

อาชญากรรมคอปกเสื้อขาว: แนวทางการป้องกันและดำเนินคดีภายใต้ข้อจำกัด
ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
White Collar Crime: How to Prevent and Take Legal Actions under the
Personal Data Protection Law Implications

อนุวัฒน์ งามประเสริฐกุล*
Anuwat Ngamprasertkul

วันที่รับบทความ 8 สิงหาคม 2563; วันที่ไขบทความ 25 กันยายน 2563; วันที่ตอบรับบทความ 5 ตุลาคม 2563

บทคัดย่อ

อาชญากรรมคอปกเสื้อขาว (White Collar Crime) เป็นอาชญากรรมทางเศรษฐกิจที่ตรวจสอบพบมากขึ้นในปัจจุบัน และเป็นอาชญากรรมที่ส่งผลกระทบต่อชื่อเสียง เงินทอง และความเชื่อมั่นต่อนักลงทุนและบุคคลภายนอก และรวมไปถึงขวัญกำลังใจของพนักงานเป็นอย่างมาก โดยที่การกระทำความผิดประเภคนี้นักกระทำโดยผู้บริหารระดับสูง หรือพนักงานที่อยู่ภายในองค์กรเป็นระยะเวลานาน โดยอาศัยช่องว่างที่ตนเองมีอำนาจหน้าที่ที่สามารถเข้าถึงข้อมูล ทำการแก้ไข ดัดแปลง ทำการใด ๆ รวมถึงการอนุมัติให้สิ่งที่ไม่ถูกต้องเป็นสิ่งที่ถูกต้อง เพื่อที่จะให้เกิดผลประโยชน์กับตนเองหรือพวกพ้อง ซึ่งการทุจริตโดยอาศัยตำแหน่งหน้าที่ (Occupational Crime) นี้ มักจะใช้วิธีที่แยบยล หรือซับซ้อนเพื่อปกปิดความผิดของตน หรือทำให้ยากต่อการตรวจสอบ ซึ่งตัวอย่างของอาชญากรรมคอปกเสื้อขาว ได้แก่ การตกแต่งบัญชีโดยผู้บริหารเพื่อให้บริษัทมีมูลค่าสูงขึ้น การสมรู้ร่วมคิดระหว่างพนักงานกับคู่ค้าอันเนื่องมาจากผลประโยชน์ทับซ้อน (Conflict of Interest) เป็นต้น

ต้นเหตุของอาชญากรรมคอปกเสื้อขาวมีการวิจัยและวางหลักการไว้เกี่ยวกับ สามเหลี่ยมทุจริต (The Fraud Triangle) ซึ่งประกอบไปด้วยปัจจัย 3 ประการที่สำคัญ ได้แก่ ความกดดันหรือแรงจูงใจ (Motivation) โอกาสในการกระทำความผิด (Opportunity) และการมีข้ออ้างหรือเหตุผลที่ทำให้ผู้กระทำความผิดรู้สึกดีขึ้น (Rationalization) ด้วยเหตุนี้ บริษัทโดยส่วนใหญ่จะมีการกำหนดนโยบายสำหรับมาตรการเชิงป้องกัน และป้องปรามเพื่อมิให้เกิดเหตุทุจริตขึ้นภายในองค์กร เช่น การแจ้งเบาะแสการกระทำผิด (Whistle Blowing) การตรวจสอบประวัติอาชญากรรมของผู้สมัครงาน การตรวจสอบพฤติกรรมและประวัติของผู้สมัครงาน การตรวจสอบการขัดกันของผลประโยชน์ระหว่างพนักงานกับบุคคลภายนอกที่มีความสัมพันธ์กับองค์กร การสืบสวน และสอบสวนพนักงานและผู้กระทำผิดที่เกี่ยวข้องการดำเนินคดีแรงงาน คดีแพ่ง และคดีอาญา อย่างจริงจัง เพื่อลดโอกาสในการกระทำความผิดลง

* หุ้นส่วน และหัวหน้าส่วนคดีและการรับข้อพิพาท บริษัท บลูเมนทอล ริชเตอร์ แอนด์ สุมธ จำกัด
ที่อยู่ : บริษัท บลูเมนทอล ริชเตอร์ แอนด์ สุมธ จำกัด เลขที่ 990 อาคารอับดุลราฮิม เฟส 31 ห้อง 3101
ถนนพระรามสี่ แขวงสีลม บางรัก กรุงเทพมหานคร 10500
Email : anuwat@brslawyers.com

แต่อย่างไรก็ตาม ประเทศไทยได้มีการอ้างอิงหลักการของ “General Data Protection Regulation” (GDPR) ซึ่งเป็นกฎหมายของสหภาพยุโรปว่าด้วยมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล โดยได้นำมาประกาศใช้เป็นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) ในราชกิจจานุเบกษาไปเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 และจะมีผลบังคับใช้อย่างเต็มรูปแบบในวันที่ 1 มิถุนายน พ.ศ. 2564 เป็นต้นไป ซึ่งกฎหมายนี้จะควบคุมบริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของผู้สมัครงาน/พนักงาน/อดีตพนักงาน/คู่ค้า และบุคคลอื่น ๆ ที่บริษัทได้นำมาใช้เพื่อดำเนินการตามมาตรการเชิงป้องกันและป้องปรามเพื่อมิให้เกิดเหตุทุจริตขึ้นภายในองค์กรนี้ ด้วยเหตุดังกล่าว การรักษาสมดุลระหว่างการป้องกันและปราบปรามเหตุทุจริตภายในองค์กร และการคุ้มครองข้อมูลส่วนบุคคลจึงต้องดำเนินการต่อไปด้วยความระมัดระวังมากขึ้น เพื่อมิให้เกิดคดีความฟ้องร้องกับบริษัท ซึ่งอาจรวมไปถึงการดำเนินคดีแบบกลุ่ม อันเนื่องมาจากการกระทำความผิดที่กระทบกับข้อมูลส่วนบุคคลจำนวนมาก อันขัดกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

คำสำคัญ: อาชญากรรมคอปกเสื้อขาว, สามเหลี่ยมทุจริต, การแจ้งเบาะแสการกระทำผิด, การขัดกันของผลประโยชน์, กฎหมายคุ้มครองข้อมูลส่วนบุคคล

Abstract

White collar crime is an economic crime that is increasingly coming under investigation. It is an offense that can affect a company's reputation and trustworthiness in the eyes of investors and other third parties, and it can reduce employee morale and cause financial loss. This kind of offense is usually committed by senior management or employees who have been part of the organization for a long time, by relying on gaps in which they have the authority to access information and make modifications, including approving erroneous things as correct for personal gain. Ingenious or complicated methods are often used to conceal one's mistakes or make them difficult to verify. Also known as occupational crimes, examples of white collar crimes include fraudulent accounting practices by executives in order to increase company value, procurement fraud due to a conflict of interest between employees and business partners and so on.

The causes of white collar crime are generally referred to as the Fraud Triangle, which consists of Motivation, Opportunity and Rationalization. Most companies have policies in place to prevent these causes of fraud within the organization, such as whistle blowing, checking any criminal records of job applicants, checking references of job applicants, conducting conflict of interest checks between employees and outsiders who have relationships with the organization, conducting investigations on employees and related offenders and talking about serious civil, criminal and litigation labor cases.

A novel factor in white collar crime in Thailand is the country's introduction of the Personal Data Protection Act (PDPA) which is similar to the European Union's General Data Protection Regulation and will come into full force on June 1, 2021. Under the PDPA, a company will be considered as a personal data controller when it collects uses or discloses the personal data of job applicants, employees, former employees, partners and other persons for the purpose of implementing measures to prevent fraud inside the organization. Therefore, greater caution is needed in the balance between preventing corruption within the organization and protecting personal information in order to prevent counter lawsuits against the company which could even be stepped up to class action litigation.

