Thai

information and privacy commission
new south wales

เอกสารเผยแพร่ข้อมูล

พฤศจิกายน ค.ศ. 2023

คำถามที่มักพบบ่อยเกี่ยวกับข้อกำหนดให้แจ้งการละเมิดข้อมูล (ข้อกำหนด MNDB)

ข้อมูลนี้จัดทำขึ้นสำหรับใคร	บุคคลทั่วไปในรัฐนิวเซาท์เวลส์ที่ต้องการข้อมูลเกี่ยวกับข้อกำหนดให้แจ้งการละเมิดข้อมูล (Mandatory Notification of Data Breach Scheme)
เพราะเหตุใดข้อมูลนี้จึงมีความสำคัญสำหรับบุคคลทั่วไป	เอกสารเผยแพร่ข้อมูลนี้จะช่วยให้บุคคลทั่วไปมีความเข้าใจมากยิ่งขึ้นเกี่ยวกับข้อกำหนดดังกล่าวและสิทธิที่ตนมีเมื่อเกิดการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของตน

ข้อกำหนดให้แจ้งการละเมิดข้อมูลคืออะไร

ข้อกำหนดให้แจ้งการละเมิดข้อมูล (Mandatory Notification of Data Breach Scheme — ข้อกำหนด MNDB) คือ ข้อกำหนดที่บังคับให้ต้องแจ้งการละเมิดข้อมูล ภายใต้*พระราชบัญญัติว่าด้วยการคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล ค.ศ. 1998 (Privacy and Personal Information Protection Act 1998* — PPIP Act) สำหรับหน่วยงานภาครัฐของรัฐนิวเซาท์เวลส์ในกรณีที่เกิดเหตุการณ์ 'การละเมิดข้อมูลที่เข้าข่ายที่กำหนด'

ข้อกำหนด MNDB เริ่มต้นขึ้นเมื่อใด

ข้อกำหนด MNDB เริ่มต้นเมื่อวันที่ 28 พฤศจิกายน ค.ศ. 2023

ข้อกำหนด MNDB บังคับใช้กับบุคคลใด

ข้อกำหนด MNDB บังคับใช้กับหน่วยงานภาครัฐของรัฐนิวเซาท์เวลส์ รัฐมนตรี มหาวิทยาลัย เทศบาล และรัฐวิสาหกิจ ที่ไม่ได้รับการครอบคลุมภายใต้กฎหมายว่าด้วยความเป็นส่วนตัวของรัฐบาลเครือรัฐ

นโยบายว่าด้วยการละเมิดข้อมูลคืออะไร

นโยบายว่าด้วยการละเมิดข้อมูล (Data Breach Policy) (หรือ DBP) เป็นนโยบายหรือแผนงานที่จัดทำขึ้น เพื่อกำหนดวิธีการที่หน่วยงานจะตอบสนองต่อการละเมิดข้อมูล หน่วยงานต่าง ๆ ต้องมีนโยบาย DBP ภายใต้กฎหมายดังกล่าว นโยบาย DBP ควรระบุบทบาทและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในหน่วยงานในเรื่องการจัดการการละเมิดข้อมูล และขั้นตอนที่หน่วยงานดังกล่าวจะปฏิบัติตามเมื่อเกิดการละเมิดข้อมูลขึ้น

หน่วยงานต่าง ๆ ต้องเผยแพร่นโยบาย DBP ของหน่วยงานให้บุคคลทั่วไป ซึ่งก็คือ หน่วยงานควรจัดเผยแพร่นโยบาย DBP ทางเว็บไซต์ของหน่วยงาน

'การละเมิดข้อมูลที่เข้าข่ายที่กำหนด' คืออะไร

ภายใต้ข้อบังคับ MNDB นั้น หน่วยงานจะต้องแจ้งให้บุคคลที่ได้รับผลกระทบและกรรมาธิการคุ้มครองความเป็นส่วนตัว (Privacy Commissioner) ทราบเมื่อเกิดการละเมิดข้อมูลที่เข้าข่ายที่กำหนด 'การละเมิดข้อมูลที่เข้าข่ายที่กำหนด' เกิดขึ้นเมื่อมีเหตุการณ์ดังต่อไปนี้

- การเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลที่หน่วยงานเก็บไว้ โดยไม่ได้รับอนุญาต ที่น่าจะมีแนวโน้มว่าจะส่งผลให้เกิด**ความเสียหายร้ายแรง**ต่อบุคคลที่ข้อมูลนั้นเกี่ยวข้อง
- การสูญหายของข้อมูลส่วนบุคคลที่หน่วยงานเก็บไว้ ในสถานการณ์ซึ่งมีแนวโน้มว่าจะเกิดการเข้าถึงหรือการเปิดเผยโดยไม่ได้รับอนุญาต และน่าจะมีแนวโน้มว่าจะส่งผลให้เกิด**ความเสียหายร้ายแรง**ต่อบุคคลที่ข้อมูลนั้นเกี่ยวข้อง

ความเสียหายร้ายแรงคืออะไร

ความเสียหายร้ายแรง อาจรวมถึง ความเสียหายทางร่างกาย ความเสียหายทางการเงินหรือต่อทรัพย์สิน ความเสียหายทางอารมณ์หรือจิตใจ หรือความเสียหายต่อชื่อเสียง ทั้งนี้ ผลกระทบจากความเสียหายดังกล่าวอาจแตกต่างกันสำหรับแต่ละบุคคล ซึ่งอาจรวมถึงผลกระทบดังต่อไปนี้

- การสูญเสียทางการเงินจากการฉ้อโกง
- แนวโน้มความเสี่ยงต่อความเสียหายทางร่างกายหรือทางจิตใจ เช่น โดยอดีตคู่ครองที่มีพฤติกรรมข่มเหงรังแก
- การโจรกรรมอัตลักษณ์บุคคล ซึ่งอาจส่งผลกระทบต่อการเงินและ/หรือประวัติเครดิตของคุณ
- ความเสียหายร้ายแรงต่อชื่อเสียงของบุคคล

การละเมิดข้อมูลอาจเกิดขึ้นได้อย่างไรบ้าง

ในภาพรวมแล้ว การละเมิดข้อมูลสามารถเกิดขึ้นได้จากความผิดพลาดของบุคลากร ความล้มเหลวของระบบ หรือการละเมิดที่มุ่งร้ายหรือทางไซเบอร์

ตัวอย่างการละเมิดข้อมูลมีอะไรบ้าง

ตัวอย่างการละเมิดข้อมูลมีดังนี้

ความผิดพลาดของบุคลากร

- มีการส่งจดหมายหรืออีเมลไปยังผู้รับผิดราย
- มีการอนุญาตผิดพลาดให้บุคคลที่ไม่ได้รับอนุญาตเข้าใช้ระบบ หรือมีการปกป้องรหัสผ่านอย่างไม่แน่นหนาเพียงพอ
- ทรัพย์สินที่มีข้อมูลส่วนบุคคลสูญหาย/หาไม่พบ เช่น บันทึกข้อมูล แล็ปท็อป ยูเอสบี โทรศัพท์

ความล้มเหลวของระบบ

- เกิดข้อผิดพลาดเกี่ยวกับการเขียนคำสั่ง ซึ่งทำให้มีการอนุญาตเข้าใช้ระบบโดยไม่ต้องพิสูจน์ตัวตน หรือมีการแจ้งข้อมูลโดยอัตโนมัติ
- ระบบไม่ได้รับการบำรุงรักษาโดยใช้แพตช์ที่ทราบและรับรองระบบ

การโจมตีปองร้ายหรือทางอาชญากรรม

- เหตุการณ์ทางไซเบอร์ เช่น มัลแวร์เรียกค่าไถ่ มัลแวร์ การเจาะข้อมูล การหลอกลวง การพยายามเข้าสู่ระบบโดยการคาดเดาชื่อผู้ใช้งานและรหัสผ่าน
- การหลอกล่อทางจิตวิทยา/การปลอมเป็นบุคคลอื่น ซึ่งทำให้มีการเปิดเผยข้อมูลส่วนบุคคลอย่างไม่เหมาะสม
- ภัยคุกคามภายใน (พนักงาน) โดยใช้รายละเอียดการลงชื่อเข้าใช้ที่ได้รับอนุญาต เพื่อเข้าถึง/เปิดเผยข้อมูลส่วนบุคคลที่อยู่นอกเหนือหน้าที่ของตนหรือขอบเขตที่ได้รับอนุญาต

