

HR Conference: Rights, Risks & Responsibilities in the Modern Malaysian Workplace



23 SEPTEMBER 2025
9:00 AM - 5:00 PM



AUDITORIUM, LEVEL 3
BANGUNAN SULAIMAN,
ASIAN INTERNATIONAL
ARBITRATION CENTRE
(AIAC), KL



arlegal.my



+6014-9817605



sarah@arlegal.my

SCHEDULE

23 SEPTEMBER 2025

HR CONFERENCE: RIGHTS, RISKS & RESPONSIBILITIES IN THE
MODERN MALAYSIAN WORKPLACE

AM 8:30	REGISTRATION + BREAKFAST
AM 9:00	WORKPLACE BULLYING & SEXUAL HARRASSMENT Speaker: Suzanne Arockiaraj
AM 10:15	BREAK
AM 10:30	MANAGING REMOTE WORKERS & DIGITAL NOMADS Speaker: Crystal Cha
PM 12:15	LUNCH Private Legal Clinic (By Appointment Only)
PM 1:30	SAFEGUARD YOUR BUSINESS AGAINST DATA BREACHES Speaker: Mike Lee
PM 2:45	BREAK
PM 3:00	RECENT TREND OF DISCIPLINARY CASES: INDUSTRIAL AND CONTENT CREATOR Speaker: Alwin Rajasurya
PM 4:30	CLOSING & NETWORKING SESSION

WORKPLACE BULLYING & SEXUAL HARASSMENT: Legal & Practice Insights

Speaker:

Suzanne Arockiaraj

Slides Prepared by:

Kelly Yong

Hareesa Qadija

DISCLAIMER

The contents of this presentation have been prepared for ease of reference of the readers and any sections referred to herein are sections that have been paraphrased and simplified. You are advised to refer to the actual wordings of the Statutes for a complete appreciation of the sections referred. Professional advice should also first be sought before making decisions based on the knowledge provided in this general presentation.

PART ONE

WORKPLACE BULLYING

Bullying: What is it (and Isn't)

- Repeated, unreasonable conduct that harms safety & dignity

Forms:

- Verbal — insults, yelling, gossip
- Psychological — isolation, sabotage, unfair criticism
- Physical — intimidation, unwanted contact
- Cyber — hostile messages, online shaming, doxing
- **NOT** bullying: fair performance management with clear reasons & targets

Bullying vs Not Bullying

Bullying	Not Bullying
“You’re useless. You’ll never meet this deadline.”	“This report is late. Let’s set clear deadlines and supports.”
“Everyone knows you’re incompetent.” (said in front of peers)	“I noticed errors in your work. Let’s go through them together.”
<i>Manager sends 20 hostile WhatsApps at 2 AM: “Answer me now, or else!”</i>	<i>Manager sends email during work hours: “Please update me on the project by tomorrow.”</i>
“I’ll make sure you don’t get promoted.”	“To be promoted, you need to improve teamwork and leadership.”
<i>Sharing colleague’s personal details online without consent (doxing).</i>	<i>Sharing contact list with HR for official work purposes.</i>

Why It Matters?

For Employers

- Legal duty: safety includes psychosocial risks
- New Penal Code offences (bullying/harassment, incl. online)
- Business risks: productivity, attrition, brand, lawsuits

For Employees

- Mental health harm & career derailment
- Right to a safe, respectful workplace
- Need clear channels to speak up without retaliation

Applicable Laws in Malaysia

- **Employment Act 1955 & Industrial Relations Act 1967** — contracts, misconduct, dismissal
- **Occupational Safety & Health Act 1994 (OSHA)** — duty to ensure safety incl. psychosocial risks (s.15)
- **DOSH 2024 Guideline** — psychosocial risk assessment & management
- **Penal Code (Amendment) Act 2025** — bullying, harassment, doxxing now criminal offences (ss.507B–507G)
- **Communications & Multimedia Act 1998 (s.233)** — online abuse

Employment Act & Industrial Relations Act

- No express definition of bullying
- Bullying can be treated as gross misconduct
- Employers may discipline/dismiss with just cause & excuse
- Industrial Court consistently upholds dismissals for severe bullying/harassment

OSHA & DOSH Guideline

- OSHA 1994, s.15: duty to ensure safety, health & welfare
- Covers psychosocial risks (stress, harassment, bullying)
- DOSH Guideline 2024: screening, assessment & control steps for psychological hazards
- Employers expected to show proactive measures

Penal Code Amendments 2025 (In force: 11 July 2025)

SECTIONS	OFFENCES	PUNISHMENT
507B	Threatening, abusive or insulting language or behaviour, including verbal abuse, intimidation, or hostile outbursts	Imprisonment up to 3 years.
507C	Harassing or intimidating someone (via email or chat)	Up to 1 year or fine.
507D (1) & (2)	(1) Sustained psychological provocation, including repeated taunting or deliberate emotional pressure that causes distress or fear or (2) harassment leads to a suicide attempt	Imprisonment up to 1 year Imprisonment up to 10 years.
507E & 507F	Publishing or misusing someone's personal or identity information with intent to cause harm, alarm or distress, including doxxing	Imprisonment up to 3 years.

Vicarious Liability — Can Employers Be Liable?

- Employers may be held vicariously liable for employees' misconduct if it occurs in the course of employment
- **Maslinda bt Ishak v Mohd Tahir Osman & Ors [2009] 6 CLJ 653** — govt agencies & RELA officer; invasion of privacy → agencies held jointly liable
- Test: Was the act closely connected to duties? (even if unauthorised, improper, or prohibited)
- Implication: In bullying/harassment cases, liability can extend to employer if misconduct happens in workplace context or during work functions

Nik Hishamuddin Nik Mansor v PETRONAS (IC KL, Award 1366/2024)

Facts: Manager insulted subordinate (“stupid, no brain, shut up”), belittled work, caused her to cry.