Keywords: white collar crime, fraud triangle, whistles blowing, conflict of interest, personal data protection act,

บทนำ

อาชญากรรมคอปกเสื้อขาว (White Collar Crime) เป็นคำศัพท์ที่ Mr. Edward Sutherland นักอาชญาวิทยาและนักสังคมวิทยาเป็นบุคคลแรกที่ใช้คำนี้ โดยให้คำนิยามไว้ว่าเป็น อาชญากรรมที่กระทำโดยบุคคลมีสถานะทางสังคมระดับสูงและเป็นที่เคารพนับถือโดยอาศัยโอกาสหรืออาชีพของตนในการกระทำความผิด ซึ่งรวมถึงการกระทำความผิดโดยบริษัทหรือนิติบุคคลอื่นด้วย ซึ่งต่อมา กระทรวงยุติธรรมสหรัฐ (Department of Justice) ได้ให้คำนิยาม White Collar Crime ว่าหมายถึง การกระทำความผิดที่ไม่ใช่ความผิดรุนแรง เพื่อให้ได้ผลประโยชน์ทางการเงิน โดยวิธีการฉ้อโกงของบุคคลหรือคณะบุคคลผู้ซึ่งมีสถานะประกอบอาชีพในฐานะผู้เป็นเจ้าของกิจการ หรือมีวิชาชีพ หรือกึ่งวิชาชีพเฉพาะ โดยใช้วิธีการทั้งหลายซึ่งจะต้องมีความชำนาญ เฉพาะและโอกาสในการกระทำความผิด นอกจากนี้ ยังรวมความถึงการกระทำความผิดที่ไม่รุนแรง เพื่อให้ได้ประโยชน์ทางการเงินโดยใช้วิธีการอันเป็นการฉ้อโกง และกระทำความผิดโดยบุคคลใดก็ตาม ซึ่งมีความรู้พิเศษหรือทางเทคนิควิธีการทางธุรกิจและทางการบริหารงาน โดยไม่คำนึงว่าบุคคลนั้น จะมีอาชีพอะไร ซึ่งตัวอย่างคดีที่พบจะมีดังต่อไปนี้

- ความผิดของบริษัทหรือนิติบุคคลอื่น และปัจเจกบุคคลที่เกี่ยวข้องกับบริษัท
- ความผิดฐานสมคบ (Conspiracy) ที่เกี่ยวกับคดีอาชญากรรมทางเศรษฐกิจอื่น ๆ
- ความผิดเกี่ยวกับการฉ้อโกงโดยวิธีการทางจดหมาย (Mail Fraud) การฉ้อโกงเงินผ่านระบบธนาคาร (Wire Fraud) การฉ้อโกงธนาคาร (Bank Fraud) การฉ้อโกงประกันภัย (Health Care Fraud) และการฟ้องคดีอันเป็นเท็จ (False Government Claims) การแจ้งล้มละลายอันเป็นการฉ้อโกง (Bankruptcy Fraud)
- การฉ้อโกงหลักทรัพย์ (Securities Fraud)
- อาชญากรรมคอมพิวเตอร์ (Computer crime)
- ความผิดเกี่ยวกับสิ่งแวดล้อม (Environmental Crimes)
- การติดสินบนเจ้าพนักงาน (Bribery and Gratuities)
- ความผิดฐานกรรโชก (Extortion)
- การแจ้งความอันเป็นเท็จ (False Statements) โดยเฉพาะความผิดเกี่ยวกับภาษีและความผิดเกี่ยวกับการฟอกเงิน
- การเบิกความอันเป็นเท็จต่อศาล (Perjury)
- ความผิดฐานขัดขวางกระบวนการยุติธรรม (Obstruction of Justice)
- การกระทำความผิดเกี่ยวกับทางภาษี (Tax Crimes)
- การกระทำความผิดเกี่ยวกับการรายงานธุรกรรมทางการเงิน (Currency Transaction Reporting Crimes) ซึ่งเป็นมาตรการที่เกี่ยวข้องกับความผิดในฐานฟอกเงิน
- ความผิดฐานฟอกเงิน (Money Laundering) เป็นต้น¹

¹ ศิริพล กุศลศิลป์วุฒิ, ‘กฎหมายอาชญากรรมทางเศรษฐกิจของสหรัฐอเมริกา’ (Siriphonku's Blog, 27 สิงหาคม 2551) <<https://siriphonku.wordpress.com/2008/08/27>> สืบค้นวันที่ 22 กรกฎาคม 2563

ทั้งนี้ อาชญากรรมคอปกเสื้อขาวในบางครั้งก็จัดให้อยู่ในประเภทอาชญากรรมทางเศรษฐกิจ (Economic Crime) ซึ่งสามารถแบ่งประเภทย่อยออกมาได้อีก 2 กลุ่มใหญ่ ๆ ได้แก่ การทุจริตโดยอาศัยตำแหน่งหน้าที่ (occupational crime) ซึ่งเป็นความผิดที่พนักงานกระทำต่อบริษัท และอาชญากรรมองค์กร (organizational crime) ซึ่งเป็นความผิดที่บริษัทกระทำต่อสาธารณชนหรือลูกค้าของบริษัท²

โดยจากผลการสำรวจเกี่ยวกับการทุจริตและอาชญากรรมทางเศรษฐกิจของ PricewaterhouseCoopers³ ในปี พ.ศ. 2562 ที่ทำการสำรวจบริษัทในประเทศไทยพบข้อมูลเชิงสถิติที่น่าสนใจว่า

- การทุจริตในตำแหน่งหน้าที่ (occupational crime) โดยพนักงานภายในบริษัทมีสัดส่วนมากถึงร้อยละ 59 และระหว่างพนักงานภายในร่วมกับบุคคลภายนอกองค์กรอีกร้อยละ 18 และเมื่อเทียบกับอาชญากรรมที่กระทำโดยบุคคลนอกองค์กรจะมีเพียงร้อยละ 18 จะเห็นได้ว่าการทุจริตในตำแหน่งหน้าที่ (occupational crime) โดยพนักงานภายในไม่ว่าด้วยตนเองหรือร่วมกับบุคคลอื่นจะมีสัดส่วนมากที่สุด
- ตำแหน่งที่ตรวจสอบพบว่ากระทำทุจริตจะเป็นพนักงานระดับปฏิบัติการประมาณร้อยละ 46 ระดับผู้บริหารระดับกลางที่ร้อยละ 35 และผู้บริหารระดับสูงที่ร้อยละ 17
- ความผิดที่เกิดขึ้นและตรวจพบเป็นจำนวนสัดส่วนที่สูงที่สุดคือ ความผิดเกี่ยวกับการฉ้อโกงทรัพย์สิน (Asset Misappropriation) ถึงร้อยละ 62 ซึ่งสูงขึ้นกว่าผลสำรวจในปี พ.ศ. 2561 ถึงร้อยละ 24 และรองลงมาคือ ความผิดที่เกิดจากการจัดซื้อจัดจ้าง (Procurement Fraud) ในสัดส่วนร้อยละ 33 ซึ่งสูงขึ้นกว่าผลสำรวจในปี พ.ศ. 2561 ถึงร้อยละ 17 และความผิดที่มีสัดส่วนใกล้เคียงกันคือ ความผิดฐานการติดสินบนและคอร์รัปชัน (Bribery and Corruption) ที่ร้อยละ 31 และความผิดฐานการตกแต่งบัญชี (Accounting/Financial Statement Fraud) ที่ร้อยละ 29 ซึ่งสูงขึ้นกว่าผลสำรวจในปี พ.ศ. 2561 ถึงร้อยละ 13 และ 14 ตามลำดับ