หน่วยงานนั้นจำเป็นต้องแจ้งให้กรรมาธิการคุ้มครองความเป็นส่วนตัวทราบหรือไม่

ในกรณีที่เหตุการณ์การละเมิดข้อมูลได้รับการประเมินว่าเป็นการละเมิดข้อมูลที่เข้าข่ายที่กำหนด หน่วยงานจะต้องแจ้งให้กรรมาธิการคุ้มครองความเป็นส่วนตัวทราบทันที โดยใช้แบบฟอร์มบนเว็บไซต์ IPC

ฉันจะได้รับแจ้งหรือไม่ หากฉันได้รับผลกระทบจากการละเมิดข้อมูลที่เข้าข่ายที่กำหนด

หากหน่วยงานตัดสินใจว่ามีการละเมิดข้อมูลที่เข้าข่ายที่กำหนด ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลของคุณ หน่วยงานนั้นจะต้องแจ้งให้คุณทราบถึงการละเมิดนั้นทันทีที่จะกระทำได้ โดยหน่วยงานจะต้องแจ้งคุณเป็นลายลักษณ์อักษร และให้ข้อมูลคุณเกี่ยวกับการละเมิดข้อมูลที่เข้าข่ายที่กำหนดที่เกิดขึ้น พร้อมแจ้งข้อมูลดังต่อไปนี้

- สิ่งที่หน่วยงานได้ดำเนินการไปแล้ว หรือแผนควบคุมหรือบรรเทาความเสียหายนั้นที่เกิดขึ้นกับคุณ
- ขั้นตอนที่คุณควรพิจารณาดำเนินการหลังจากเกิดการละเมิดข้อมูล
- ข้อมูลเกี่ยวกับวิธีการร้องขอให้มีการทบทวนภายในต่อการดำเนินงานของหน่วยงานนั้น หรือวิธีการยื่นเรื่องร้องเรียนเรื่องความเป็นส่วนตัวต่อกรรมาธิการคุ้มครองความเป็นส่วนตัว

ฉันควรได้รับแจ้งเมื่อใดหลังจากเกิดการละเมิดข้อมูล

เมื่อหน่วยงานมีเหตุอันควรให้สงสัยว่าอาจเกิดเหตุการณ์การละเมิดข้อมูลที่เข้าข่ายที่กำหนดขึ้น หน่วยงานต้องดำเนินการต่าง ๆ ดังนี้

- ดำเนินการทุกอย่างตามความเหมาะสมในการควบคุมการละเมิดข้อมูลนั้น
- ประเมินว่ามีการเข้าถึงข้อมูลหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือการสูญหายของข้อมูลส่วนบุคคลที่หน่วยงานเก็บไว้หรือไม่ภายใน 30 วัน
- ประเมินว่ามีแนวโน้มที่จะเกิดความเสียหายร้ายแรงต่อบุคคลใดที่ได้รับผลกระทบหรือไม่ภายใน 30 วัน
- ดำเนินการทุกอย่างตามความเหมาะสมเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากเหตุการณ์ที่สงสัยว่าเป็นการละเมิดนั้น

หลังจากที่ดำเนินการตามขั้นตอนข้างต้นแล้ว หากหน่วยงานสรุปว่ามีการละเมิดข้อมูลที่เข้าข่ายที่กำหนด ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลของคุณ หน่วยงานนั้นจะต้องแจ้งให้คุณทราบถึงการละเมิดนั้นโดยเร็วที่สุดที่จะกระทำได้

จะเกิดอะไรขึ้นหากหน่วยงานนั้นไม่มีรายละเอียดสำหรับติดต่อฉันเพื่อแจ้งเรื่องการละเมิดข้อมูลนั้น

หน่วยงานมีอำนาจแบ่งปันข้อมูลภายใต้ข้อกำหนด MNDB โดยสามารถขอข้อมูลส่วนบุคคลที่เกี่ยวข้องจากหน่วยงานภาครัฐอีกแห่งได้ ข้อมูลที่หน่วยงานจะขอได้นั้นจะจำกัดเฉพาะข้อมูลที่จำเป็นในการยืนยันชื่อและรายละเอียดติดต่อของบุคคลที่ได้รับผลกระทบจากการละเมิดข้อมูล

