HR-LAB · ความปลอดภัยและข้อมูลพนักงาน

PDPA สำหรับงาน HR

งาน HR ใช้ข้อมูลส่วนบุคคลด้วยฐานกฎหมายอะไร เมื่อไรต้องขอความยินยอม ข้อมูลสุขภาพและใบหน้าต้องระวังอย่างไร และถ้าข้อมูลรั่วต้องแจ้งภายในเท่าไร

ชื่อ _____ หน่วยงาน _____ วันที่ _____

คำถามหลัก

บริษัทจะใช้ระบบสแกนใบหน้าลงเวลาและเก็บใบรับรองแพทย์ ต้องทำอะไรให้ถูกตาม PDPA

คำตอบสั้น

ทุกการใช้ข้อมูลต้องมีวัตถุประสงค์และฐานกฎหมาย งาน HR ส่วนใหญ่ใช้ฐานสัญญา หน้าที่ตามกฎหมาย หรือประโยชน์โดยชอบด้วยกฎหมาย จึงไม่ต้องขอความยินยอมทุกเรื่อง แต่ข้อมูลอ่อนไหว เช่น สุขภาพ ชีวภาพ (ใบหน้า ลายนิ้วมือ) หรือประวัติอาชญากรรม ต้องมีความยินยอมโดยชัดแจ้งหรือข้อยกเว้นตามมาตรา 26 ต้องแจ้งนโยบายความเป็นส่วนตัว จำกัดผู้เข้าถึง กำหนดระยะเก็บ และถ้าข้อมูลรั่วที่มีความเสี่ยงต้องแจ้งสำนักงานคณะกรรมการภายใน 72 ชั่วโมง

ม.24	ม.26	72	Notice
ฐานกฎหมาย	**ข้อมูลอ่อนไหว**	**ชั่วโมง**	**ก่อนเก็บ**
สัญญา หน้าที่ตามกฎหมาย ประโยชน์โดยชอบ ความยินยอม	สุขภาพ ชีวภาพ ประวัติอาชญากรรม สหภาพ	แจ้งเหตุข้อมูลรั่วต่อสำนักงานคณะกรรมการ	แจ้งวัตถุประสงค์และสิทธิ
PDPA	PDPA	ม.37	ม.23

01 ขอบเขตของเรื่องนี้

ผู้ควบคุมและผู้ประมวลผลข้อมูล | ประกาศความเป็นส่วนตัว | ฐานกฎหมายการประมวลผล | ข้อมูลอ่อนไหวมาตรา 26 | ระยะเก็บและผู้เข้าถึง | เหตุข้อมูลรั่วไหล

ฐานกฎหมาย: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562; ประกาศ PDPC เรื่อง security, ROPA, breach ฯลฯ ฉบับปัจจุบัน

สิ่งที่อยากรู้หรือคำถามจากหน้างาน

01 หลักตัดสินที่ต้องใช้

1. เก็บ ใช้ และเปิดเผยข้อมูลได้เมื่อมีฐานกฎหมาย เช่น สัญญา หน้าที่ตามกฎหมาย ประโยชน์โดยชอบด้วยกฎหมาย หรือความยินยอม (ม.24)
2. แจ้งวัตถุประสงค์ ประเภทข้อมูล ระยะเก็บ ผู้รับข้อมูล และสิทธิของเจ้าของข้อมูลก่อนหรือขณะเก็บ (ม.23)
3. ข้อมูลอ่อนไหว เช่น สุขภาพ ชีวภาพ ประวัติอาชญากรรม ความเชื่อ สหภาพแรงงาน ต้องมีความยินยอมโดยชัดแจ้งหรือข้อยกเว้นตามมาตรา 26
4. ความยินยอมต้องให้อย่างอิสระ เฉพาะเรื่อง และถอนได้ จึงไม่เหมาะเป็นฐานของทุกเรื่องในความสัมพันธ์การจ้างงาน
5. ข้อมูลรั่วไหลที่มีความเสี่ยง แจ้งสำนักงานคณะกรรมการภายใน 72 ชั่วโมงนับแต่ทราบ และแจ้งเจ้าของข้อมูลเมื่อมีความเสี่ยงสูง (ม.37)

02 ตัดสินใจทีละขั้น — ไล่จากบนลงล่าง หยุดเมื่อเจอผลลัพธ์

#	คำถาม	ใช่	ไม่ใช่
1	**ข้อมูลที่จะเก็บเป็นข้อมูลอ่อนไหว เช่น สุขภาพหรือใบหน้าหรือไม่**	→ ข้อถัดไป	ใช้ฐานตามมาตรา 24 ที่เหมาะสม แจ้ง notice และจำกัดการใช้ตามวัตถุประสงค์
2	**มีข้อยกเว้นตามมาตรา 26 เช่น หน้าที่ตามกฎหมายแรงงานหรือคุ้มครองแรงงานหรือไม่**	ประมวลผลตามข้อยกเว้น พร้อมมาตรการคุ้มครองที่เหมาะสม	→ ข้อถัดไป
3	**ได้ความยินยอมโดยชัดแจ้งที่ปฏิเสธได้ และมีทางเลือกอื่นให้หรือไม่**	ประมวลผลได้ เก็บหลักฐานความยินยอมและให้ถอนได้	ห้ามเก็บข้อมูลนั้น ใช้วิธีอื่นที่ไม่ใช้ข้อมูลอ่อนไหว

