Personal Data Protection Act Guideline on Vehicle GPS Tracking in Logistics Industry through Legitimate Interest Assessment

Natdanai Homkong
Department of Industrial Engineering
Faculty of Engineering, Chiang Mai University
Chiang Mai, Thailand
natdanai_homk@cmu.ac.th

Rajayudt Laothong, CIPP/E
Gradient Group Co., Ltd.
Chiang Mai, Thailand
rajayudt.laothong@gmail.com

***Abstract*— In this digital era, vehicle GPS tracking has been implemented to improve the performance and efficiency in logistics industry where vehicle needs to travel across the land and countries from one location to another in order to deliver goods and services. Various data, including driver's behavior and personal data, has been collected to use as a tool and catalyst to promote growth and enhance the logistic operational system. As a global trend of digital transformation emerges, countries around the world are setting rules and regulations on how to process personal data to protect data subject fundamental right and freedom. As a part of a growing economy, Thailand has implemented Personal Data Protection Act (PDPA), B.E. 2562 (2019) which went into effect on the 1st of June 2022. PDPA brought a new set of rules to protect data subject fundamental right and freedom by regulating how organization process personal data. As vehicle GPS tracking collects personal data, PDPA is applied. Thus, organization with such technology needs to assess and determine the line of work in compliance to PDPA through legitimate interest assessment.**

Keywords*— *Personal Data Protection Act, PDPA, Vehicle GPS Tracking, logistics, legitimate interest, legitimate interest assessment

I. INTRODUCTION

Efficiently allocating resources and time are one of the main features that will promote any businesses. For logistics industry, effective transportation and logistics have become a valuable part in the logistics system. Technology, such as vehicle GPS tracking, is one of the tools that can be used to increase the efficiency of the operation and reduce unnecessary cost in order to increase the organization profit margin and create a sustainable business. With vehicle GPS tracking being widely used and affordable, logistics company can understand more about the activity of the driver, the route that has been taken, the time took to deliver goods and services and how the business can be improved. The technology can assist organization in fleet management operation and reduce transportation time and distance [1,2]. However, such technology can hinder the fundamental right and freedom of the data subject and cause and infringement of PDPA.

II. PERSONAL DATA PROTECTION ACT

PDPA is a new set of law that the Thai government decide to implement in order to promote data protection to data subject and align data protection act with other countries. It can be defined as a law that protect human rights and fundamental freedoms. The European Convention on Human Rights (ECHR), an international treaty to protect human rights and fundamental freedoms, define human rights as

"the right to respect for his private and family life, his home and his correspondence". [3]

Thus, invading personal space through personal data or using personal data as a marketing tool without the consent or permission of the data subject is equivalent to invading data subject fundamental human rights and freedom.

By law, all organizations that handle personal data in Thailand are required to comply with the PDPA. Non-compliance may lead to trade barrier from other countries and result in criminal penalty, civil penalty and administrative fine. Without the vehicle GPS tracking, logistics industry is one of the industries that involves processing personal data from data subject around the world, with personal data from clients, employee and partners. Furthermore, to secure a smooth operation, these personal data will be processed and circulate with other department within the organization and outside to suppliers and vendors to deliver goods and services. Hence, there is a risk in process personal data.

III. DATA PROTECTION PRINCIPLE

All organization should complied to data protection principle in order to demonstrate an accountability towards PDPA. The data protection principles include lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability.

Under the PDPA, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Lawfulness means that personal data must only be processed when data controllers have a legal ground for processing the data. For example, logistics company can collect the information of its clients to create a contract. In this case, the personal data is being process lawfully using contract as a legal ground. This enforces the data controller to limit when the personal data can be processed. In addition to being lawful, the processing of personal data must be fair which means that the data subject must know how their personal data will be processed. The logistics company can inform all data subject through privacy notice at the point where the personal data is being collected. Directly linked to fairness, the principle of transparency means that a controller must be open and clear towards data subjects when processing personal data by providing clear and easily accessible information. Thus, the logistics company needs to allocate channels for data subject to exercise their right such as the right to object or the right to assess their personal data.

The data controllers must identify the specific purposes for which personal data is being collected and process. Therefore, the logistics company only can collect the data if there is a purpose. The company cannot collect as many data as possible without specific purposes. This will reduce the amount of data collected by the company and the company will only collect necessary data. Furthermore, the data controllers must only collect and process personal data that is relevant, necessary and adequate to accomplish the purposes for which it is processed.

For every collection of data, the data controllers must take reasonable measures to ensure the data is accurate. An inaccurate data can give a misleading information and can create a negative cause to the data subject. If the delivery information in delivering goods and services is inaccurate, this can cause the delay in the delivery and cost the clients time and money.