Principle: Bullying = repeated humiliation, not “management style.”

Decision: Dismissal upheld.

Ratio: harassment/bullying intolerable; performance issues ≠ excuse for abuse.

Prabakharan Balakrishnan v Entegris Malaysia (IC KL, Award 540/2022)

Facts: Manager stalked subordinate's FB, used her late mother's photo as WhatsApp DP, sent repeated unwanted personal DMs.

Principle: Harassment via social media/WhatsApp ≠ private — misconduct if it undermines dignity at work.

Decision: Dismissal upheld.

Ratio: harassment is grave; employers must protect dignity.

Lee Ted Yong v Syarikat Sesco (IC Sarawak, Award 706/2017)

Facts: At company dinner, employee shouted vulgarities at boss, assaulted colleagues (kicks, punches).

Principle: Off-site misconduct at company event = still “in course of employment.”

Decision: Dismissal upheld.

Ratio: Misconduct = Conduct inconsistent with duties; trust destroyed.

Afnizahanim v Kemaman Bitumen (IC KL, Award 2541/2019)

Facts: HR Manager spread rumours of affair, intimidated witness, breached confidentiality.

Principle: HR = higher duty of trust; misconduct erodes workplace harmony.

Decision: Dismissal upheld.

Ratio: Abuse of position by HR creates toxic environment; termination justified.

Bina Goodyear Bhd v Subramaniam (IC KL, Award 773/2000)

Facts: Manager swore at subordinate in front of staff, causing humiliation → resignation.

Principle: Public humiliation can breach implied term of trust/confidence.

Decision: Recognised as misconduct; can justify constructive dismissal.

Ratio: Persistent abusive conduct = repudiation of contract.

Shaun Khee v Carigali Hess (2016) & Khaw Yao Shun v PETRONAS (2019)

Shaun Khee: Harassment = grave misconduct; dismissal upheld.

Khaw Yao Shun: Harassment + dishonesty = breach of trust; dismissal upheld.

Principle: Zero tolerance for harassment & integrity breaches.

Preventing Workplace Bullying — Employer Actions

POLICIES & PROCEDURES

- Handbook/code of conduct: define bullying, harassment, examples
- Regular training & acknowledgment (not just paper policy)
- Clear disciplinary framework: show-cause, inquiry, sanctions

SAFE & OPEN CHANNELS

- Multiple reporting options (HR, hotline, anonymous)
- Clear purpose: raise misconduct concerns early
- Guarantee of confidentiality & non-retaliation

Preventing Workplace Bullying — Employer Actions

TRAINING & FAIR INVESTIGATIONS

- Managers trained to handle complaints without bias
- Show-cause letter + fair domestic inquiry
- Due notice, right to be heard, documented process
- Neutral panel & full records (letters, minutes, evidence)

PROPORTIONATE DISCIPLINE

- Range: warnings, counselling, PIPs, retraining
- Termination for severe/repeated misconduct
- Consistency across cases to avoid claims of unfairness

If Workplace Bullying Has Occurred — Company Response

1. Receiving the Complaint

- Record initial details (who, what, when, where, witnesses).
- Acknowledge complaint promptly (verbal/written).
- Assure confidentiality & protection against retaliation.

2. Preliminary Assessment

- Check if allegations fall under bullying/harassment policy
- Assess urgency (safety risks, immediate harm)
- Decide on interim/temporary measures (separate staff, paid leave)

3. Formal Investigation

- Appoint impartial investigator/committee (HR + neutral manager).
- Gather evidence: interviews, review emails, CCTV, documents
- Maintain written records at every stage

4. Findings & Evaluation

- Assess credibility, corroboration, consistency
- Apply “balance of probabilities” standard.
- Produce written report (facts, analysis, conclusion)

5. Decision & Disciplinary Action

- Proven: proportionate sanction (warning, demotion, suspension, dismissal)
- Not proven: close case, but monitor for retaliation
- Ensure consistency with handbook & legal requirements

6. Communication

- Inform both complainant and accused of outcome
- Give rationale without breaching confidentiality

7. Post-Resolution Support

- Offer counselling / EAP support
- Monitor workplace climate for retaliation or further conflict
- Reinforce anti-bullying policy (team briefing/refresher training)

PART TWO

SEXUAL HARASSMENT AT WORKPLACE

Sexual Harassment at Work

- Serious workplace issue across industries, levels, and roles
- Involves unwelcome sexual conduct — verbal, non-verbal, visual, or physical
- Creates intimidating, hostile, or offensive environment
- Harms dignity, well-being, productivity, and morale
- Legal & reputational risks for employers (Anti-Sexual Harassment Act 2022)

Why Addressing Sexual Harassment Matters?

For Employer

- Ensures safe & respectful workplace
- Protects brand, morale & productivity
- Avoids legal liability & lawsuits
- Builds trust & accountability culture

For Employees

- Protects dignity, safety & well-being
- Encourages respect & equal opportunity
- Boosts morale and engagement
- Provides clear channels to report without fear

Definition of Sexual Harassment

- **Section 2 of the Employment Act 1955:**

“Unwanted conduct of a sexual nature, verbal, non-verbal, visual, gestural, or physical, directed at a person which is offensive, humiliating, or threatens well-being, arising in the course of employment.”