โดยที่การกระทำความผิดสำหรับการทุจริตในตำแหน่งหน้าที่เป็นความผิดที่บุคคลภายในใช้อำนาจหน้าที่การทำงานของตนก่อให้เกิดความเสียหายอันมิควรได้ หรือการใช้ทรัพยากรบุคคลหรือทรัพย์สินขององค์กรโดยผิดวัตถุประสงค์ เช่น การค้าหุ้นโดยใช้ข้อมูลภายในเพื่อแสวงหาผลประโยชน์จากการซื้อขายหลักทรัพย์ (Insider Trading Fraud) การฉ้อโกงเงิน (Embezzlement) การทำใบเสร็จรับเงินเท็จ (False Billing Schemes) การทุจริตเกี่ยวกับหลักทรัพย์ (Securities Fraud) การปลอมแปลงลายมือหรือเอกสาร (Forgery) การคอร์รัปชันอันเนื่องมาจากการขัดแย้งทางผลประโยชน์ (Conflict of Interest) โดยเฉพาะในการจัดซื้อจัดจ้าง การทุจริตในงบการเงิน (Fraudulent Statement) ในการตกแต่งบัญชีให้มีสถานะทางการเงินดีกว่าที่เป็นจริง การจ่ายค่าสินค้าหรือบริการที่ไม่มีความจำเป็นหรือสูงเกินจริง (Overinflated invoices or payments for Phantom services) การจ่ายเงินให้กับพนักงานที่ไม่มีตัวตน (Ghost Employees) เป็นต้น

² Sarah Soley, 'White Collar Crime: The Role Of The Firm In Occupational Crime' (University of Pennsylvania, 2017) <https://repository.upenn.edu/cgi/viewcontent.cgi?article=1034&context=joseph_wharton_scholars> assessed 22 July 2020

³ PwC, 'PwC's Thailand Economic Crime and Fraud Survey 2020' (PwC, 2020) <<https://www.pwc.com/th/en/consulting/forensic/assets/GECS-report-2020-th-5.pdf>> assessed 22 July 2020

ทั้งนี้ หากทำการวิเคราะห์ต่อไปถึงมูลเหตุที่ก่อให้เกิดความผิดสำหรับการทุจริตในตำแหน่งหน้าที่ ส่วนใหญ่จะมีมูลเหตุหรือปัจจัยทุจริตหลัก 3 ประการ ที่เรียกว่า สามเหลี่ยมทุจริต (The Fraud Triangle) ได้แก่

- **ความกดดันหรือแรงจูงใจ (Motivation)** เช่น ความกดดันจากการปฏิบัติงาน และความกดดัน และแรงจูงใจส่วนตัว เช่น เป้ายอดขาย ภาระหนี้สิน หรืออุปนิสัยส่วนตัว
- **โอกาสในการกระทำความผิด (Opportunity)** เช่น โอกาสในการกระทำทุจริต โอกาสที่จะปกปิด การกระทำความผิด และโอกาสที่จะแปลงสภาพทรัพย์สินที่ได้จากการทำทุจริต โอกาส ในการกระทำผิดอันเกิดจากจุดอ่อนในการควบคุมภายในที่จะป้องกันและปราบปราม การกระทำทุจริต ขาดการแบ่งแยกหน้าที่ที่มีความเสี่ยงต่อความเสียหายขององค์กร เพื่อถ่วงดุลอำนาจ เป็นต้น
- **ข้ออ้างหรือเหตุผลที่ทำให้ผู้กระทำความรู้สึกดีขึ้น (Rationalization)** เช่น อ้างความเป็น เดือดร้อนส่วนตัว อ้างว่าเป็นประเพณีทางธุรกิจ ไม่ทราบว่าเป็นความผิดเพราะเป็นสิ่งที่ใคร ๆ ก็ทำ หรืออ้างว่าทำเพื่อประโยชน์ส่วนรวม เช่น ตกแต่งงบการเงินให้มีผลกำไรเพื่อให้ผู้ถือหุ้นพอใจ เพราะได้รับเงินปันผลและราคาหุ้นสูงขึ้น หรืออ้างว่าทำเพื่อไม่ให้กิจการล้มละลาย เป็นต้น

ทั้งนี้ การที่จะป้องกันและป้องปรามการเกิดขึ้นของอาชญากรรมคอปกเสื้อขาว จึงควรที่จะพิจารณา ถึงมูลเหตุแต่ละปัจจัยในสามเหลี่ยมทุจริต โดยเฉพาะการกำจัดโอกาสที่จะเกิดขึ้นของการกระทำทุจริต โดยมีขั้นตอนที่สำคัญ ได้แก่

1. **การป้องกัน (Prevention)** การพิจารณาความเสี่ยงจากการทุจริตและหาวิธีป้องกันผ่านระบบ การควบคุมภายในเพื่อไม่ให้เกิดเหตุทุจริตขึ้น เช่น การจัดฝึกอบรมพนักงานและส่งสัญญาณว่ามี การเฝ้าติดตาม ปัญหาการทุจริต

2. **การตรวจจับ (Detection)** การพบทุจริตภายในองค์กรมักจะมาจากการให้ข้อมูลของพนักงาน หรือที่เรียกว่า Whistle Blowing ซึ่งเป็นช่องทางในการแจ้งเหตุทุจริตที่มีประสิทธิภาพ ซึ่งบริษัทต้องสามารถ รักษาความลับและรับรองความปลอดภัยให้กับผู้แจ้งได้

3. **การตอบสนอง (Response)** โดยตอบสนองในรูปแบบต่าง ๆ เช่น บทลงโทษที่เข้มงวดพนักงาน ที่ทุจริตจะต้องรับผิดชอบและถูกฟ้องร้องดำเนินคดีเพื่อเป็นการส่งสัญญาณถึงความจริงจังของฝ่ายบริหาร ขั้นตอนการสืบสวนสอบสวน และการตั้งคณะกรรมการเพื่อหาข้อสรุปต้องมีความชัดเจนและยุติธรรม เพื่อป้องกันการถูกฟ้องกลับว่ามีกรกล่าวหาอย่างไม่ถูกต้อง⁴

ทั้งนี้ โดยจากผลการสำรวจเกี่ยวกับการทุจริตและอาชญากรรมทางเศรษฐกิจของ PricewaterhouseCoopers ในปี พ.ศ. 2562 ข้างต้นยังสำรวจพบต่อไปอีกว่าการตรวจจับเหตุทุจริตภายใน องค์กรที่มีประสิทธิภาพและตรวจสอบได้มากที่สุดในประเทศไทยเกิดจากการแจ้งเบาะแสการกระทำผิด (Whistle Blowing) มากที่สุดถึงร้อยละ 30 แต่อย่างไรก็ตาม การที่พนักงานภายในบริษัทจะทำการแจ้ง เหตุทุจริตภายในองค์กรก็เป็นเรื่องยาก เพราะในบางครั้งก็มีความกังวลเกี่ยวกับเรื่องความปลอดภัยของตนเอง ข้อมูลส่วนบุคคลต่าง ๆ ที่ได้ให้ไป ความใกล้ชิดหรืออิทธิพลของบุคคลที่กระทำความผิด⁵ เป็นต้น

⁴ โอฟาร จันท์คำ, 'จรรยาบรรณและแนวทางปฏิบัติที่ดีในการให้บริการ พร้อมทั้งกรณีศึกษา' (สำนักงานคณะกรรมการกำกับ และส่งเสริมการประกอบธุรกิจประกันภัย, 2562)

<<http://www.oic.or.th/sites/default/files/content/85944/bth6.pdf>> สืบค้นวันที่ 22 กรกฎาคม 2563

