DataGuidance Daily News Report

16 November, 2016 | created by DataGuidance

Hong Kong: PCPD clarifies companies' processing of employees' Octopus card data

Nov 16, 2016 12:00AM

The Privacy Commissioner for Personal Data ('PCPD') issued, on 14 November 2016, its response to an enquiry on the collection and use of employees' personal data relating to Octopus cards, which are used for making payments and accessing public transport, and employee monitoring activities by franchised bus companies. The PCPD stated that it has not received complaints from any individual employees so far, and will make any future decisions on a case by case basis.

In addition, the PCPD clarified that bus companies should comply with data protection principles 1 and 3 of the Personal Data (Privacy) Ordinance 1997, which govern the collection and processing of data. Furthermore, the PCPD explained that bus companies may be exempted from notifying employees of their processing activtities provided that the collection is for investigation of improper behaviour and that obtaining consent in advance may contradict this purpose.

You can read the press release here, only available in Chinese.

USA: DHS publishes strategic principles for IoT security

Nov 16, 2016 12:00AM

The U.S. Department of Homeland Security ('DHS') published, on 15 November 2016, a set of Strategic Principles for Securing the Internet of Things ('IoT') ('the Principles') and a fact sheet on the IoT ('the Fact Sheet'). The Principles outline best practices 'to fortify the security of the IoT and […] make responsible and risk-based security decisions as [stakeholders] design, manufacture, and use internet-connected devices and systems.'

In particular, the Principles set out rules on how to address IoT security challenges. Stakeholders, including IoT developers, IoT manufacturers, service providers, as well as industrial and business-level consumers, are advised to incorporate security at the design phase, advance their IoT security updates and vulnerability management, adopt recognised security practices (e.g. the National Institute of Standards and Technology's Cybersecurity Risk Management Framework), prioritise security measures according to their potential impact, promote transparency among the IoT industry, and scrutinise their IoT connections.

You can read the press release here, the Principles here and the Fact Sheet here.

Senegal: CDP releases rules on video surveillance in the workplace

Nov 16, 2016 12:00AM

The Senegalese data protection authority ('CDP') released, on 11 November 2016, rules regarding the installation and operation of video surveillance systems in the workplace ('the Rules'). Organisations are required under the Rules to seek authorisation of video monitoring specifying the purpose and location of the monitoring.

Requirements relating to data retention and data security are included in the Rules. In addition, the Rules contain specific provisions setting out restrictions on installing surveillance cameras in locker rooms, toilets, employee work stations and staff rooms.

According to the Rules, notice should be provided to all employees about video monitoring. This notice must be in the form of a visible sign displayed on the premises that states the existence of the surveillance system, the name of the system manager, the authorisation receipt by the CDP and contact details for subject access requests.

You can read the Rules, in French only, here.

South Korea: Supreme Court clarifies wiretapping evidence admissibility in KakaoTalk case

Nov 16, 2016 12:00AM

DataGuidance confirmed with Hyun-Jeong Kang, Partner at Shin & Kim, on 16 November 2016, that the Supreme Court of South Korea ruled that conversations via Kakao Corp's KakaoTalk app and stored on its servers are not admissible as wiretapping evidence because the data was not seized in real time.

According to Kang, "The Protection of Communications Secrets Act 2002 regards wiretapping as seizing the conversation in real time along telecommunications, not as the subsequent disclosure of conversations saved in servers […] Therefore, it is illegal to

acquire the conversation by issuing a wiretapping warrant, and accordingly any illegally-taken evidence is inadmissible in court."

Kang added, "The data saved in servers can actually be acquired by issuing a search and seizure warrant, so investigation agencies generally prefer issuing wiretappong warrants for intercepting conversations. Notification in advance is, however, required prior to the execution of a search and seizure warrant […] Following the court's decision, telecommunication operators or Over-The-Top service providers without technical means to seize conversations in real time, such as KakaoTalk, do not have to provide conversations to the prosecution as wiretapping evidence."

Canada: CRTC introduces regulatory policy on filtering unsolicited communications

Nov 16, 2016 12:00AM

The Canadian Radio-television and Telecommunications Commission ('CRTC') announced, on 7 November 2016, a regulatory policy ('the Policy'), which introduces requirements for telecommunications service providers ('TSPs') and the CRTC Interconnection Steering Committee ('CISC') to develop policies to help citizens filter unsolicited calls.

In the Policy, the CRTC discussed several regulatory options for filtering telemarketing calls. It concluded that universal blocking of nuisance calls across networks would 'unduly limit the ability of legitimate telemarketers to conduct business,' and that the telecommunications industry should provide citizens with the tools to manage nuisance calls. In particular, the Policy requires TSPs to report to the CRTC with 'details on the opt-in filtering service(s) they offer or propose to offer to their subscribers' within 180 days of the announcement. Moreover, the Policy obliges CISC to 'develop practices to block blatantly illegitimate calls at the network level' within 90 days.

You can read the Policy here.

Netherlands: PDA publishes guidance on employees' sickness leave systems

Nov 16, 2016 12:00AM

The Personal Data Authority ('PDA') published, on 15 November 2016, clarifications on the use of absence/sickness leave systems by employers ('the Clarifications').

Wouter Seinen, Partner at Baker & McKenzie Amsterdam N.V., told DataGuidance, "The [Clarifications] deal with the specific legal situation in the Netherlands where sick employees are monitored and assisted by a doctor/ health care personnel ('HCP') that is independent from the employer, but yet paid by the latter. Employers use such systems to log absence, and all relevant data of when an employee was sick, how he/she is recovering, etc. Such systems can be deployed by the employer; other systems are operated by the HCP or its processors. In the latter case, the employee data may be recorded in the system, provided that only the HCP has access to medical data. The employer may have the possibility to upload data or communicate with the HCP but must not have access to the files. If the employer is using its own system, it may not collect any medical data in that system, just the absence data."

You can read the Clarifications, only available in Dutch, here.

USA: NIST publishes standard on systems security engineering

Nov 1, 2016 12:00AM

The National Institute of Standards and Technology ('NIST') published, on 14 November 2016, the final version of its Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems ('the Standard'). The Standard includes recommendations on ways to incorporate security principles and concepts into information technology systems throughout their entire lifecycle.

In particular, the purpose of the Standard is to address 'the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems.'

You can read the press release here and the Standard here.