In the face of data retention period, the data controllers must verify whether statutory data retention periods exist in relation to the type of processing. The personal data must not be kept for longer than necessary for the purposes for which the personal data is processed. Therefore, once the information is no longer needed, personal data must be securely deleted in the system. In protecting the personal data, data controllers must implement an information security policy framework to prevent from possible data breach and data leakage. To summarize, the data controllers must be able to demonstrate compliance to show its accountability to PDPA [4].

IV. VEHICLE GPS TRACKING

Vehicle GPS Tracking is a technology that track the movement of the vehicle, not the movement of a person. The technology has been deployed in business of all sizes in logistics industry mainly to secure the property of the company and to monitor the behavior and the activity of the employee. Such technology gives the data controller the actionable data to improve their operational system. With the track record of trip and the vehicle footprint, the organization can plan on the route to reduce the cost of fuel and time spent on the road. The GPS tracking data also help organization in increase the service performance by creating an expectation of arrival time. Furthermore, in the case of accident or robbery, this technology can warn the owner about such incident. Thus, it can be deemed as a necessary tools to help logistic industry flourishes.

In Thailand, vehicle GPS tracking can be seen as necessary in comparison to other countries. According to the World Health Organization, Thailand has one of the most dangerous roads to drive in the world with about 20,000 people die in the road accidents each year [17]. [18] believes that vehicle GPS tracking is one of the technologies that can reduce the road accident. With the large amount of information from the technology, the authority or the government can use the data to analysis the sudden break of the vehicle, the optimal speed on the road, rest area analysis and the starting and ending points of the vehicle. However, the information from the technology demonstrates a processing of personal data.

Data gathers from vehicle GPS tracking includes personal data. Location data is considered personal data [5]. On the same hand, geographical information is a connector node that connects all data together such as consumer behavioural data, financial data and health data which can also be seen as a personal data. Without a proper data security, the information then can be used to form a direct marketing based on data subject location and behaviour causing the risk of fundamental human rights and freedom breach. Leading back to data protection principles, all data must have a specific purpose and limitation to how the data can be processed.

For the vehicle GPS tracking activity, there are two legal ground that can be considered consent and legitimate interest. However, given the imbalancing of power between the employee and the employer, consent is not suitable. Hence, rejecting to give consent can cause the employee to loss their job or being treated unfairly in the workplace [6]. Thus, following Opinion 2/2017 [1], it is said that in the employment context the personal data process should be legitimate by legal grounds different from consent.

V. LEGITIMATE INTEREST

The legitimate interest can be is stated in Article 24 (5) that

" The Data Controller shall not collect Personal Data without the consent of the data subject, unless it is necessary for legitimate interests of the Data Controller or any other Persons or juristic person other than the Data Controller, except where such interests are overridden by the fundamental rights of the data subject of his or her personal data." [4]

When using legitimate interests as a lawful basis for processing personal data, the data controller must conduct a legitimate interest assessment (LIA) [7] and keep a record of it to ensure that the employer decision to process personal data is justify. By using LIA, the employer is demonstrating compliance in line with their accountability.

In the Opinion 249/2017, it is outlined that the use of GPS tracking system must be assess on its necessary and whether the actual implementation complies with the principles of proportionality and subsidiarity [8]. Thus, LIA is designed to assist the data controller to decide whether or not the legitimate interest basis is likely to apply to such processing.

VI. LEGITIMATE INTEREST ASSESSMENT

To perform LIA, the data controller needs to be able to do three tests [9]:

1) Purpose Test – the data controller needs to assess whether there is a legitimate interest behind the processing. This includes the reason for processing the data, the benefit for the data controller and third parties, how the process is complying with other relevant laws and in line with any other ethical issues with the processing. This test provides the data controller the checklist whether it is align to the data protection principle or not.

2) Necessity Test – the data controller needs to assess whether the processing is necessary for the purpose the data controller have identified. This includes whether the

processing of personal data is proportionate to the purpose, are there are ways to achieve such purpose without the processing of the personal data and can the data controller achieve the same purpose by processing less data or by processing the data in another more obvious or less intrusive way that comply to the data protection principles. In some cases, there might be other technology or method that can solve the problem instead of processing personal data. Thus, this test reconfirm with the data controller on how importance is the method.

3) Balancing Test – the data controller needs to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides the data controller legitimate interests. This includes assess whether childen's data is being process, whether the data subject can expect the processing of data, what is the impact of the processing on the people and what is the likelihood and severity of any potential impact. This test concerns about whether the processing of the personal data is not more than what the data subject expected and does not hinder their fundamental rights and freedom.

Overall, the results from these three tests will assess the impact towards the data subject relative to their fundamental right and freedom and illustrate whether it is necessary to use legitimate interest basis instead of other legitimate ground.

Furthermore, LIA involves evaluating and balancing the benefits between the data subject and the data controller, employee and employer respectively. The data controller needs to make sure that the processing of such data is beneficial to the human beings rather than the organization [10].