อย่างไรก็ตาม หากหน่วยงานนั้นไม่สามารถแจ้งคุณโดยตรงได้ หน่วยงานต้องเผยแพร่ประกาศทางเว็บไซต์ของหน่วยงาน และดำเนินการประชาสัมพันธ์ประกาศนั้นตามความเหมาะสม ประกาศแจ้งดังกล่าวต้องเผยแพร่อยู่ในทะเบียนประกาศสำหรับบุคคลภายนอกบนเว็บไซต์ของหน่วยงานเป็นเวลาอย่างน้อย 12 เดือน

มีเหตุผลใดหรือไม่ที่หน่วยงานอาจไม่แจ้งให้ฉันทราบ

มี มีข้อยกเว้นเฉพาะสำหรับข้อกำหนดที่ให้หน่วยงานแจ้งบุคคลที่ได้รับผลกระทบจากการละเมิดข้อมูล เช่น หากหน่วยงานดำเนินการคลี่คลายการละเมิดข้อมูลอย่างรวดเร็ว และการดำเนินการเช่นนั้นทำให้การละเมิดข้อมูลที่เกิดขึ้นมีแนวโน้มว่าจะไม่ส่งผลให้เกิดความเสียหายร้ายแรง เช่นนั้นแล้ว ไม่กำหนดว่าจะต้องแจ้งให้บุคคลที่ได้รับผลกระทบรายใด ๆ ทราบ

หน่วยงานนั้นจะช่วยเหลือฉันหรือไม่หลังจากที่แจ้งเรื่องแล้ว

ประเภทของความช่วยเหลือหรือการสนับสนุนที่หน่วยงานอาจให้หลังจากแจ้งเรื่องแล้ว จะขึ้นอยู่กับสภาพการณ์เฉพาะของการละเมิดข้อมูลนั้น เช่น

- ช่วยเหลือในการออกทดแทนเอกสารหรือข้อมูลประจำตัวที่รัฐบาลออกให้ที่ได้รับผลกระทบจากเหตุการณ์ เช่น ใบอนุญาตขับขี่
- ให้คำแนะนำเกี่ยวกับวิธีปกป้องข้อมูลส่วนบุคคลของคุณ
- ประสานให้คุณได้รับความช่วยเหลือเพิ่มเติมและการบริการให้คำปรึกษา

ฉันควรทำอย่างไรหากได้รับแจ้ง

มีขั้นตอนที่เป็นประโยชน์ที่คุณสามารถดำเนินการได้ เพื่อปกป้องข้อมูลส่วนบุคคลของตนเอง และลดความเสี่ยงที่คุณจะได้รับความเสียหายจากการละเมิดข้อมูล การจะดำเนินการลักษณะใดนั้นขึ้นอยู่กับสภาพการณ์ของการละเมิดข้อมูลที่เกิดขึ้นและประเภทของข้อมูลที่เกี่ยวข้อง หนังสือแจ้งที่คุณได้รับควรแนะนำข้อปฏิบัติที่คุณจะสามารถดำเนินการ เพื่อรับมือกับการละเมิดข้อมูลในรูปแบบนั้น ๆ ที่ระบุในหนังสือแจ้ง

หากคุณต้องการข้อมูลเพิ่มเติมเกี่ยวกับการละเมิดข้อมูลนั้นและวิธีปกป้องข้อมูลส่วนบุคคลของคุณ คุณควรติดต่อหน่วยงานที่ส่งหนังสือแจ้งให้คุณ

ฉันจะหาข้อมูลเพิ่มเติมได้อย่างไร

คณะกรรมการข้อมูลและความเป็นส่วนตัวรัฐนิวเซาท์เวลส์ (Information and Privacy Commission NSW - IPC) มีข้อมูลและเอกสารเผยแพร่เพิ่มเติมทางเว็บไซต์ หรือคุณสามารถติดต่อ IPC โดยใช้รายละเอียดทางด้านล่าง

หากต้องการข้อมูลเพิ่มเติม

โปรดติดต่อคณะกรรมการข้อมูลและความเป็นส่วนตัวรัฐนิวเซาท์เวลส์ (Information and Privacy Commission NSW - IPC)

โทรฟรี 1800 472 679

อีเมล ipcinfo@ipc.nsw.gov.au

เว็บไซต์ www.ipc.nsw.gov.au

หมายเหตุ ข้อมูลในเอกสารเผยแพร่ข้อมูลนี้มีไว้เพื่อเป็นคำแนะนำเท่านั้น คุณควรขอคำปรึกษาทางกฎหมายเกี่ยวกับสภาพการณ์ในแต่ละกรณี