

Case No. 2

1. On Time Software Pte. Ltd. is a software developer of a payroll software application, called "PayMeOnTime". Between March and April 2020, it was discovered that the personal data of the current and former employees of three organisations that directly and indirectly used the PayMeOnTime software had been exposed online on On Time Software's servers and could be found using the Google search engine. These organisations are KnowItAll LLP, Hedge Fund LLP and IT Vendor Pte. Ltd.
2. KnowItAll runs the PayMeOnTime software on its own servers within its own premises. In connection with an IT project to add customized functionality to the PayMeOnTime software, it contracted with On Time Software to develop the extra functionality and provided real employee data to On Time Software to do the testing and development work. There was nothing in the contract that would've imposed any specific regulations on On Time Software's treatment of the employee data. However, KnowItAll relied upon a privacy statement provided by On Time Software that its staff would handle all personal data with care and would retrieve data from the system only with the consent of On Time Software's clients. There was nothing in the statement that spoke to any minimum security measures that On Time Software had to implement or any obligation in relation to data storage.
3. HR MNC Pte. Ltd. is a provider of human resource professional services, including management of payroll operations for its clients. Hedge Fund and IT Vendor hired the services of HR MNC to manage payroll for their employees. As a result, Hedge Fund and IT Vendor provides their employee data to HR MNC on a regular basis.
4. HR MNC is a multinational company that has adopted and implemented a global personal data protection policy, data protection statements that are compliant to the EU General Data Protection Regulation and comprehensive written on data processing and protection that set out the duties and obligations and the roles and responsibilities that HR MNC has with regards to the personal data that it processes on behalf of its clients (the "**Contracted Obligations**"). In HR MNC's contracts with each of Hedge Fund and IT Vendor, HR MNC promised to process the data in accordance with its Contracted Obligations.
5. HR MNC licenses PayMeOnTime from On Time Software to provide a subset of the HR MNC services to Hedge Fund LLP and IT Vendor Pte. Ltd. HR MNC wanted to engage On Time Software to provide data migration services and to develop new functionality within the PayMeOnTime application for Hedge Fund and IT Vendor in 2015 (the "**Tool Development Project**"). To that end, HR MNC provided Hedge Fund and IT Vendor's employee data (the "**Hedge Fund and IT Vendor Data**") to On Time Software. On Time Software completed the Tool Development Project in December 2015.
6. HR MNC's contract with On Time Software concerning the Tool Development Project consisted of a series of emails that confirmed the specification, deliverables, timeline and price.
7. All of the employee data handed over to On Time Software by KnowItAll and HR MNC (including Hedge Fund and IT Vendor Data) was stored in a File Server System ("**FSS**"). At some point in February 2020, a hard disk failure affected the FSS. To remediate this, On Time Software restored a backup of the data in the FSS at the end of February 2020 and reset the FSS operating system settings to their default settings, which included disabling the password. As

the FSS was accessible over the Internet, the employee data that was stored in the FSS was exposed to web crawlers and indexed by the Google search engine and stored in Google's cache.

8. In total, 1,000 unique sets of data were exposed. The data included: name, NRIC, marital status, nationality, race, residential address, contact number, work designation, duration of employment, base salary, bank account information, income tax account number and mobile number.

QUESTIONS

1. Which sections of the PDPA did On Time Software breach?
2. Which sections of the PDPA did KnowItAll breach?
3. Which sections of the PDPA did HR MNC breach?
4. Which sections of the PDPA did Hedge Fund and IT Vendor breach?
5. What could they have done to prevent each such breach?
6. Do you think that the data that was breached required a higher degree of security arrangement? Why or why not?