VII. LEGITIMATE INTEREST ASSESSMENT ON VEHICLE GPS TRACKING

1) Purpose Test: The data controller wants to process the data to reduce costs and increase efficiency in the operational system. By installing the Vehicle GPS tracking, the data controller can optimize its resources, boost productivity, plan route, bolster security and prevent theft. Therefore, the third parties or the customers can gain cheaper and better services. Without the Vehicle GPS Tracking, there is a risk of losing the asset and fail to deliver the goods and services to its clients. This can lead to losing in business.

There might be the risk of over collecting personal data, such as non-working hour and when the data subject uses the vehicle for private-use. This can be seen as profiling or monitoring of the data subject behavior.

2) Necessity Test: By applying the vehicle GPS tracking, the data controller can locate where its asset is. The other alternative to the method of tracking is to track through other asset such as mobile phone or GPS tracking tag. However, it might not 100% locate the whereabout of the vehicle in the case where the mobile or the GPS tracking tag leave the vehicle.

Another alternative to any tracking device is having the data subject or the employee to report on their location on a certain time or certain checkpoint. This allows the data subject to inform the data controller by themselves. The recording is not done automatically but manually. Therefore, there is a chance of not reporting the data. Furthermore, manually reporting might not be solution when the vehicle is driving out of the suggested zone or destination. The vehicle can be lost without the data controller knowing or being notice which can cause the company to loss out their assets.

In collecting data, the data controller needs to ensure that only the location data is being collected to comply with the data ministration principle, only use the location data for ethical purposes to comply with purpose limitation, inform all data subject about the activities to comply with lawfulness and transparency and keep record of all activity to show its accountability.

3) Balancing Test: Using vehicle GPS tracking will not harm the privacy of the data subject if other personal data is not being processed. The vehicle GPS tracking shall be used only during working hours and shall not be used during leisure time of the data subject. The drive of the company will be notified about the GPS tracking before driving and working for the company.

Vehicle GPS tracking is widely used in the logistics industry. Therefore, it is something that all driver will be expected. In the case where the data subject wants to exercise their data subject right, the data subject can do so to the data controller and the data controller has the responsibility to response to the request and explain how their personal data is being processed.

VIII. DISCUSSION

Vehicle GPS Tracking has been deployed all around the world and in the place where data protection law has been enforced. In Spain, the Spanish Supreme Court states that the employer is deemed lawful to use the data from the GPS tracking if the employee is informed beforehand about the installation of the device, the vehicle is being used for working activities and the data collected by the device includes only the information on the movement and location of the vehicle not the behavior of the employee [11]. Similarly in New Jersey [12], the employee privacy law prohibits employers using any tracking device without written notice to the employee. This can be seen as non-transparent and the employee losses their right to be informed.

On the other hand, in Austria [13], the Supreme Court concludes that the GPS tracking qualified as a control measure – can be defined as the systematic monitoring of an employee's actions, conduct and traits by their employer. The employee (plaintiff) states that the employer (defendant) is invading his privacy causing emotional distress due to GPS tracking on the company car which the plaintiff uses during both in the on and off working hours. The defendant (employer) asserted that the employee knew about the GPS tracking and its purpose, the employee had agreed to its use, and the GPS tracking was necessary for an efficient fleet management and deployment of the employer's resources. However, employees cannot validly consent to a control measure that violates human dignity, such as during non-working hours. Thus, GPS tracking was unlawful.

Overall, there is a limit to how Vehicle GPS Tracking can be implemented correctly. [14] suggests that:

1) Vehicle GPS Tracking will only be implemented on the company's asset and not use to track the employee;

2) Vehicle GPS Tracking will only be used to collect location data and not the behavior of the data subject, only necessary information should be gathered;

3) Vehicle GPS Tracking will only be activated during the working hour of the data subject and not operate during their non-working hour. It should be able to switch on and off by the employee after working hours;

4) The data controller must inform the data subject about such activity, its policy, when and how the data subject should expect to be monitored and how the data controller will use and safeguard data collected. This will comply to the data protection principle of lawfulness and transparency *[15]*.

In the event of disagreement or proof of assessment, the data subject can exercise its right to object the processing of his or her personal data. Article 32 states that

"The data subject has the right to object the processing of their personal data. Therefore, once they exercise their right to object, the data controller needs to pause the processing their personal data and demonstrate the reason behind processing the data and what lawful legal basis they are using to process such data [4]."

Therefore, the data controller needs to keep record of the LIA. Once the data subject exercise her right to object, the data controller can inform them about the LIA.

IX. Conclusion

GPS tracking is legal with some limitation to how the data controller processes the personal data. The data controller needs to keep in mind that there should be a limit to the time and location when tracking takes place to minimize the risk of monitoring data subject during their non-working hour and into their personal space. Furthermore, it would be best for the data subject to be able to switch tracking off easily when the employee is using the vehicle outside of their working hour.