- **Code of Practice (1999):**

Unwanted sexual conduct that:

- *Can be seen as placing a sexual condition on employment, or*
- *Can be seen as offensive, humiliating, or threatening, even without a direct link to employment.*

Elements of Sexual Harassment



CATEGORIES OF SEXUAL HARASSMENT

Sexual Annoyance

- Conduct that is sexually offensive, hostile or intimidating and no direct link to any job benefits
- Repetitive in nature to annoy the victim



Sexual Coercion

- Directly affecting the victim's employment
- The employee is threatened to lose his/ her employment benefits [possible bonus, promotion]
- Power imbalance between the employer and employee or between the victim and the perpetrator



Forms of Sexual Harassment

Physical

Psychological

Visual

Non-verbal

Verbal

How Sexual Harassment Affects Victims?

- Depression — prolonged sadness, withdrawal, hopelessness
- Low self-esteem — loss of confidence, shame, self-blame
- Anxiety — constant worry, fear of being at work
- Sleep disorders — insomnia, nightmares, fatigue
- Decline in work performance — absenteeism, disengagement, errors



Statutory Protection & Guidelines in Malaysia

Anti-Sexual Harassment Act 2022

- Establishes Tribunal for Anti-Sexual Harassment (TAGS)
- Provides remedies: apology, damages, corrective orders

Penal Code (Act 574)

- Criminalises sexual offences (outrage of modesty, assault, harassment)

Employment Act 1955 & Amendment Act 2022

- s.81A: defines “complaint of sexual harassment”
- s.81B–81H: inquiry procedure, obligation to display notice

Statutory Protection & Guidelines in Malaysia

Industrial Relations Act 1967

- s.20: unfair dismissal remedy available if dismissed after complaining

Code of Practice 1999 (MOHR)

- Non-binding guideline on prevention, awareness & procedures

Communications & Multimedia Act 1998 (s.233)

- Criminalises obscene/menacing/offensive online messages
- Penalty: up to RM50,000 fine or 1 year jail

Penal Code (Act 576)

Sections	Offences	Punishment
354	Molestation (Assault or use of criminal force on a person with intent to outrage her modesty).	Imprisonment maximum 10 years or fine or whipping or any two of such punishment.
355	Assault or use of criminal force with intent to dishonour a person, otherwise than on grave provocation.	Imprisonment maximum 2 years or fine or both.
377D	Outrages on decency.	Imprisonment maximum 2 years.
509	Word or gesture intended to insult the modesty of any person.	Imprisonment maximum 5 years or fine or both.

Employment Act & Industrial Relations Act

Employment Act 1955 (as amended)

Section 81A: Complaint of sexual harassment =

- Employee v. employee
- Employee v. employer
- Employer v. employees.

Section 81B–81E: Employer must inquire into every complaints.

Section 81H: Employers must display notice raising awareness of sexual harassment

Industrial Relations Act 1967

Section 20: Wrongful dismissal claims.

Employee who is dismissed after lodging harassment complaint may file representation within 60 days.

Communications & Multimedia Act 1998 (s.233)

Section 233 CMA

- Offence to knowingly make, create, or transmit any communication that is:
 - Obscene or indecent
 - False or menacing
 - Offensive in character
- Intent: to annoy, abuse, threaten, or harass another person
- Penalty: Fine $\leq$ RM50,000, imprisonment $\leq$ 1 year, or both
- Additional fine RM1,000 for each day offence continues

Melewar Corporation Bhd v Abu Osman [1994] 2 ILR 807

Facts:

- Employee accused of sexually harassing a colleague.
- Employer received credible complaints of harassment.

Principle:

- Employer has a duty to inquire into sexual harassment complaints.
- If proven after inquiry, employer has a duty to act firmly against the offender.

Decision:

- Industrial Court held: credible complaints cannot be ignored.
- Employers must investigate promptly and decisively.

Employer owes contractual obligation to his or her employees to provide safe and conducive working environment in which the employees can function.

Employer would be in breach of fundamental terms of the contract of employment if failed to steps to stop the sexual harassment complain that was brought to his attention.

The breach would be a basis for employees who have been sexually harassed to leave their jobs. They would then may claim that by the employer repudiatory breach, constructive dismissal has occurred.

Employees who had been sexually harassed are entitled to call in aid the doctrine of constructive dismissal and seek their remedies in law.

Legal Recourse for Victims of Sexual Harassment

1. Workplace / Employment Law:

- Employment Act 1955 (ss.81A–81H): complaint → employer must inquire
- Industrial Relations Act 1967 (s.20): unfair dismissal claims (e.g., dismissal after complaining)
- Constructive dismissal possible if harassment ignored