⁵ Richard Waters, 'The importance of whistleblowers in the war on white-collar crime' (Macquarie Business School, 15 January 2020) <<https://lighthouse.mq.edu.au/article/january-2020/the-importance-of-whistleblowers-in-the-war-on-white-collar-crime>> assessed 22 July 2020

แต่อย่างไรก็ตาม นอกเหนือไปจากการแจ้งเบาะแสการกระทำผิด (Whistle Blowing) บริษัทควรที่จะดำเนินการมาตรการเชิงป้องกันและป้องปรามเพื่อมิให้เกิดเหตุทุจริตขึ้นภายในองค์กร เช่น การตรวจสอบประวัติอาชญากรรมของผู้สมัครงาน การตรวจสอบพฤติกรรมและประวัติของผู้สมัครงาน การมีระบบตรวจสอบและถ่วงดุลอำนาจ การตรวจสอบการขัดกันของผลประโยชน์ระหว่างพนักงานกับบุคคลภายนอกที่มีความสัมพันธ์กับองค์กร โดยเฉพาะการจัดซื้อจัดจ้างที่อาจเกิดการให้เงินทอนหรือส่วนแบ่ง (Kickback) การตรวจสอบคู่ค้า (Vendor Due Diligence) การสืบสวนและสอบสวนพนักงานและผู้กระทำผิดที่เกี่ยวข้องการดำเนินคดีแรงงาน คดีแพ่ง และคดีอาญา ซึ่งทั้งหมดจำต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นจำนวนมาก ซึ่งในปัจจุบันได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) ในราชกิจจานุเบกษาไปเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 และมีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 แล้วในบางส่วน โดยเริ่มแรกได้กำหนดให้วันที่ 27 พฤษภาคม พ.ศ. 2563 เป็นวันที่กฎหมายนี้มีผลบังคับใช้ตามกฎหมายทั้งฉบับ แต่อย่างไรก็ดี ในวันที่ 20 พฤษภาคม พ.ศ. 2563 ได้มีการประกาศพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยกำหนดให้หน่วยงานภาครัฐและองค์กรธุรกิจรวม 22 กิจการไม่ต้องอยู่ภายใต้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลตั้งแต่วันที่ 27 พฤษภาคม พ.ศ. 2563 ถึง วันที่ 31 พฤษภาคม พ.ศ. 2564 ดังนั้น วันที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลนี้จะมีผลบังคับใช้อย่างเต็มรูปแบบ คือ ตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2564 เป็นต้นไป

โดยสรุปแล้ว กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยอ้างอิงหลักการของ “General Data Protection Regulation” (GDPR) ซึ่งเป็นกฎหมายของสหภาพยุโรปว่าด้วยมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล โดยที่บทบัญญัติส่วนใหญ่ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะอ้างอิงมาจาก GDPR⁶ ซึ่งตั้งอยู่บนพื้นฐานที่เป็นหลักการสำคัญดังกล่าวคือข้อมูลส่วนบุคคลจะต้องตั้งอยู่บนพื้นฐานต่อไปนี้⁷

1. ถูกประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรม และด้วยวิธีการอันโปร่งใสเมื่อสัมพันธ์กับผู้ถูกประมวลผล (“ความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส” / “Lawfulness, fairness and transparency”)
2. ถูกรวบรวมเพื่อวัตถุประสงค์ที่เฉพาะ ชัดเจน และชอบธรรม และไม่ถูกประมวลผลนอกเหนือไปจากที่ตกลงกันไว้ตั้งแต่ต้น (“การกำหนดขอบเขตของวัตถุประสงค์” / “Purpose limitation”)
3. เพียงพอ เกี่ยวเนื่อง และอยู่ในขอบเขตที่จำเป็นโดยสัมพันธ์กับวัตถุประสงค์ที่ข้อมูลถูกประมวลผล (“การใช้ข้อมูลให้น้อยที่สุด” / “data minimization”)
4. แม่นยำและเป็นปัจจุบันเสมอ หากจำเป็น ขั้นตอนที่ยืนยันทั้งหมดจะต้องถูกปฏิบัติเพื่อรับประกันว่าข้อมูลส่วนบุคคลที่ไม่แม่นยำจะถูกลบหรือแก้ไขโดยไม่ล่าช้า (“ความแม่นยำ” / “Accuracy”)

⁶ John P. Formichella, ‘Comparing Privacy Laws: GDPR v. Thai Personal Data Protection Act’ (Blumenthal Richter & Sumet, 2562) <<https://brslawyers.com/news/comparing-privacy-laws-gdpr-v-thai-personal-data-protection-act/>> สืบค้นวันที่ 31 กรกฎาคม 2563

⁷ นคร เสรีรักษ์, ผู้แปล. ‘GDPR ฉบับภาษาไทย’ (Privacy Thailand, 2562) <<https://www.kas.de/documents/274654/4437066/Publication++PT++GDPR+Thai+Version.pdf/9a712458-cc1d-3921-a802-78ec21dbdeac?version=1.1&t=1580789255309>> สืบค้นวันที่ 31 กรกฎาคม 2563

5. โดยคำนึงถึงวัตถุประสงค์ที่ข้อมูลถูกประมวลผล ถูกเก็บรักษาในรูปแบบที่อนุญาตให้การระบุตัวตนของผู้ถูกประมวลผลข้อมูลไม่เป็นไปนานกว่าที่จำเป็นสำหรับวัตถุประสงค์ที่ข้อมูลส่วนบุคคลถูกประมวลผล (“การกำหนดขอบเขตการเก็บรักษา” / “Storage limitation”)

6. ถูกประมวลผลด้วยวิธีการที่รับประกันความปลอดภัยของข้อมูลส่วนบุคคลตามสมควรอันรวมถึงการคุ้มครองจากการประมวลผลที่ไม่ได้รับอนุญาตหรือไม่ชอบด้วยกฎหมายและจากการสูญเสีย การถูกทำลาย หรือความเสียหายโดยอุบัติเหตุ โดยใช้มาตรการทางเทคนิคหรือการจัดการองค์กรตามสมควร (“ความสมบูรณ์ และเป็นความลับ” / “Integrity and confidentiality”)

จากหลักการข้างต้นนำมาสู่บทนิยามและพื้นฐานสำคัญในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย อันอาจจะกล่าวได้โดยสรุปดังต่อไปนี้

ข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (มาตรา 6) เช่น ชื่อ - นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เบอร์โทรศัพท์, วันเกิด, อีเมล, การศึกษา, เพศ, อาชีพ, รูปภาพ, ข้อมูลทางการเงิน

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) (มาตรา 26) ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ได้แก่

เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลธรรมดาที่เป็นเจ้าของข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ “ตัดสินใจ” เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามกฎหมายคุ้มครองส่วนบุคคล โดยดำเนินการดังต่อไปนี้

1. การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลต้องเก็บโดยตรงจากเจ้าของข้อมูลส่วนบุคคล ภายใต้ฐานตามที่กฎหมายกำหนด ดังต่อไปนี้

1.1 ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Consent) โดยการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลต้องทำภายใต้เงื่อนไขดังต่อไปนี้

- ความยินยอมโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ (a clear affirmative action) เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

- การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย (informed)

- การขอความยินยอมนั้น ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน (Separate from other terms and conditions)

- มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว (Unambiguous – concise, easy to understand and user-friendly)

- ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม (Freely given)
- ในการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการนั้น ๆ (Not a precondition of signing up to a service)
- หากเจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ ผู้ไร้ความสามารถ หรือผู้เสมือนไร้ความสามารถ ต้องได้รับความยินยอมจากผู้อำนาจปกครอง ผู้อนุบาล หรือผู้พิทักษ์ (แล้วแต่กรณี) เว้นแต่เป็นกรณีผู้เยาว์ที่มีอายุตั้งแต่ 10 ปีขึ้นไป อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ (Parental Consent)