LIA is one of the tools that the data controller can used to assess the use of legitimate interest. Another tool that can be implemented to assess risk is Data Protection Impact Assessment (DPIA). DPIA is required by GDPR in some cases such as systematic monitoring or involve new technology. However, in Thailand, the PDPA does not expressly provide for DPIAs. However, Article 37(1) outlines that data controllers have a duty to provide appropriate security measures and review them when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards.

In the case of data breach, each organization needs to have a breach response incident plan as stated in PDPA Article 37(4). The PDPA states that data controllers and data processors must provide appropriate security measures in order to prevent the loss, access, use, change, revision, or disclosure of personal data without authorization. A personal data breach must be notified to the PDPC without undue delay and, where feasible, no later than 72 hours after having become aware of the breach. Therefore, each organization needs to be prepared for all circumstances.

We believe that in the near future the Personal Data Protection Committee (PDPC) will announce more about how to assess LIA and the procedure to perform risk assessment or what other assessment needs to be done to comply with PDPA [16].

References

[1] Article 29 Working Party, "Opinion 249/2017 on data processing at work," 8 June 2017. [Online]. Available: https://t.co/FNH77m3b5B.

[2] K. Michael, A. McNamee and M. G. Michael, "The emerging ethics of humancentric GPS tracking and monitoring," International Conference on Mobile Business, 2006, pp. 1-10.

[3] S. Rudgard, "Origins and Development of European Data Protection Law," in European Data Protection 2nd Edition, The International Association of Privacy Professional Publication, 2019, pp. 17-49.

[4] Ministry of Digital Economy and Society, "Personal Data Protection Act, B.E.2562 (2019)," Government Gazette, no.136 Chapter 69 Gor, May. 2019.

[5] Article 29 Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices," 16 May 2011. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

[6] C. Ogriseg, "GDPR and Personal Data Protection in the Employment Context," Labour & Law Issues, vol. 3, 2017.

[7] Information Commissioner's Office, "Legitimate Interests," in Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office, 2021, pp. 76-81.

[8] Article 29 Working Party, "Opinion 5/2005 on the use of location data with a view to providing value-added services," 25 November 2005. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion- recommendation/files/2005/wp115_en.pdf

[9] I. Kamara and P. De Hert, "UNDERSTANDING THE BALANCING ACT BEHIND THE LEGITIMATE INTEREST OF THE CONTROLLER GROUND: A PRAGMATIC APPROACH," Brussels privacy hub, vol. 4, no. 12, Aug. 2018.

[10] C. A. Tschider, "AI'S LEGITIMATE INTEREST: TOWARDS A PUBLIC BENEFIT PRIVACY MODEL," Houston Journal of Health Law & Policy, no. 21, 2021, pp. 125-184.

[11] Consejo General Del Poder Judicial, "The Judicial Documentation Centre (CENDOJ)," September 2020. [Online]. Available: https://www.poderjudicial.es/search/openDocument/8adba1406c95ebc3. [Accessed 03 11 2020].

[12] Robinson+Cole's Data Privacy & Cybersecurity Team, "Robinson+Cole," 1 April 2022. [Online]. Available: https://www.dataprivacyandsecurityinsider.com/2022/04/tracking-employees-with-gps-new-jersey-law-requires-employers-to-give-written-notice-to-employees-before-using-a-tracking-device-in-employee-vehicles.

[13] J. Widner, "Supreme Court rules on compensation for illegal GPS tracking," 16 September 2020. [Online]. Available: https://www.lexology.com/commentary/employment-immigration/austria/graf-isola-rechtsanwlte-gmbh/supreme-court-rules-on-compensation-for-illegal-gps-tracking.

[14] E. Austermuehle, "Greensfelder Attorneys at Laws," 18 Feburary 2016. [Online]. Available: https://www.greensfelder.com/business-risk-management-blog/monitoring-your-employees-through-gps-what-is-legal-and-what-are-best-practices.

[15] Data Protection Commission, "Employer Vehicle Tracking," May 2020. [Online]. Available: https://www.dataprotection.ie/en/dpc-guidance/employer-vehicle-tracking.

[16] Article 29 Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices," European Commission, 2011.

[17] J. Sukruay, "Road Accidents Biggest Health Crisis," 11 November 2020. [Online]. Available: https://www.bangkokpost.com/opinion/opinion/2017727/road-accidents-biggest-health-crisis.

[18] P. Rungruangvirojin, A. Sumalee, W. Ngamsorn, N. Chankaew and T. Threepak, "Trends and Development of GPS Technology for Road Safety in Thailand," Thailand Development Research Institution, March 2017, vol. 32, no. 1.