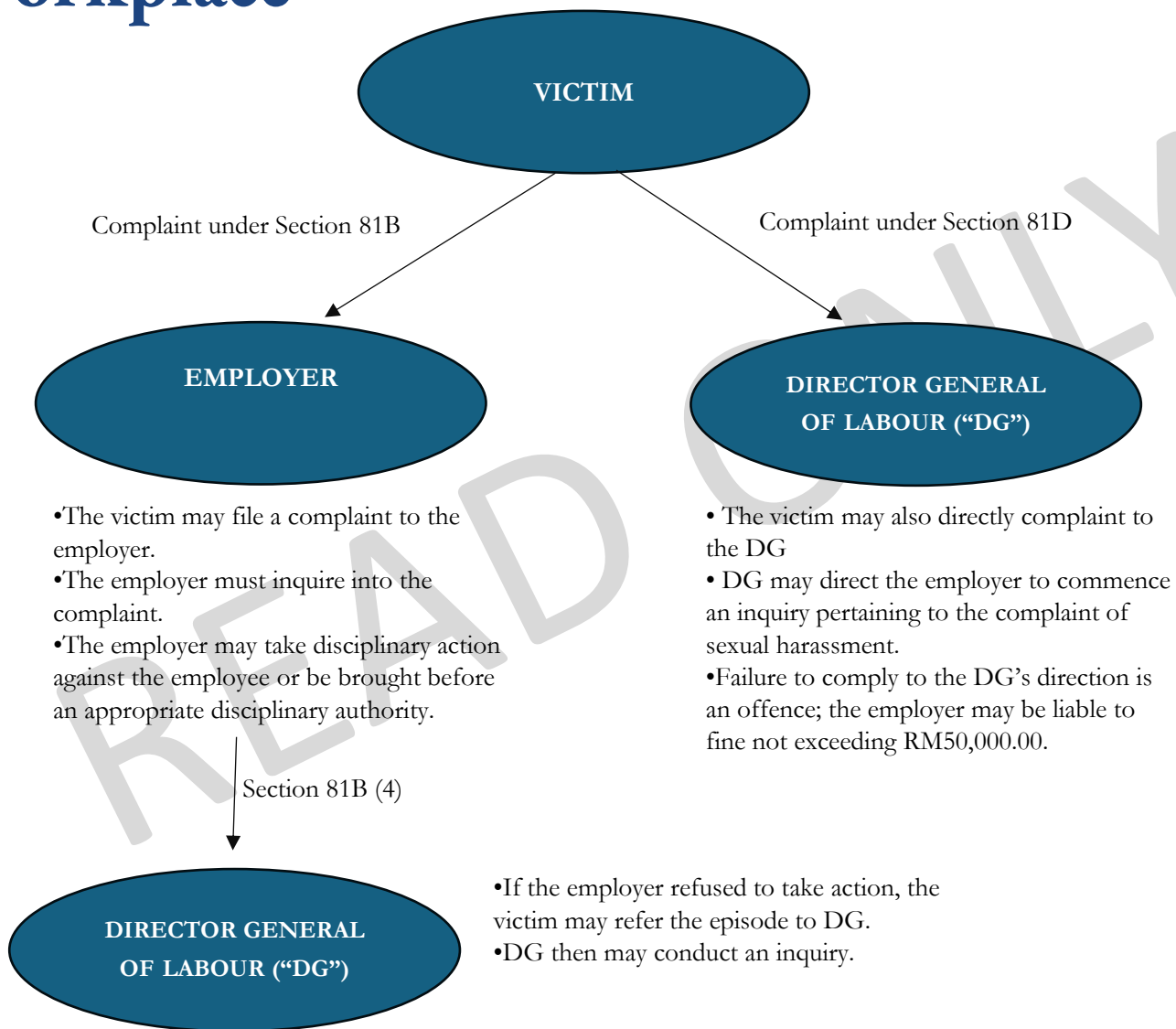
2. Civil & Criminal Law

- Penal Code s.354 – Assault or use of criminal force with intent to outrage modesty (up to 10 yrs jail, fine, or whipping)
- Penal Code s.509 – Word, gesture, or act intended to insult modesty (up to 5 yrs jail, fine, or both)
- Civil suit in tort: damages for emotional distress, harassment

3. Anti-Sexual Harassment Act 2022

- Establishes Tribunal for Anti-Sexual Harassment (TAGS)
- Accessible to all (employees & non-employees)
- Remedies: apology, compensation, corrective orders
- Speedier & cheaper than court proceedings

(1) At the Workplace



(2) Lodge a Police Report

- Triggers police investigation → possible criminal charges

Penal Code:

- S.354 – Assault or use of force to outrage modesty (10 yrs jail, fine, whipping)
- S.509 – Word/gesture intended to insult modesty (5 yrs jail or fine) Police report may support civil claim (IO can testify as witness)

(3) File a Civil Suit

- Malaysian courts now recognise tort of sexual harassment (Mohd Ridzwan v Asmah [2016] FC)
- Victim can sue perpetrator directly for damages (emotional distress, loss of dignity, reputational harm)

Evidence is crucial:

- WhatsApp / emails / recordings
- Witnesses to behaviour
- Medical or psychiatric reports
- Internal investigation findings

Tribunal under Anti-Sexual Harassment Act 2022 (ASHA)

(1) Jurisdiction (S.7 of ASHA)

- Hears any complaint of sexual harassment — employees, clients, contractors, public
- Accessible to minors & persons with disabilities (via guardian/next friend)

(2) Composition (S.12 of ASHA)

- Panel of 3: President/Deputy President + 2 Tribunal members

(3) Powers (S.19 & S.20 of ASHA)

- Order for the Respondent to issue a statement of apology to the complainant as specified in the order;
- Pay any compensation or damages not exceeding RM250,000.00 for any loss or damage suffered by the complainant in respect of the act of sexual harassment; or
- An order for the parties to attend any programme as the Tribunal thinks necessary.