1.2 การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการป้องกันที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Archives, research or statistics for public interest)

1.3 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital interest)

1.4 เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (Performance of contract) เช่น การปฏิบัติตามสัญญาจ้างพนักงาน หรือสัญญาที่ทำกับคู่ค้า เป็นต้น

1.5 เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล (Public task)

1.6 เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล (Legitimate interest) โดยควรต้องดำเนินการศึกษาวิเคราะห์ความเหมาะสมของการใช้ฐานประโยชน์อันชอบธรรม (Legitimate Interests Assessment) ว่าเป็นไปตามกฎหมายโดยตรวจสอบใน 3 ด้านที่สำคัญ ได้แก่ การตรวจสอบวัตถุประสงค์ (Purpose test) การตรวจสอบความจำเป็น (Necessity Test) และการตรวจสอบความเหมาะสม (Balancing Test)

1.7 เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legal obligation) ซึ่งเป็นกรณีที่กฎหมายบัญญัติให้บริษัทต้องดำเนินการใด ๆ ให้เป็นไปตามกฎหมาย เช่น การแจ้งข้อมูลไปยังสำนักงานประกันสังคม หรือกรมสรรพากร ตามที่กฎหมายกำหนด

2. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) จะต้องกระทำภายใต้ฐานตามที่กฎหมายกำหนด

หากบริษัทจะดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน บริษัทต้องอาศัยฐานตามกฎหมายที่มีความเฉพาะเจาะจงมากกว่าข้อมูลส่วนบุคคลทั่วไป ดังต่อไปนี้

2.1 ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล (Explicit Consent)

2.2 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม (Vital Interest)

2.3 เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสุขภาพแรงงาน

ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิกหรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น (Social Protection & Non-profit)

2.4 เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล (Manifestly made public)

2.5 เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตาม หรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย (Legal Claim) ยกตัวอย่างเช่น ในกรณีที่ผู้ทรงสิทธิเรียกร้องอยู่ระหว่างการเตรียมคำฟ้องเพื่อขอให้ศาลยุติธรรมบังคับการตามสิทธิเรียกร้องของตน ซึ่งการเตรียมคำฟ้องดังกล่าวนั้นทนายความผู้รับมอบอำนาจอาจมีความจำเป็นที่จะต้องเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลที่สาม⁸

2.6 เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

2.6.1 เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมาย และข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพ หรือวิชาชีพ หรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ (Preventive or Occupational Medicine)

2.6.2 ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจง เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ (Public Health)

2.6.3 การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Health or Social Care System)

2.6.4 การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด (Archiving, Scientific or Historical Research)

2.6.5 ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (Substantial Public Interest) โดยสามารถยกตัวอย่างได้ เช่น การป้องกันการดำเนินการที่ไม่ชอบด้วยกฎหมาย การคุ้มครองสาธารณชนจากการกระทำอันไม่สุจริต

⁸ ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ‘แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล Thailand Data Protection Guidelines 2.0’

<<https://www.law.chula.ac.th/wpcontent/uploads/2019/10/TDPG2.0-C5-20191009.pdf>>

สืบค้นเมื่อวันที่ 31 กรกฎาคม 2563

(ซึ่งหมายรวมถึงการดำเนินการของสื่อมวลชนเกี่ยวกับการกระทำอันไม่สุจริต) การป้องกันการฉ้อโกง การต้องสงสัยเกี่ยวกับการสนับสนุนทางการเงินสำหรับการก่อการร้ายหรือการฟอกเงิน⁹

3. การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล และในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

3.1 วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

3.2 แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

3.3 ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

3.4 ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

3.5 ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

3.6 สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย (Data Subject) ได้แก่

- สิทธิขอถอนความยินยอม (Consent Withdrawal)
- สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access) โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคล โดยจะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบต่อโอกาสก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

- สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
- สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
- สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (Right to erasure / right to be forgotten) ในกรณีที่มิเหตุตามที่กฎหมายกำหนด ยกเว้นในกรณีการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือ มาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

- สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)
- สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)
- สิทธิร้องเรียน

⁹ เพิ่งอ้าง

4. บทลงโทษหากไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

4.1 ความรับผิดทางแพ่ง ตามความเสียหายที่เกิดขึ้นจริง และอาจต้องชดเชยค่าสินไหมทดแทนเพิ่มขึ้นอีก โดยสูงสุดไม่เกิน 2 เท่าของค่าเสียหายที่แท้จริงทั้งนี้ขึ้นอยู่กับดุลยพินิจของศาล

4.2 โทษทางอาญา กับบริษัทรวมถึงกรรมการและบุคคลที่มีหน้าที่สั่งการ โดยมีโทษจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ ตามฐานความผิดทางอาญาที่ได้รับไว้

4.3 โทษทางปกครอง ปรับสูงสุดไม่เกิน 5 ล้านบาท ตามฐานความผิดทางปกครองที่กำหนดไว้

นอกจากนี้ การดำเนินคดีแพ่งในคดีเกี่ยวกับความผิดเกี่ยวกับข้อมูลส่วนบุคคลดังกล่าวยังอาจเข้าเกณฑ์ในการดำเนินคดีแบบกลุ่ม (Class Action) ซึ่งเป็นการดำเนินคดีแพ่งรูปแบบหนึ่งที่มีผู้เสียหายจำนวนมาก ซึ่งได้รับผลกระทบจากข้อเท็จจริงและข้อกฎหมายอย่างเดียวกันหรือมีเหตุกระทำเดียวกัน โดยมีโจทก์ที่เป็นตัวแทนของกลุ่มในการดำเนินการฟ้องร้องคดี ซึ่งเมื่อศาลมีคำพิพากษาแล้ว ผลของคำพิพากษาจะผูกพันสมาชิกทุกคนในกลุ่มที่ได้รับความเสียหายจากเหตุเดียวกัน แม้จะไม่ได้เข้ามาเป็นคู่ความในคดีด้วยก็ตาม¹⁰ ซึ่งการดำเนินคดีแบบกลุ่มสามารถนำไปบังคับใช้ได้กับการดำเนินคดีแพ่งที่ครอบคลุมฐานความผิดที่มีขอบเขตกว้างขวางอย่างมาก¹¹

5. บทวิเคราะห์

จากที่ได้อ้างหลักการไว้ข้างต้นเกี่ยวกับ อาชญากรรมคอปกเลื้อขาว สามเหลี่ยมทุจริต และข้อจำกัดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล จะเห็นได้อย่างชัดเจนว่ามาตรการเชิงป้องกันและป้องปรามเพื่อมิให้เกิดเหตุทุจริตขึ้นภายในองค์กรที่แต่ละบริษัทได้ดำเนินการอยู่ในปัจจุบัน เพื่อลดโอกาสการเกิดขึ้นของอาชญากรรมคอปกเลื้อขาว โดยเฉพาะในการกระทำความผิดของพนักงานซึ่งมีอัตราส่วนที่มีนัยสำคัญที่ก่อเหตุทุจริตภายในองค์กรด้วยตนเอง หรือร่วมกับบุคคลภายนอกนั้น จำต้องพิจารณาภายใต้บริบทของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ได้ประกาศใช้และกำลังจะมีผลใช้บังคับในประเทศไทยอีกด้วย ทั้งนี้ บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจำต้องตระหนักถึงข้อจำกัดภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ทั้งเรื่องการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของพนักงานและบุคคลที่เกี่ยวข้องว่ามีวัตถุประสงค์ที่เฉพาะชัดเจน และชอบธรรม มีฐานตามกฎหมายที่สามารถทำได้ เก็บเท่าที่จำเป็นเพียงพอเกี่ยวเนื่อง และอยู่ในขอบเขตที่จำเป็นโดยสัมพันธ์กับวัตถุประสงค์ที่ข้อมูลถูกประมวลผล แม่นยำ และเป็นปัจจุบันเสมอ ภายใต้ระยะเวลาที่เหมาะสม เก็บโดยตรงจากเจ้าของข้อมูลส่วนบุคคล และเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการเก็บข้อมูลเกี่ยวกับประวัติอาชญากรรม ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนหรือไม่

