website for approximately five hours that included names and other personally identifiable information, along with immigration information, of approximately 6,000 non-citizens in ICE custody. ICE took swift action to immediately rectify as it was a breach of policy. The government will notify people who downloaded the information that they should delete it.

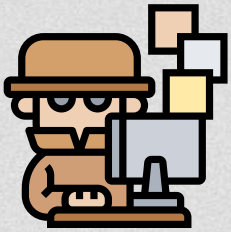
Dutch political party suffers data leak
December 1, 2022

Forum for Democracy, Dutch political party had its entire membership leaked through its mobile application, ForumApp. Nearly 93,000 party members had personal identifiable information leaked, including bank account numbers and addresses, after the app was recently launched during a General Meeting of Members. Leak occurred due to an attack on their IT systems.

OAIC launches investigation on Medibank amid data leak on dark web

December 1, 2022

The Office of the Australian Information Commissioner launched an investigation into the Medibank data breach. OAIC claims that the investigation could result in civil penalties of up to AU$2.2 million for each violation of Australian privacy law. Medibank breached database has been published on the dark web by the hackers which contained six zipped files of customer data which covers around 9.7 million impacted customers.



Health authority suffers cyberattack; data exposed

December 8, 2022

A cyberattack on health authority Eastern Health exposed private data of more than 58,000 Newfoundland and Labrador residents and 280 current and former staff members. The Office of the Information and Privacy Commissioner for Newfoundland and Labrador said an investigation into the breach won't be complete until March 2023. Eastern Health said the social insurance numbers of less than 20 patients and banking information of less than five patients were accessed.

Medical provider suffers ransomware attack; patient data exposed

December 8, 2022

Chicago-based health provider CommonSpirit Health confirmed it suffered a ransomware attack which exposed personally identifiable information of more than 620,000 patients in 21 states. Recently, the company said it was targeted by a ransomware attack but did not state the number of affected patients.

New Appointments / New laws

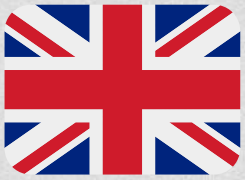
India and EU FTA talks focuses on data flow and privacy
December 29, 2022

India and European Union in the recent Free Trade Agreement third round talks discussed about the data flows, privacy, consumer protection, open government data, and issues related to capital movements and payments under the ongoing free trade agreement negotiations. The fourth round of talks is scheduled for March 2023.

Mandatory cyber incident reporting for managed service announced by UK
December 1, 2022

UK announced mandatory incident reporting obligations for managed service providers (MSPs) and minimum security requirements. This is an update to the Network and Information Systems Regulations and fines can be levied for non-compliance of the same for up to 17 million GBP. This comes after the government recognised MSPs as high value target for malicious threat actors, and can be used as staging points through which threat actors can compromise the clients of those managed services.

UK and Japan reach digital partnership
December 7, 2022



U.K. and Japan have established the U.K.-Japan Digital Partnership, a framework to "jointly deliver concrete digital policy outcomes" for citizens, businesses and economies. The partnership will focus initially on four pillars: digital infrastructure and technologies, data, digital regulation and standards, and digital transformation.

EC adopts Digital Operational Resilience Act
December 1, 2022

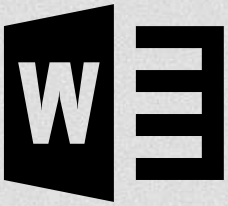
The European Council adopted the Digital Operational Resilience Act(DORA) to ensure member states' financial sectors can stay resilient through a severe operational disruption. DORA creates uniform requirements for network security and information technology systems of financial services companies, as well as third party information communication technology providers. Member states must now pass parts of the legislation that require national transposition. Simultaneously, relevant European Supervisory Authorities, including the European Banking Authority, will develop required technical standards for financial institutions.

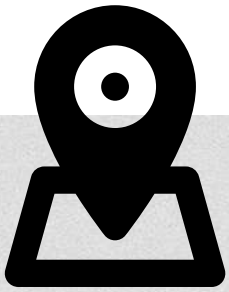
DSK introduces resolution for processing of health data
December 1, 2022

The Conference of the Independent Data Protection Authorities of Germany introduced a resolution for the processing of personal health data at its 104th conference. Measures will include encryption and pseudonymization of patient data by a trust authority.