(4) Procedures

- Complaint filed using Form 1 (4 copies) + RM30 fee
- Hearings closed to public; lawyers only allowed if complex
- Evidence: witnesses, documents, recordings admissible
- Award delivered within 60 days; final & enforceable

(5) Appeal (s.23 ASHA)

- To High Court only on “serious irregularity” grounds

Tribunal Form 1

P.U. (A) 80/2024

FORM 1

ANTI-SEXUAL HARASSMENT ACT 2022

ANTI-SEXUAL HARASSMENT (TRIBUNAL FOR ANTI-SEXUAL HARASSMENT)
REGULATIONS 2024

IN THE TRIBUNAL FOR ANTI-SEXUAL HARASSMENT

IN THE STATE OF _____

MALAYSIA

COMPLAINT NO.: _____

COMPLAINT OF SEXUAL HARASSMENT

Name of Complainant	:	
Name of Respondent	:	
Address of Respondent	:	
Occupation and Work Address of Respondent (if known)	:	
Telephone No./Handphone No. of Respondent (if known)	:	
Particulars of complaint of sexual harassment:		

Cont...

(for the record of Tribunal for Anti-Sexual Harassment only)

COMPLAINT NO:

Name of Complainant	:	
NRIC No. of Complainant	:	
Email address of Complainant	:	
Telephone No./Handphone No. of Complainant	:	
Address of Complainant	:	
Occupation and work address of Complainant	:	

Cont...

Order required: (refer to section 20 of the Act)

☐

I hereby declare **HAVE/ HAVE NOT** lodged the complaint on the above matter on any other legal platform. If yes, please state:

(SEAL)

Signature/Right thumb-print and full
name of Complainant/ Next friend or
Guardian *ad litem*

Secretary/ Staff of the Tribunal

Date:

Date of filing:

TO RESPONDENT:

You shall file the statement of defence in Form 2 within fourteen working days from the date of receipt of this Form.

Key Takeaways

- Accessible, low-cost remedy (RM30 filing fee)
- Faster than court (award within 60 days of hearing)
- Awards = legally binding, enforceable as court orders
- Victims may pursue Tribunal claim even if internal complaint already filed
- Significant shift: Government recognition of trauma + statutory sanction of perpetrators
- Employers must update handbooks & grievance procedures to reflect ASHA

Lim Po Seng v Resort Villa Golf Course Berhad (Award No. 471 of 2023)

Facts:

- Complainant informed her superior of the alleged sexual harassment incident, lodging a police report on the same day, and lodging a written complaint to the Human Resource Department. In response to the said complaint, the Company issued the Claimant a suspension letter on allegations he had committed serious misconduct in sexually harassing the Complainant.
- The Company **did not issue a show cause letter to the Claimant or take any statements from the Claimant**, and after conducting an internal investigation proceeded to notify the Claimant that a domestic inquiry will be held to consider three charges of misconduct (in brief — grabbing the Complainant's hand and moving it towards his crotch, trying to hug her without consent, and using sexually suggestive language).
- The panel of inquiry at the domestic inquiry found the Claimant guilty of all the charges, and the Company dismissed the Claimant.

Court findings:

- The Claimant was dismissed without just cause or excuse and awarded him 30 months wages (maximum backwages of 24 months, plus compensation in lieu of reinstatement of 6 months wages).
- The tone of the suspension letter issued to the Claimant suggested that the Company did not even care to state that it was only an allegation which required further investigation. The problematic language appears to be that the letter read: “In view of the above report and misconduct, you are being suspended [...]”.
- Regarding the charge that the Claimant had grabbed the Complainant’s hand and moved it towards his crotch, the Company did not produce any evidence to support this.
- The Company “rushed” to obtain “hasty statements” from witnesses two days before the domestic inquiry. The Company also “conveniently omitted” to obtain a statement from the Claimant and issue a show cause letter to seek his explanation.

Lim Po Seng v Resort Villa Golf Course Berhad (Award No. 471 of 2023)

Court findings:

- The formulation of the three charges of misconduct which led to the Claimant's dismissal was based on "a proven false" police report and complaint, and the evidence against the Claimant was rife with "contradiction and inconsistency".
- The manner in which the domestic inquiry was conduct was "unsatisfactory" and the Company reached a "biased conclusion" **without properly considering all material evidence.**
- The Court found that **there was overwhelming evidence that the Company had a "premeditated intention" of finding the Claimant guilty.** The Claimant had informed the Company that there was a CCTV at the location of the alleged incident which would prove his innocence, and also raised this during the domestic inquiry. However, the Company did not take any steps to produce the CCTV recording during the domestic inquiry or at the Industrial Court proceedings.

Best Practices in Handling Complaints

Follow the Code / Policy

- If a guideline or policy exists, it must be followed strictly
- Include clear timelines for investigation & decisions

Ensure Consistency

- Same process for all complaints
- Similar offences = consistent punishments
- Avoid perceptions of bias or unfairness

Best Practices in Handling Complaints

Fair Hearing for Accused

- Accused must be allowed to respond to allegations
- No decision without hearing both sides