ด้วยเหตุนี้ การรักษาสอดคล้องระหว่างมาตรการเชิงป้องกันและป้องปรามเพื่อมิให้เกิดเหตุทุจริตกับการคุ้มครองข้อมูลส่วนบุคคลจึงจำเป็นต้องกระทำโดยพิจารณาอย่างถี่ถ้วน เพื่อมิให้เกิดเหตุที่ผู้กระทำความผิดจะยกกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อฟ้องร้อง หรือดำเนินคดีโต้กลับบริษัทที่ดำเนินคดีแรงงาน

¹⁰ ธนพร ฟาร์รุ่งสา, 'สรุปสาระสำคัญของการดำเนินคดีแบบกลุ่มตามประมวลกฎหมายวิธีพิจารณาความแพ่ง (Class Action)' (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 28 มกราคม 2563)

<<https://www.sec.or.th/TH/Documents/LawsandRegulations/ClassAction-summary.pdf>>

สืบค้นเมื่อวันที่ 31 กรกฎาคม 2563

¹¹ นนทวัชร นวตระกูลพิสุทธิ, "การดำเนินคดีแบบกลุ่ม": ข้อเสนอแนะบางประการเกี่ยวกับร่างพระราชบัญญัติว่าด้วยการดำเนินคดีแบบกลุ่มของไทยและบทบาท "ใหม่" ของศาล" (วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, มิถุนายน 2554)

<[http://digi.library.tu.ac.th/journal/0022/40-2-2554.pdf?_ga=2.124842894.503040098.1578889160-](http://digi.library.tu.ac.th/journal/0022/40-2-2554.pdf?_ga=2.124842894.503040098.1578889160-611977851.1558665468)

611977851.1558665468> สืบค้นเมื่อวันที่ 31 กรกฎาคม 2563

คดีแพ่ง และคดีอาญา ซึ่งอาจรวมไปถึงการดำเนินคดีแบบกลุ่มที่อาจเกิดขึ้นได้ หากบริษัทได้ดำเนินการใด ๆ ไปโดยมิได้พิจารณาถึงข้อจำกัดภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลดังกล่าว

ทั้งนี้ มาตราการเชิงป้องกันและปราบปรามเพื่อมิให้เกิดเหตุทุจริตขึ้นภายในองค์กรที่สำคัญ เช่น การแจ้งเบาะแสการกระทำผิด (Whistle Blowing) การตรวจสอบประวัติอาชญากรรมของผู้สมัครงาน การตรวจสอบพฤติกรรมและประวัติของผู้สมัครงาน การตรวจสอบการขัดกันของผลประโยชน์ระหว่างพนักงานกับบุคคลภายนอกที่มีความสัมพันธ์กับองค์กร โดยเฉพาะการจัดซื้อจัดจ้าง การตรวจสอบคู่ค้า (Vendor Due Diligence) การสืบสวนและสอบสวนพนักงานและผู้กระทำความผิดที่เกี่ยวข้อง จึงจำเป็นต้องพิจารณาถึงประเด็นปัญหาทางข้อกฎหมายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. การเก็บรวบรวมข้อมูลของผู้สมัครงาน/พนักงาน

ในเบื้องต้น การเก็บข้อมูลส่วนบุคคลของผู้สมัครงานหรือพนักงานโดยตรง ย่อมกระทำได้เท่าที่จำเป็นเพื่อให้เป็นไปตามความจำเป็น เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (Performance of contract) ทั้งนี้ “ความจำเป็น” ในที่นี้จำกัดอยู่แค่เพียง “การปฏิบัติตามสัญญา” ตามปกติของการดำเนินงานให้เป็นไปตามสัญญาเท่านั้น แต่หากบริษัทประสงค์จะเก็บข้อมูลส่วนบุคคลจากผู้สมัครงานหรือพนักงานที่นอกเหนือไปจากความจำเป็นในการปฏิบัติตามสัญญา จำเป็นต้องได้รับความยินยอม (Consent) จากผู้สมัครงานหรือพนักงานเพิ่มเติมอีกด้วย ซึ่งในการขอความยินยอมในการเก็บรวบรวม ใช้ข้อมูลส่วนบุคคล ระหว่างบริษัทและผู้สมัครงานหรือพนักงานนั้น อาจพิจารณาได้ว่าเป็นกรณีที่มีความยินยอมไม่เป็นไปตามกฎหมายอย่างแท้จริง เนื่องจากเกิดจากบุคคลที่มีอำนาจต่อรองไม่เท่ากัน และความยินยอมไม่ได้เกิดขึ้นโดยสมัครใจอย่างแท้จริง ยกเว้นแต่ในกรณีที่เจ้าของข้อมูลสามารถเลือกในการปฏิเสธที่จะไม่ให้ข้อมูลได้จริง ๆ

ดังนั้น บริษัทจึงต้องพิจารณาถึงเหตุผลและความจำเป็นของบริษัทในการเก็บข้อมูลเพิ่มเติมดังกล่าว ในกรณีที่จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรม (Legitimate Interest) ของผู้ควบคุมข้อมูล และบุคคลอื่นโดยไม่เกินขอบเขตที่เจ้าของข้อมูล สามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันอาชญากรรมและการฉ้อโกง การส่งต่อในเครือบริษัทเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวมการส่งไปต่างประเทศ ทั้งนี้ บางบริษัทมีการเฝ้าระวังการใช้งานอินเทอร์เน็ตของพนักงาน เพื่อป้องกันไม่ให้พนักงานใช้ทรัพยากรไอทีของบริษัทไปเพื่อการส่วนตัวมากเกินไป ข้อมูลที่เก็บรวบรวมเพื่อการเฝ้าระวังนี้ รวมถึงข้อมูลลูกก็ที่แสดงประวัติการเข้าชมเว็บไซต์และการดาวน์โหลด การเฝ้าระวังนี้ หากกระทำโดยมิได้แจ้งให้พนักงานหรือสหภาพแรงงานทราบก่อน และไม่ได้แจ้งรายละเอียดของการประมวลผลข้อมูลอย่างชัดเจน ในกรณีเช่นนี้แม้บริษัทจะมีผลประโยชน์อันชอบธรรม แต่ว่าเป็นการขัดกับสิทธิความเป็นส่วนตัวของพนักงานอย่างมาก รวมไปถึงการเก็บรวบรวมข้อมูลอาจกระทำเกินจำเป็นไม่ได้สัดส่วน และไม่โปร่งใส อีกทั้งยังมีวิธีอื่นที่ละเมิดสิทธิของพนักงานน้อยกว่า เช่น จำกัดการเข้าชมเว็บไซต์บางประเภทจากคอมพิวเตอร์ของบริษัท เป็นต้น จึงไม่สามารถอ้างฐานผลประโยชน์อันชอบธรรมได้¹²

2. การเก็บข้อมูลของบุคคลในครอบครัวและบุคคลที่เกี่ยวข้องของผู้สมัครงาน/พนักงาน เพื่อทำการตรวจสอบความขัดแย้งทางผลประโยชน์กับคู่ค้า