DSK bans use of Microsoft Office 365 in schools
December 1, 2022

The Conference of the Independent Data Protection Authorities of Germany banned the use of Microsoft Office 365 in all schools. The ban came after concerns were raised on security of student's data on cloud servers based in US. German DPA working group also found that the company has not resolved privacy compliance issues around its Microsoft Office 365 products even after 2 years.





HHS Office of Civil Rights issues notice for entities using tracking technology

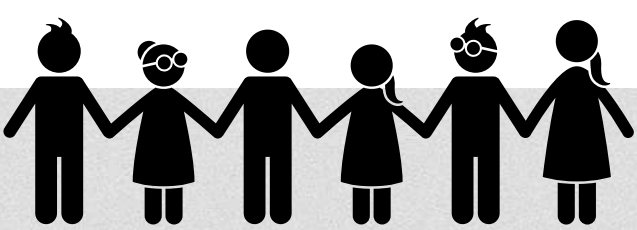
December 1, 2022

The U.S. Department of Health and Human Services Office of Civil Rights issued guidance to entities and business associates using tracking technology under the Health Insurance Portability and Accountability Act. OCR noted some regulated entities often share electronic protected health information with online tracking providers in a manner that violates the HIPAA Rules. The guidance covers issues around tracking on webpages, Tracking within mobile apps and HIPAA compliance obligations for regulated entities when using tracking technologies.

e-Evidence regulation agreement reached by EU lawmakers

December 1, 2022

The Council of the European Union, European Parliament and European Commission reached an agreement on the e-Evidence regulation. The proposed legislation aims to facilitate cross-border criminal investigations by putting in place a cooperation mechanism for European police forces to obtain evidence stored in electronic form by a service provider like an email service or messaging that is based in another EU country. Aiming to facilitate cross-border criminal investigations, the regulation implements a mechanism for law enforcement agencies to obtain electronic evidence stored in another EU country. It includes the European Preservation Order, under which a judge could order a service provider to preserve data related to a suspect that could be accessed at a later date.



New Jersey introduces bill to establish Children's Data Protection Commission

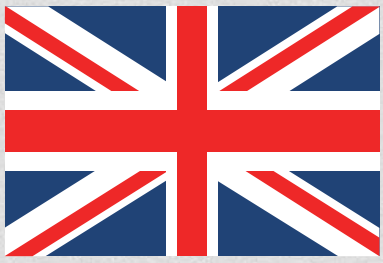
December 5, 2022

New Jersey State Assembly introduced a bill to create a New Jersey Children's Data Protection Commission. The legislation concerns "social media privacy and data management standards for children" and establishes a nine-member commission to receive feedback from a "broad range of stakeholders" recommending best practices for protecting children's personal data online. The bill requires digital companies operating in the state to conduct data protection impact assessments before launching new products likely to be accessed by children. Fines for failure to comply are proposed to be $2,500-$7,500 per affected child.

U.K. released a voluntary code of practice to improve security and privacy

December 9, 2022

The U.K. released a voluntary code of practice to improve security and privacy requirements on applications and app stores. New measures include improved reporting of software vulnerabilities and enhanced transparency around privacy and security for app users. "Today we are taking steps to get app stores and developers to keep customers even safer in the online world," Minister of State at the Department for Digital, Culture, Media and Sport Julia Lopez said. The government will work with app developers and operators over the coming nine months to ensure adoption.



Children’s Code design tests created by ICO
December 12, 2022

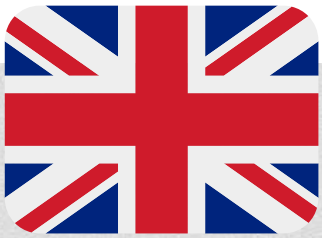
The U.K. Information Commissioner's Office created design tests to help designers assess whether products or services likely to be accessed by children comply with the Children's Code. The ICO said the tests will support designers in creating online experiences that protect children's personal data. Each test provides a report detailing areas of good practice as well as steps you can take to improve your conformance.