ใช้กับกรณีของเรา: ข้อเท็จจริงที่ต้องตรวจเพิ่ม

01 ตัวอย่างกับกรณีจริง

กรณี 1: ระบบลงเวลาด้วยการสแกนใบหน้า

บริษัทต้องการใช้ระบบสแกนใบหน้าลงเวลาแทนบัตร เพื่อป้องกันการลงเวลาแทนกัน

ประเภทข้อมูล	**ชีวภาพ (อ่อนไหว)**
ฐานที่ใช้	**ยินยอมโดยชัดแจ้ง**
ทางเลือกสำหรับผู้ไม่ยินยอม	**บัตร / PIN**
ระยะเก็บ	**ลบเมื่อพ้นสภาพ**

ผล: ขอความยินยอมโดยชัดแจ้งที่ปฏิเสธได้ มีวิธีลงเวลาอื่นให้ จำกัดผู้เข้าถึง และกำหนดการลบข้อมูลเมื่อพ้นสภาพ

กรณี 2: ไฟล์ใบรับรองแพทย์ถูกส่งผิดกลุ่มแชท

เจ้าหน้าที่ส่งไฟล์ใบรับรองแพทย์ของพนักงาน 12 คนเข้ากลุ่มแชทของทั้งแผนกโดยไม่ตั้งใจ

เป็นข้อมูลอ่อนไหว	**สุขภาพ**
ลบและจำกัดความเสียหาย	**ทันที**
ประเมินความเสี่ยงและแจ้ง สคส.	**ภายใน 72 ชม.**

ผล: ลบไฟล์ ขอให้ผู้ได้รับลบ บันทึกเหตุ ประเมินความเสี่ยง แจ้งสำนักงานคณะกรรมการภายใน 72 ชั่วโมง และแจ้งพนักงานที่ได้รับผลกระทบ

02 ลำดับเวลาและกำหนดที่ต้องไม่พลาด

ก่อนเก็บข้อมูล	ระหว่างใช้	เมื่อพบเหตุรั่ว	ครบระยะเก็บ
กำหนดวัตถุประสงค์ ฐานกฎหมาย และแจ้ง notice	จำกัดผู้เข้าถึงและบันทึกการเข้าถึง	จำกัดความเสียหาย ประเมินความเสี่ยง แจ้งภายใน 72 ชั่วโมง	ลบหรือทำให้ไม่ระบุตัวบุคคล

ลองคำนวณกรณีของคุณ

01 ความเข้าใจผิดที่พบบ่อย

เข้าใจผิด	ที่ถูกต้อง
งาน HR ต้องขอความยินยอมทุกเรื่อง	ส่วนใหญ่ใช้ฐานสัญญา หน้าที่ตามกฎหมาย หรือประโยชน์โดยชอบ
ให้เซ็นใบยินยอมครอบจักรวาลครั้งเดียวพอ	ความยินยอมต้องเฉพาะเรื่องและปฏิเสธได้
ข้อมูลรั่วภายในบริษัทไม่ต้องแจ้ง	ถ้ามีความเสี่ยงต้องแจ้งภายใน 72 ชั่วโมง

02 รายการตรวจสองฝ่าย

บริษัทและฝ่าย HR

- ☐ ทำ data map ข้อมูลพนักงานทุกประเภท
- ☐ แยกฐานกฎหมายของแต่ละวัตถุประสงค์
- ☐ ทำสัญญาประมวลผลข้อมูลกับผู้ให้บริการ
- ☐ ซ้อมขั้นตอนรับมือข้อมูลรั่ว 72 ชั่วโมง

ลูกจ้าง

- ☐ อ่านประกาศความเป็นส่วนตัวของนายจ้าง
- ☐ ใช้สิทธิขอเข้าถึงหรือแก้ไขข้อมูลเมื่อจำเป็น
- ☐ ปฏิเสธความยินยอมที่ไม่จำเป็นได้ โดยขอทางเลือกอื่น

เอกสารและหลักฐานที่ต้องมี

- ☐ ประกาศความเป็นส่วนตัวสำหรับพนักงานและผู้สมัคร
- ☐ หลักฐานความยินยอมสำหรับข้อมูลอ่อนไหว
- ☐ บันทึกเหตุข้อมูลรั่วและการแจ้ง
- ☐ บันทึกรายการกิจกรรมการประมวลผล (ROPA)
- ☐ สัญญาประมวลผลข้อมูลกับผู้ให้บริการ

03 ทดสอบความเข้าใจ

1. ข้อมูลใดเป็นข้อมูลอ่อนไหวตามมาตรา 26

(ก) ชื่อและตำแหน่ง (ข) ข้อมูลใบหน้าสำหรับยืนยันตัวตน (ค) เลขบัญชีธนาคาร

2. ข้อมูลรั่วที่มีความเสี่ยง ต้องแจ้งสำนักงานคณะกรรมการภายใน

(ก) 24 ชั่วโมง (ข) 72 ชั่วโมง (ค) 30 วัน

3. การจ่ายเงินเดือนต้องขอความยินยอมเพื่อใช้ข้อมูลบัญชีหรือไม่

(ก) ต้อง (ข) ไม่ต้อง ใช้ฐานสัญญาจ้าง (ค) ต้องทุกเดือน

เฉลย: 1(ข) ข้อมูลชีวภาพเป็นข้อมูลอ่อนไหว · 2(ข) มาตรา 37 กำหนด 72 ชั่วโมงนับแต่ทราบ · 3(ข) เป็นการปฏิบัติตามสัญญาจ้าง

บันทึก

ตรวจทานเนื้อหา 9 ตุลาคม 2569 · ใช้ประกอบการตัดสินใจร่วมกับตัวบทที่มีผลและข้อเท็จจริงของแต่ละกรณี · อ่านฉบับเต็มและภาษาอังกฤษได้ที่ www.hrlab-th.com