บางบริษัททำการเก็บข้อมูลของบุคคลในครอบครัว ได้แก่ คู่สมรส บิดา มารดา บุตร และญาติ ผ่านผู้สมัครงานหรือพนักงาน เพื่อทำการตรวจสอบความขัดแย้งทางผลประโยชน์ ดังนั้น การเก็บข้อมูล

¹² ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, ‘แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล Thailand Data Protection Guidelines 2.0’ (n 9)

ดังกล่าวย่อมเป็นการเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง ดังนั้น บริษัท จำต้องปฏิบัติตามกฎหมายเพิ่มเติมในการเก็บข้อมูลส่วนบุคคล ได้แก่ การแจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บ รวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่พิสูจน์ได้ว่า เป็นการเก็บรวบรวมข้อมูล ส่วนบุคคลด้วยความยินยอม หรือเป็นที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 เช่น ใช้ฐานความยินยอม หรือฐานผลประโยชน์อันชอบธรรม (ซึ่งจะต้องมีการประเมินแล้วว่าผลประโยชน์ ที่เกิดแก่คู่สัญญา หรือบริษัทนั้นไม่ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล (ในที่นี้คือคู่สมรส บิดา มารดา บุตร และญาติ) โดยไม่เกินขอบเขตที่ตัวเจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผลด้วย)¹³

ทั้งนี้ มาตรการอีกส่วนหนึ่งที่บริษัทมักกระทำควบคู่กัน คือ การประกาศนโยบายความขัดแย้ง ทางผลประโยชน์ (Conflict of Interest Policy) โดยกำหนดให้กรรมการ ผู้บริหาร และพนักงานพึงหลีกเลี่ยง การกระทำใด ๆ อันเป็นการขัดต่อผลประโยชน์ของบริษัท ไม่ว่าจะเป็นเกิดจากการติดต่อกับผู้เกี่ยวข้องทางการค้า ของบริษัท เช่น คู่ค้า ลูกค้า คู่แข่งขัน หรือจากการใช้โอกาสหรือข้อมูลที่ได้จากการเป็นกรรมการ ผู้บริหาร หรือพนักงานในการหาประโยชน์ส่วนตน และในเรื่องการทำธุรกิจที่แข่งขันกับบริษัทหรือการทำงานอื่น นอกเหนือจากงานของบริษัท ซึ่งส่งผลกระทบต่องานในหน้าที่ โดยทำการตรวจสอบความขัดแย้ง ทางผลประโยชน์ระหว่างคู่ค้า กับพนักงานของบริษัท (Vendor Due Diligence) โดยการขอให้ทั้งพนักงาน และคู่ค้าดำเนินการเปิดเผยข้อมูล หากจะมีกรณีที่ข้อสงสัยว่าจะมีความขัดแย้งทางผลประโยชน์เกิดขึ้น ซึ่งการกระทำดังกล่าวกับคู่ค้าอาจจะพิจารณาถึงฐานตามกฎหมาย (Legal Obligation) หากเป็นบริษัท ที่จดทะเบียนอยู่ในตลาดหลักทรัพย์ฯ หรือฐานตามสัญญา (Contractual Obligation) โดยกำหนดไว้ ให้เป็นส่วนหนึ่งของสัญญา หรือฐานผลประโยชน์อันชอบธรรม (Legitimate Interest) โดยจะต้องมีการแจ้งนโยบาย ความเป็นส่วนตัว (Privacy Notice) ให้กับคู่ค้าทราบ เพื่อให้เกิดความชัดเจนในเรื่องเกี่ยวกับวัตถุประสงค์ และรายละเอียดที่เกี่ยวข้องต่าง ๆ

3. การตรวจสอบประวัติอาชญากรรม รวมไปถึงการตรวจสอบประวัติการทำงานกับอดีตนายจ้าง ของผู้สมัครงาน/พนักงาน

วิธีการหนึ่งในปัจจุบันที่บริษัทหลายแห่งได้นำมาใช้เพื่อป้องกันเหตุทุจริตที่จะเกิดขึ้นภายในองค์กร คือ การคัดสรรคนจากบุคคลผู้อ้างอิง อดีตนายจ้าง และประวัติอาชญากรรม เพื่อให้สามารถป้องกันปัญหาทุจริตภายใน องค์กร¹⁴ โดยบางบริษัทตรวจสอบประวัติในอดีตที่ผ่านมา ทั้งประวัติการทำงาน และประวัติอาชญากรรม ของผู้สมัครงาน เพื่อคัดกรองเบื้องต้นว่าเคยมีประวัติไม่ดีที่ไม่เหมาะสมในการให้เข้ามาทำงานด้วยหรือไม่ โดยเฉพาะในตำแหน่งหน้าที่ที่สำคัญและเกี่ยวข้องกับด้านการเงิน ทั้งนี้ ภายใต้บริบทกฎหมายคุ้มครอง ข้อมูลส่วนบุคคล การตรวจสอบดังกล่าวต้องพิจารณาถึงความยินยอมของผู้สมัครงานเป็นสำคัญ ซึ่งประเด็น ที่มีข้อควรระวัง เนื่องจากการขอความยินยอมนั้นจำต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของ ข้อมูลส่วนบุคคลในการให้ความยินยอม (Freely given) และต้องไม่มีเงื่อนไขในการให้ความยินยอม เพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีเจตนาเป็นหรือเกี่ยวข้องกับสำหรับการเข้าทำสัญญา รวมถึงการให้บริการนั้น ๆ ซึ่งนอกเหนือไปจากอำนาจต่อรองที่ต่างกันของผู้สมัครงาน

¹³ เฟ็งอั้ง

¹⁴ Piotr Foitzik, 'How to 'Background Check' under the GDPR International Association of Privacy Professionals' (1 October 2019) <<https://iapp.org/news/a/how-to-background-check-under-the-gdpr/>> assessed 22 July 2020

ทั้งนี้ บางบริษัทประสงค์ที่จะตรวจสอบประวัติการทำงานในอดีตของผู้สมัครงานโดยใช้วิธีสอบถามไปยังอดีตนายจ้างโดยตรง ซึ่งเมื่อพิจารณาถึงกรอบทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว จะมีส่วนที่เกี่ยวข้องกับบริษัทใหม่และอดีตนายจ้างว่าได้ปฏิบัติโดยถูกต้องหรือไม่ สำหรับในส่วนของผู้สมัครงาน หากยังเก็บข้อมูลส่วนบุคคลไว้จำเป็นต้องพิสูจน์ถึงฐานตามกฎหมาย และระยะเวลาที่กำหนดให้อดีตนายจ้าง ยังคงสามารถเก็บข้อมูลนั้นต่อไปได้ และฐานตามกฎหมายที่จะเปิดเผยข้อมูลดังกล่าว ซึ่งในเบื้องต้น อดีตนายจ้างอาจไม่สามารถเปิดเผยข้อมูลส่วนบุคคลของอดีตลูกจ้างให้กับบริษัทได้ เนื่องจากไม่อาจหาฐานตามกฎหมายใด ๆ ที่ให้อำนาจอดีตนายจ้างกระทำการดังกล่าว โดยหากจะอ้างอิงไปถึงฐานประโยชน์อันชอบธรรม ก็อาจจะไม่ผ่านเกณฑ์ในการใช้ได้ เนื่องจากอาจกระทบสิทธิกับอดีตพนักงานเกินสมควร ด้วยเหตุนี้ บริษัทใหม่ อาจพิจารณาดำเนินการจัดทำหนังสือยินยอมจากผู้สมัครงาน เพื่อให้บริษัทสามารถขอข้อมูลไปยังอดีตนายจ้าง รวมทั้งขยายขอบเขตความยินยอมไปให้ถึงอดีตนายจ้าง เพื่อให้เปิดเผยข้อมูลตามที่ระบุไว้ให้กับบริษัทได้ แต่อย่างไรก็ตาม หนังสือยินยอมดังกล่าวคงเป็นเพียงการเพิ่มน้ำหนักในการร้องขอข้อมูลจากอดีตนายจ้าง เนื่องจากอดีตนายจ้างไม่ได้มีหน้าที่ใด ๆ ตามกฎหมายที่จะต้องดำเนินการดังกล่าว¹⁵ เว้นแต่ว่า ผู้สมัครงาน จะได้ดำเนินการร้องขอไปยังอดีตนายจ้างให้ดำเนินการโอนถ่ายข้อมูลตามสิทธิของตนภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลไปยังบริษัท ซึ่งอาจต้องคำนึงถึงความยินยอมว่าเป็นไปด้วยความสมัครใจหรือเป็นเงื่อนไขในการรับสมัครงานหรือไม่ เนื่องจากอาจจะทำให้ความยินยอมดังกล่าวเป็นไปโดยมิชอบด้วยกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

