The following is a selection of global COVID-19 developments compiled by the Thomson Reuters Data Privacy news team. This news bulletin covers technology developments, cybersecurity, proposed legislation, and other key data privacy updates relating to COVID-19.

Users can sign up to receive the Daily Bulletin for more news articles through Profile Settings – Preferences.

**Technology Developments**

**How COVID-19 Pandemic Impacted India Inc.'s IT Strategies** India (March 19, 2021)

The COVID-19 pandemic and uncertain market conditions have had a significant impact on Indian organizations' IT strategies, according to the Veeam Data Protection Report 2021. The report highlighted that 64% of Indian organizations accelerated their digital transformation initiatives to enable real-time data capture, lower processing time, and accelerate business outcomes.

**Use of AI to Fight COVID-19 Risks Harming 'Disadvantaged Groups'** Eurasia (March 16, 2021)

Rapid deployment of artificial intelligence and machine learning to tackle COVID-19 must still go through ethical checks and balances, or there is a risk of harming already disadvantaged communities in the rush to defeat the disease. This is according to researchers at the University of Cambridge's Leverhulme Centre for the Future of Intelligence, who are cautioning against blinkered use of AI for data-gathering and medical decision-making as we fight to regain some normalcy in 2021.

**Cybersecurity**

**Magic Kingdom Uses COVID-19 As an Excuse to Install Facial Recognition** U.S. (March 25, 2021)

According to a Walt Disney World announcement, Magic Kingdom will be using facial recognition to ID guests between March 23 and April 23, 2021, raising privacy concerns.

**Data, Privacy, And the Health of Nations** U.S (March 23, 2021)

What may have seemed like esoteric and academic discussions about obscure issues a few months ago are now prime-time questions that directly affect the future ahead of us. How data is being treated in an effort to understand, and ultimately stop, the spread of COVID-19, and how privacy is being traded off in those efforts, will set a course that will be hard to alter.

Cyber players on Capitol Hill are likely to focus on oversight of COVID-19 response and related security issues, supply-chain security, and DHS activities in general following the enactment of the American Rescue Plan Act.

Proposed Legislation


The Washington state Legislature is in the process of reviewing new legislation aimed at safeguarding COVID-19 health data. House Bill 1127, which was passed in the state's House of Representatives last week, now sits with the Senate, where, if passed, it would establish guidelines for organizations that collect and analyze novel coronavirus health data.


The European Commission published a proposal for a regulation to create a framework for an interoperable "Digital Green Certificate" to prove that people have been vaccinated against COVID-19, received a negative COVID-19 test result, or recovered from COVID-19. The purpose of the certificates is to facilitate the exercise of free movement of persons in the European Union. The European Commission hopes that the proposal will be adopted by the summer of 2021. Personal data included in the certificates would be limited and the data would not be retained.


Under legislation proposed by Senate and House Democrats, the U.S. Department of Homeland Security's immigrant detention facilities would be required to collect and publicly report data about COVID-19 cases, vaccine distribution, and what preventative measures they have in place to curb transmission of COVID-19.

Other Key Data Privacy Updates

Check-In App Only Option Tasmania (March 19, 2021)

The use of the government's Check-In TAS app will be mandatory for business premises in Tasmania from May 1, 2021. The app will replace a mix of third-party apps and paper sign-in forms and will help address privacy concerns around the retention and use of personal data by businesses.

Public Should Not Upload Vaccination Certificates on Social Media Indonesia (March 19, 2021)

Communication and Informatics Minister Johnny G. Plate has urged people to not upload their COVID-19 vaccination certificates on social media platforms to ensure protection of personal data. Apart from refraining from posting on social media, Plate also called on the public to not share scans of the vaccination certificates with those around them.

Government Asks for Views on COVID-19 Certification UK (March 18, 2021)

The Government is reviewing whether COVID-status certification could play a role in reopening the economy, reducing restrictions on social contact, and improving safety. COVID-19 status certification involves using testing or vaccination data to confirm in
different settings that people have a lower risk of transmitting COVID-19 to others. The complex issues of ethics, privacy, and inclusion are to be fully considered during the review.


Prompted by the easing of lockdown and the re-opening of businesses, the Information Commissioner's Office (ICO) has outlined 6 key steps that organizations need to consider when using personal data. The Guidance is in keeping with data protection principles under the GDPR and the Data Protection Act 2018 and serves as a useful summary for employers.

**Government Made Mistake by Not Being Upfront About TraceTogether's Use in Criminal Probes** Singapore (March 15, 2021)

TraceTogether, which identifies people in close contact with a COVID-19 patient via Bluetooth, came under the spotlight earlier in 2021 when it was revealed that its data could be used for criminal investigations, despite earlier assurances that it would be used solely for contact tracing. The Government has said it was a mistake to not be upfront about how TraceTogether data can be used for criminal investigations, but it has since passed a law to restrict its use to serious crimes and has ensured that it will delete the information after the pandemic is over.

**Microsoft Could be Set for a US Government Windfall** U.S. (March 15, 2021)

Nearly a quarter of the COVID-19 relief funds set aside for cybersecurity defenders will be going to Microsoft. Some US lawmakers have voiced concerns that they don't want to increase funding for the company after it suffered two high-profile hacks. As first reported by Reuters, Congress allocated the funds in its new COVID-19 relief bill after two major cyberattacks took advantage of weaknesses in the software giant's products to penetrate the computer networks of government agencies as well as those at tens of thousands of companies. Not only do these two hacks pose a major national security threat for the US, but lawmakers also say that Microsoft's faulty software is making the company more profitable.

**HRW Calls for Repeal of Malaysian Government Ordinance Sanctioning the Spread of Fake News** Malaysia (March 14, 2021)

The NGO Human Rights Watch (HRW) has requested to repeal a new Malaysian Government ordinance punishable by up to six years in prison and fines of 500,000 ringgit (100,000EUR) to those who disseminate false information about the pandemic and COVID-19. NGO have said that the ordinance poses a serious threat to freedom of expression and privacy and the right to a fair trial.