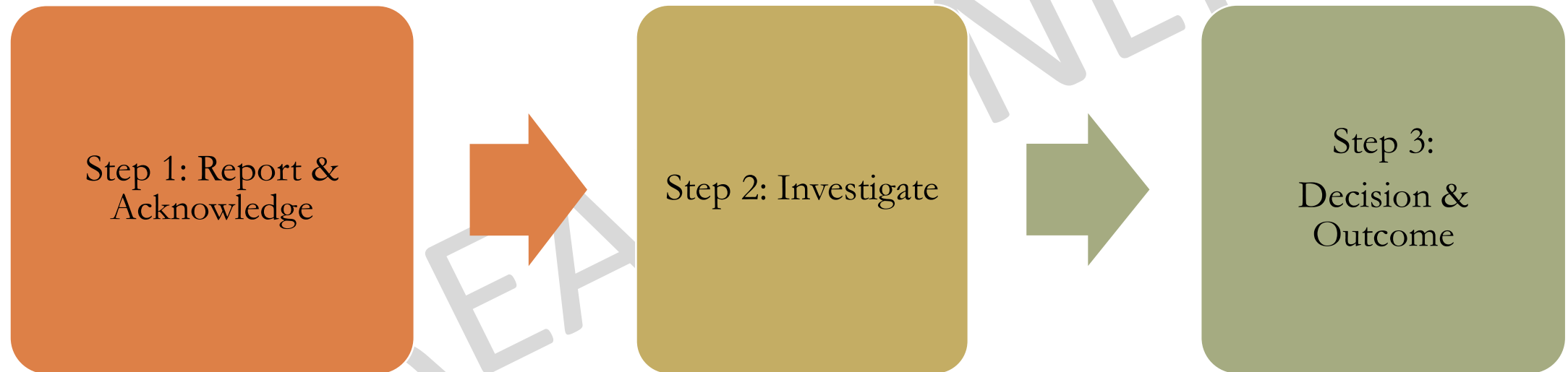
Fair & Thorough Investigations

- Collect full evidence before framing charges
- Impartial inquiry panel, documented process

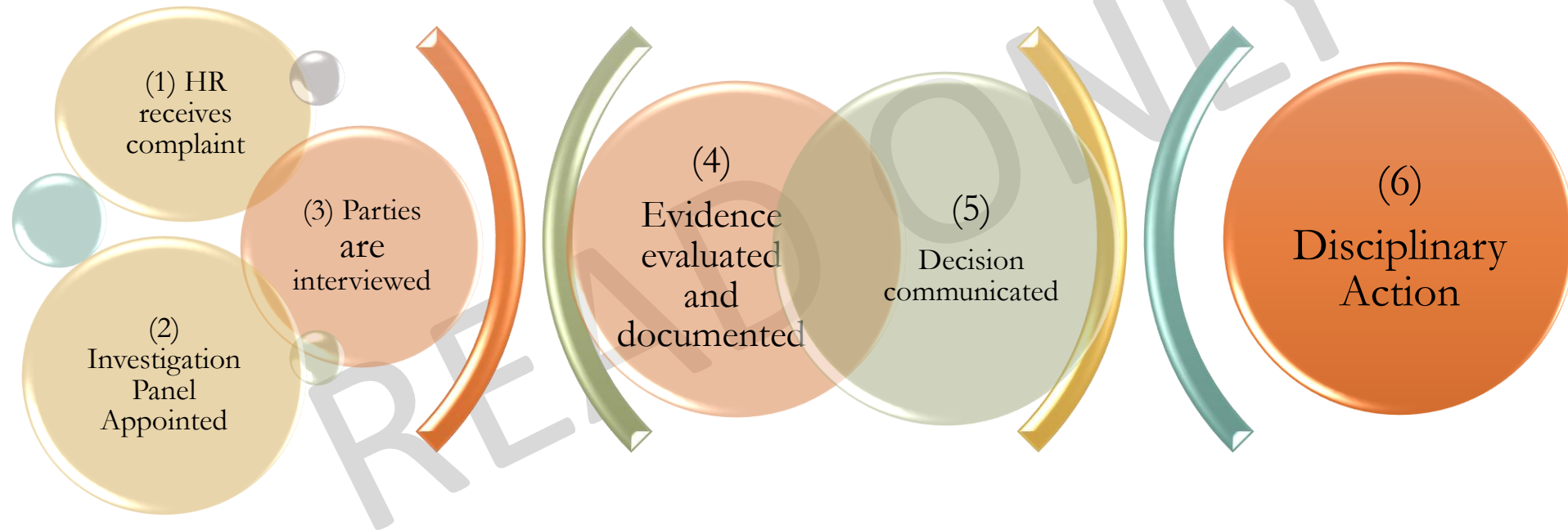
Keep Complainant Updated

- Regular status updates at defined milestones
- Builds trust, manages expectations

Complaint Procedure (Workplace Harassment)



Investigative Methods



Protection Measures For Employees

For Victims

- Encourage & support reporting without fear
- Ensure maximum confidentiality during reporting & investigations
- Restore original position if victim unfairly demoted or penalized
- Compensate for any monetary loss (e.g., benefits withheld, missed promotions)

For the Accused (if complaint baseless)

- Remedy losses suffered (reputation, position, benefits)
- Reinstate trust & workplace harmony

Final Thoughts

Zero Tolerance

- Sexual harassment is misconduct and a legal offence
- No excuses: “jokes” or “banter” are not defences

Employer's Duty

- Provide safe, respectful workplace (legal + moral duty)
- Act promptly: inquire, document, take proportionate action

Legal Framework

- Employment Act 1955, Industrial Relations Act 1967
- Penal Code (ss.354, 509), Communications & Multimedia Act 1998
- Anti-Sexual Harassment Act 2022 — Tribunal (TAGS)

Final Thoughts

Protection & Fairness

- Protect victims: confidentiality, support, restoration
- Protect accused: fair hearing, remedy if baseless

Culture Matters

- Training, awareness, leadership commitment
- Respect and accountability must be everyday practice

MANAGING REMOTE WORKERS AND DIGITAL NOMADS



Crystal Cha

- Assistant Director, Client Services Group (CSG)
- Marketing and ops professional with 14+ years of experience
- Worked across three continents in companies of all sizes, from startups to scalers to multinationals
- *For more information:*
crystal.cha@asb.edu.my

Asia School of Business:

Global Inquiry, Local Heart | Backed by world-class collaboration



BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA



- We develop **principled and transformative leaders** who drive progress across the emerging economies.
- Outstanding teaching and learning pedagogies designed to equip talent with **deep, regionally-informed expertise.**





Safeguard Your Business Against Data Breaches

Mike Lee Seang Yik

CHAN LEE & CO
ADVOCATES & SOLICITORS

DISCLAIMER

These brief slides have been prepared for ease of reference and sections referred to in the Statute have been paraphrased .
You are advised to refer to the actual wording of the Statute for a complete appreciation of its legal implication.