4. การแจ้งเบาะแสการกระทำผิด (Whistle Blowing)

หลักการสำคัญของการแจ้งเบาะแสการกระทำผิด (Whistle Blowing) คือ การเปิดโอกาสให้ผู้มีส่วนได้เสีย ทั้งภายในและภายนอกองค์กร แจ้งเบาะแสหรือข้อร้องเรียนเกี่ยวกับการกระทำผิดกฎหมาย จรรยาบรรณ รายงานทางการเงินที่ไม่ถูกต้อง หรือระบบควบคุมภายในที่บกพร่องต่อผู้บริหารสูงสุดขององค์กร หรือบุคคลที่ได้รับมอบหมาย เพื่อที่จะดำเนินการสอบสวนการกระทำผิด รวมทั้งคุ้มครองผู้แจ้งเบาะแสไม่ให้ถูกละเมิดสิทธิ โดยข้อมูลที่ได้รับจากการแจ้งเบาะแส บริษัทต้องมีการประกาศนโยบายการแจ้งเบาะแสการกระทำผิด (Whistle Blowing Policy) ไว้ ให้มีความชัดเจน และต้องดำเนินการรักษาข้อมูลที่ได้รับแจ้งดังกล่าวให้เป็นความลับ และไม่มีการเปิดเผยชื่อ ผู้ที่แจ้งเบาะแส หรือผู้ร้องเรียนต่อสาธารณชนหากไม่ได้รับความยินยอม รวมทั้งผู้แจ้งเบาะแส หรือ ข้อร้องเรียน จะได้รับการคุ้มครองสิทธิ ไม่ว่าจะเป็นพนักงานบริษัท หรือบุคคลภายนอก จึงจะทำให้เกิดผลสัมฤทธิ์ ในการดำเนินการมาตรการป้องปรามการกระทำผิดภายในองค์กร

ทั้งนี้ การดำเนินการรับแจ้งเบาะแสการกระทำผิดต้องดำเนินการให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วยเช่นกัน โดยที่การเก็บข้อมูลจากผู้ร้องเรียนและดำเนินการสอบสวนผู้ต้องสงสัย โดยอาจอ้างอิงจากฐานผลประโยชน์อันชอบธรรม ซึ่งจำเป็นต้องพิจารณาถึงองค์ประกอบของการใช้ ฐานผลประโยชน์อันชอบธรรมให้รัดกุม เนื่องจากเป็นฐานตามกฎหมายที่ต้องใช้ด้วยความระมัดระวัง มิให้ส่งผลกระทบต่อสิทธิของผู้ต้องสงสัยเกินควร โดยจำเป็นต้องพิจารณาถึงพยานหลักฐานได้รับมา จากการแจ้งเบาะแส และที่ได้จากการสืบสวนสอบสวนเพิ่มเติม ซึ่งหากเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ก็อาจสามารถอ้างอิงไปถึงฐานความจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้อง ตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้อง

¹⁵ Waterfront Solicitors LLP, 'UK: Asking For Employer References – What Can You Ask, And When? GDPR And Other Legal Considerations' (Mondaq, 9 October 2018)<<https://www.mondaq.com/uk/employee-rights-labour-relations/743916/asking-for-employer-references-what-can-you-ask-and-when-gdpr-and-other-legal-considerations>> assessed 22 July 2020

ตามกฎหมาย (Legal Claim) ได้อีกด้วย¹⁶ ทั้งนี้ จำต้องพิจารณาฐานกฎหมายในแต่ละมุมทั้งของผู้ที่แจ้งเบาะแสว่าเป็นการให้ข้อมูลส่วนบุคคลของผู้อื่นให้กับบริษัท และผู้บริหารที่นำข้อมูลดังกล่าวมาใช้เป็นกรณี ๆ ไป เพื่อให้เกิดความชัดเจน

5. การดำเนินคดีของบริษัทกับข้อโต้แย้งของพนักงาน

โดยปกติ เมื่อบริษัทได้ดำเนินการสืบสวนสอบสวนพนักงานที่ต้องสงสัยว่ากระทำความผิดภายในองค์กร การดำเนินการในขั้นต่อไป คือการดำเนินการลงโทษทางวินัยแก่พนักงานตามลำดับชั้นความร้ายแรงของการกระทำ ตั้งแต่ตักเตือนจนกระทั่งเลิกจ้างโดยให้มีผลทันทีและไม่จ่ายค่าชดเชย และควบคู่ไปกับการดำเนินคดีทางแพ่งเพื่อเรียกร้องค่าเสียหาย และดำเนินคดีทางอาญาเพื่อลงโทษต่อผู้กระทำความผิดรวมไปถึงบุคคลที่มีส่วนเกี่ยวข้อง ทั้งนี้ มาตรการนี้ถือเป็นมาตรการที่ส่งผลต่อการป้องปรามอาชญากรรมภายในองค์กรเป็นอย่างดี

แต่อย่างไรก็ดี บริษัทจำต้องพิจารณาและวางเกณฑ์ปฏิบัติในการดำเนินการทั้งทางแรงงาน ทางคดีแพ่ง และคดีอาญาอย่างรัดกุม เพื่อป้องกันมิให้เกิดคดีความฟ้องร้องกลับมายังบริษัท เช่น คดีแรงงานจากเลิกจ้างโดยไม่เป็นธรรม คดีแพ่ง และคดีอาญา อันเนื่องมาจากการข่มขืนใจให้ลงนามในเอกสารใด ๆ หนึ่งประเภท เป็นต้น นอกเหนือไปจากนั้น เมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ บริษัทก็จำต้องพิจารณาถึงสิทธิของพนักงาน/อดีตพนักงานในฐานะเจ้าของข้อมูลส่วนบุคคล และหน้าที่ของบริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลอีกด้วย เช่น หากพนักงาน/อดีตพนักงาน ขอใช้สิทธิขอให้ลบหรือทำลาย (Right to be forgotten) ก่อนหรือระหว่างดำเนินคดี หรือโต้แย้งเรื่องกำหนดระยะเวลาในการเก็บข้อมูลส่วนบุคคลของพนักงานของบริษัท ก็ต้องมีการจัดการภายในเพื่อตอบสนอง หรือปฏิเสธการใช้สิทธิของพนักงานได้ต่อไป

¹⁶ Lara White, Andrew Reeves and Sarah Greenwood, 'GDPR: What are the grounds for processing personal data during an investigation?' (The FCPA Blog, September 10, 2019)

<<https://fcpcbolog.com/2019/09/10/gdpr-what-are-the-grounds-for-processing-personal-data-durin/>>
assessed 22 July 2020