EU-US draft adequacy decision adoption process begins
December 14, 2022

Following the Executive order signing by President Joe Biden, European Commission has published and launched the process towards the adoption of an adequacy decision for the EU-U.S. Data Privacy Framework, which will foster safe trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in its Schrems-II decision of July 2020. The draft decision concluded that the United States ensures an adequate level of protection for personal data transferred from the EU to US companies.

Microsoft rolls out 'data boundary' for EU cloud customers
December 15, 2022

Microsoft is beginning a phased rollout of its "EU data boundary" enabling EU cloud customers to process and store data in the region starting from January 1, 2023. The "EU data boundary" applies to Microsoft's core cloud services. A first phase will include customer data, followed by logging and service data.

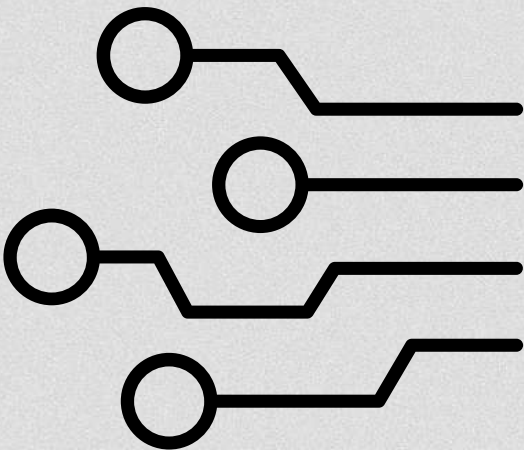


UK and UAE commit to updated data partnership
December 15, 2022

The U.K. government and Dubai International Financial Centre Authority released a joint statement committing to increased facilitation of personal data flows. The two sides called the new agreement a robust data bridge that will help realize the benefits of the important role that the trustworthy use of data across borders play. The U.K. and the DIFC indicated a mutual understanding on the importance of existing and future regulatory cooperation as a means of enhancing objectives of both countries.

EU institutions sign digital rights declaration
December 15, 2022

European Commission, the Council of the European Union and European Parliament signed a declaration on EU digital rights and principles that highlights the EU's commitment to a secure, safe and sustainable digital transformation. The declaration focused on EU core values and fundamental rights and aims to guide policy makers and companies dealing with new technologies. Institutions also put emphasis on the declaration fostering control about how personal data is used and with whom it is shared.



Slovenia passes Personal Data Protection Act
December 17, 2022

Drvani Zbor, National Assembly of Republic of Slovenia recently adopted Personal Data Protection Act (ZVOP-2). With 50-8 votes in favor, the government transposes the EU GDPR into Slovenian legislation as the country met all the requirement to fully implement the GDPR. ZVOP-2 or Personal Data Protection Act is written into Article 38 of the Constitution of the Republic of Slovenia regarding the human right to the protection of personal data. The ability to access personal data collected by companies and judicial redress for the mishandling of one's personal data are some of the aspects of the act which is covered by the act. One of the official has pointed out that video surveillance in public areas and special data processing are also important system innovations regarding certain processing of personal data with respect to the law.

OECD passes agreement on Government access to personal data
December 19, 2022

OECD countries which included US and 37 other countries adopted an agreement on safeguarding privacy when accessing personal data for national security and law enforcement reasons after 2 years of negotiations. This will be known as Declaration on Government Access to Personal Data held by Private Sector Entites. OECD Secretary-General Mathias Cormann said the agreement will enable data flows "with the safeguards needed for individuals' trust in the digital economy and mutual trust among governments regarding the personal data of their citizens." The framework also covers topics such as the purposes for which law enforcement authorities collect personal data and the oversight bodies that are in place in each country.