Professional advice should be sought before making decisions based on this general presentation.



Overview:

- Is your data protection policy PDPA-compliant?
- Discover best practices for breach detection, containment, and notification
- Could your business processes be unintentionally exposing you?

PM reveals attack on MAHB digital system with hackers demanding US\$10 mil



By Bernama / Bernama

25 Mar 2025, 01:42 pm



Aa

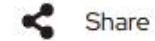


bernama

Prasarana confirms cybersecurity incident

9 MONTHS AGO

FMT Reporters



The public transport operator responds to social media reports that potentially 316GB of its data from its website has been compromised due to a ransomware attack.



— M

1

2

3

Nacsa investigates alleged breach exposing MyKad data of 17 million Malaysians

By CHRISTOPHER FAM



CYBERSECURITY

Wednesday, 04 Dec 2024

11:58 AM MYT

Related News



TECHNOLOGY 15 Jun 2025

WestJet probes cybersecurity incident affecting app and...

TECHNOLOGY 29 May 2025

Exclusive-Cybersecurity provider Netskope taps Morgan Stanley for US...



The agency urged the public to 'avoid spreading unconfirmed reports and only refer to verified information from the authorities'. — Photo by Lewis Kang'ethe Ngugi on Unsplash

Amendment to Personal Data Protection (PDP) Act 2010 tabled for first reading

By Qistina Sallehuddin, Nor Ain Mohamed Radhi - July 10, 2024 @ 1:52pm



NEWS BULLETIN

2. **Notice and Choice** Principle

3. **Disclosure** Principle

1. **General** Principle

4. **Security** Principle

**7 DATA PROTECTION
PRINCIPLES**

7. **Access** Principle

5. **Retention** Principle

6. **Data Integrity** Principle

KEY CHANGES IN THE AMENDMENT ACT

Replacement of the term
"data users" with "data
controllers"

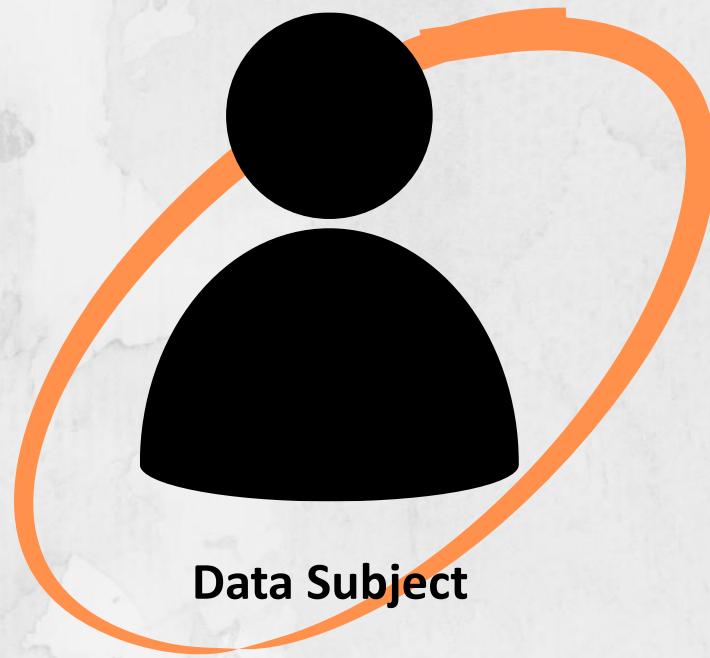
New mandatory personal
data breach notification
regime

Increased penalties for
breach of the Personal
Data Protection
Principles

New data protection
officer ("DPO")
appointment

Extension of the Security
Principle to data
processors

New right to data
portability for data
subjects



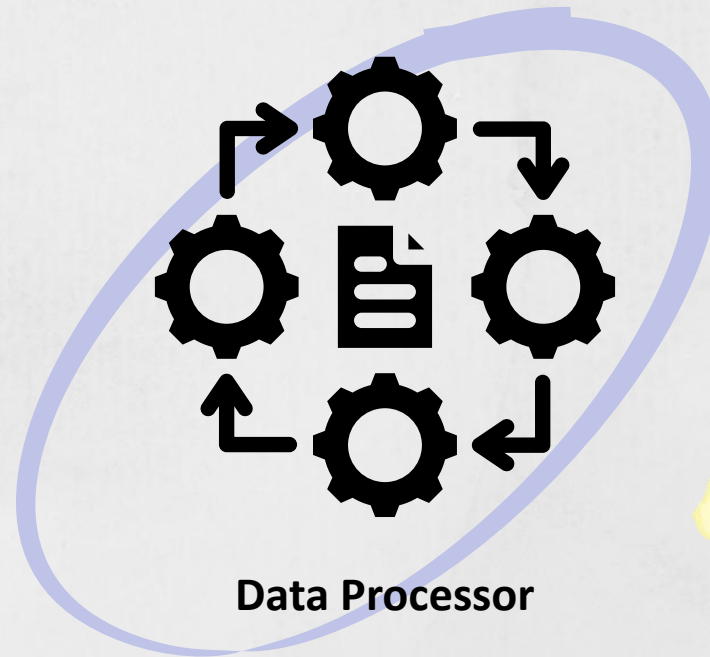
Data Subject



Data Protection Officer



Data Controller



Data Processor

What is
PERSONAL DATA?