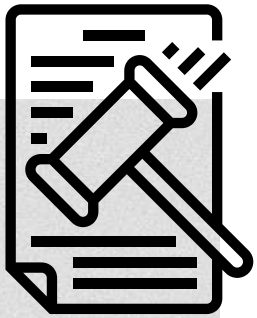
Fines and Settlements

Clubhouse owners fined 2M euros by Garante
December 5, 2022

Alpha Exploration, owner of the social media app Clubhouse got fined €2 million due to GDPR violations by Italian DPA. The app supports voice conversations that take place in conversation rooms and is available to the public through an app. There were various violations found by the DPA which were based on lack of transparency, profiling and sharing of the account information without legal basis, indefinite storage of the data and many more which led to violation by the social media platform. In 2021, Clubhouse had more than 16M global users and about 90k users in Italy. The Garante said Alpha Exploration will implement measures to protect users and conduct an impact assessment on data processed through Clubhouse.

WhatsApp fine of 225M euro upheld by CJEU
December 7, 2022

The Court of Justice of the European Union denied a challenge by Meta's WhatsApp over its 225 million euro fine issued by Ireland's Data Protection Commission in September 2021. WhatsApp filed for annulment of the European Data Protection Board decision that led to the DPC fine. The CJEU upheld the EDPB's role and authority to arrive at a collective decision under the EU General Data Protection Regulation's consistency mechanism while noting WhatsApp was not directly concerned by the board's decision.



Phone company fined 300,000 euros by CNIL
December 8, 2022

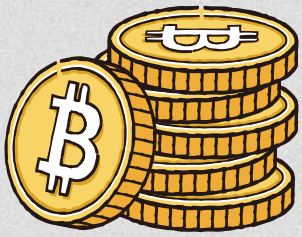
FREE, a French phone provider was fined 300,000 euros by France's data protection authority. The CNIL found FREE in violation of several EU General Data Protection Regulation provisions, including individuals' right to access their data, right to erasure, failure to ensure the protection of data and failure to document data breaches.

National Institute of Statistics fined 4M euros by CNPD
December 12, 2022

Portugal's National Data Protection Commission fined the National Institute of Statistics 4.3 million euros for five violations of the EU General Data Protection Regulation related to the 2021 census. The CNPD determined the INE unlawfully processed personal health and religious data, failed to notify respondents of the 2021 census questionnaire, violated data transfer provisions, failed to conduct a data protection impact assessment and did not meet due diligence in selecting a subcontractor.

Cryptocurrency exchange fined 2M AU$ by ACMA
December 15, 2022

Cryptocurrency exchange Binance Australia paid an AU$2 million fine, handed down by the Australian Communications and Media Authority, for spamming customers. An ACMA investigation found the company sent more than 5.7 million spam emails advertising trading services without obtaining consent from the recipients, between October 2021 and May 2022.

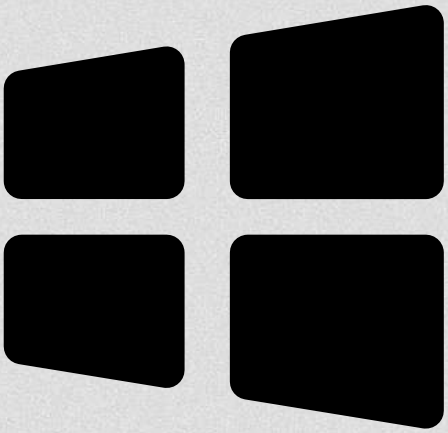


FTC and Epic games reach $520M COPPA settlement
December 19, 2022

US FTC (Federal Trade Commission) agreed settlement with Epic games to a $520 million settlement due to certain data privacy violations on their game called “Fortnite”. The record-breaking settlement includes in 2 folds which the company has to pay, $275 million in civil penalties and $245 million in refunds to users affected by "dark patterns."

Microsoft fined 60M euros by CNIL
December 22, 2022

CNIL imposed Microsoft a penalty of 60M € for imposing advertised cookies forcefully on users. This came after the following complaint and investigation by CNIL for advertised cookies on "bing.com". The French regulator said that after investigations it found that "when users visited this site, cookies were deposited on their terminal without their consent, while these cookies were used, among others, for advertising purposes." CNIL has justified the penalty by considering various elements like the scope of the processing, the number of data subjects and the profits the company made from advertising profits indirectly generated from the data collected via cookies.



Azure Data Protection Consultants LLP

Contact us for any queries:

http://www.azuredpc.com

Azure Data Protection Consultants LLP

+91- 9599706305

DISCLAIMER