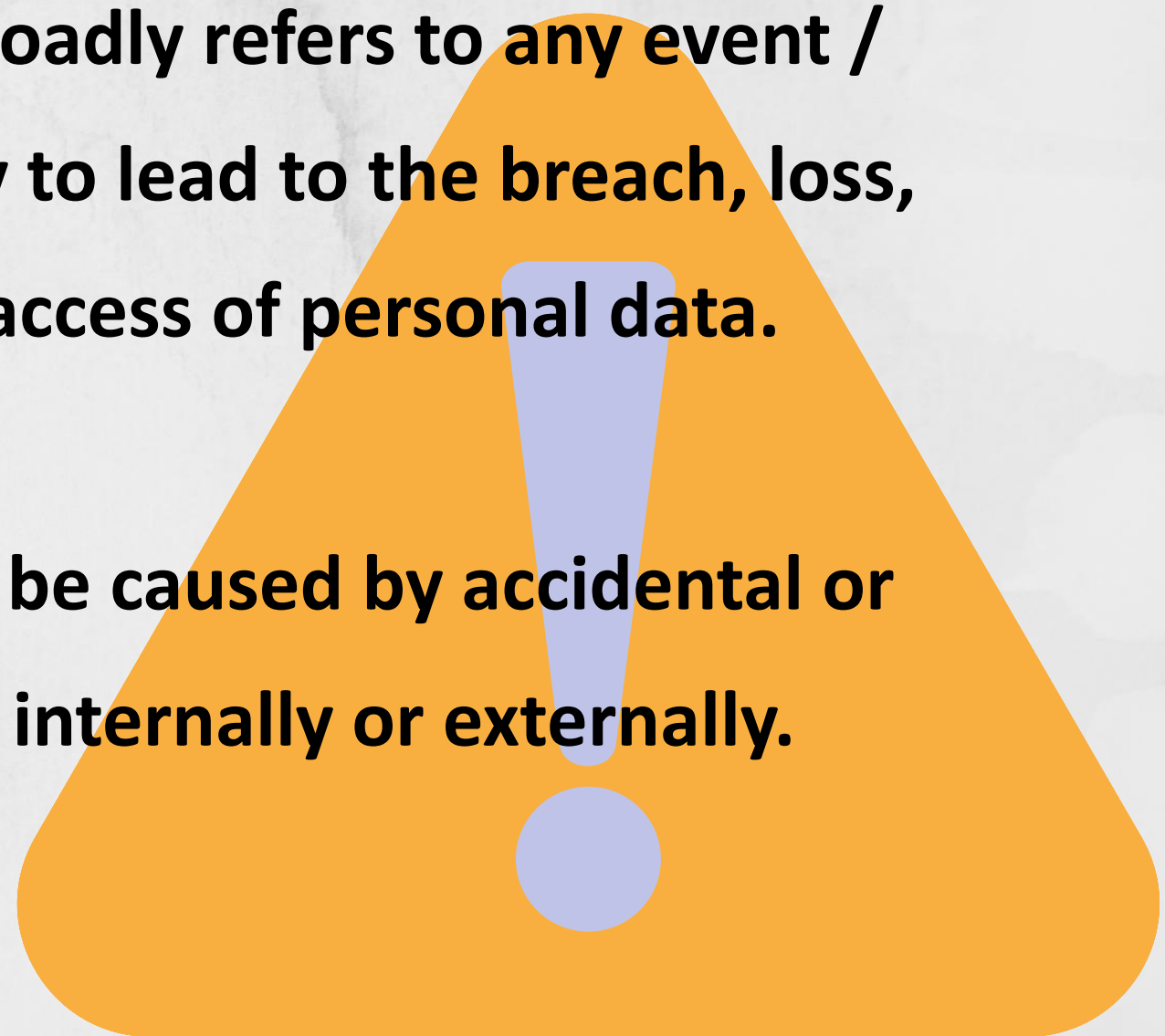
Procedure on Data Breach Notification (DBN)

What is **Personal Data Breach?**

A thick, vibrant red brushstroke underline that starts under the first word of the title and extends across the width of the text, ending with a slight upward curve on the right side.

A “personal data breach” broadly refers to any event / incident that leads or is likely to lead to the breach, loss, misuse or unauthorised access of personal data.

A personal data breach may be caused by accidental or deliberate actions, either internally or externally.





YES ~~NO~~

- (i) Access to personal data held by the data controller by unauthorised third party.
- (ii) Salesman accidentally sending a promotion email to the wrong recipient.
- (iii) Operation Manager accidentally losing / misplacing a company-issued laptop containing unencrypted personal data, leading to potential unauthorised access of personal data.



YES ~~NO~~

(iv) CEO misplacing or losing the clients' name card.

(v) An external party gaining access by unlawful means to the data controller's network or user accounts and extracting personal data.

(vi) Receptionist pass wrong cheque to the despatch.

Not all personal data breaches are notifiable to the Commissioner. A data controller is ONLY required to notify the Commissioner of a personal data breach if the personal data breach causes or is likely to cause “significant harm”.



What is **Significant Harm?**



Significant Harm

1. May result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property;
2. May be misused for illegal purposes;
3. Consists of sensitive personal data;
4. Consists of personal data and other personal information which, when combined, could potentially enable identity fraud; or
5. Is of significant scale.



Under Malaysia's Personal Data Protection Act (PDPA),

"SENSITIVE PERSONAL DATA"

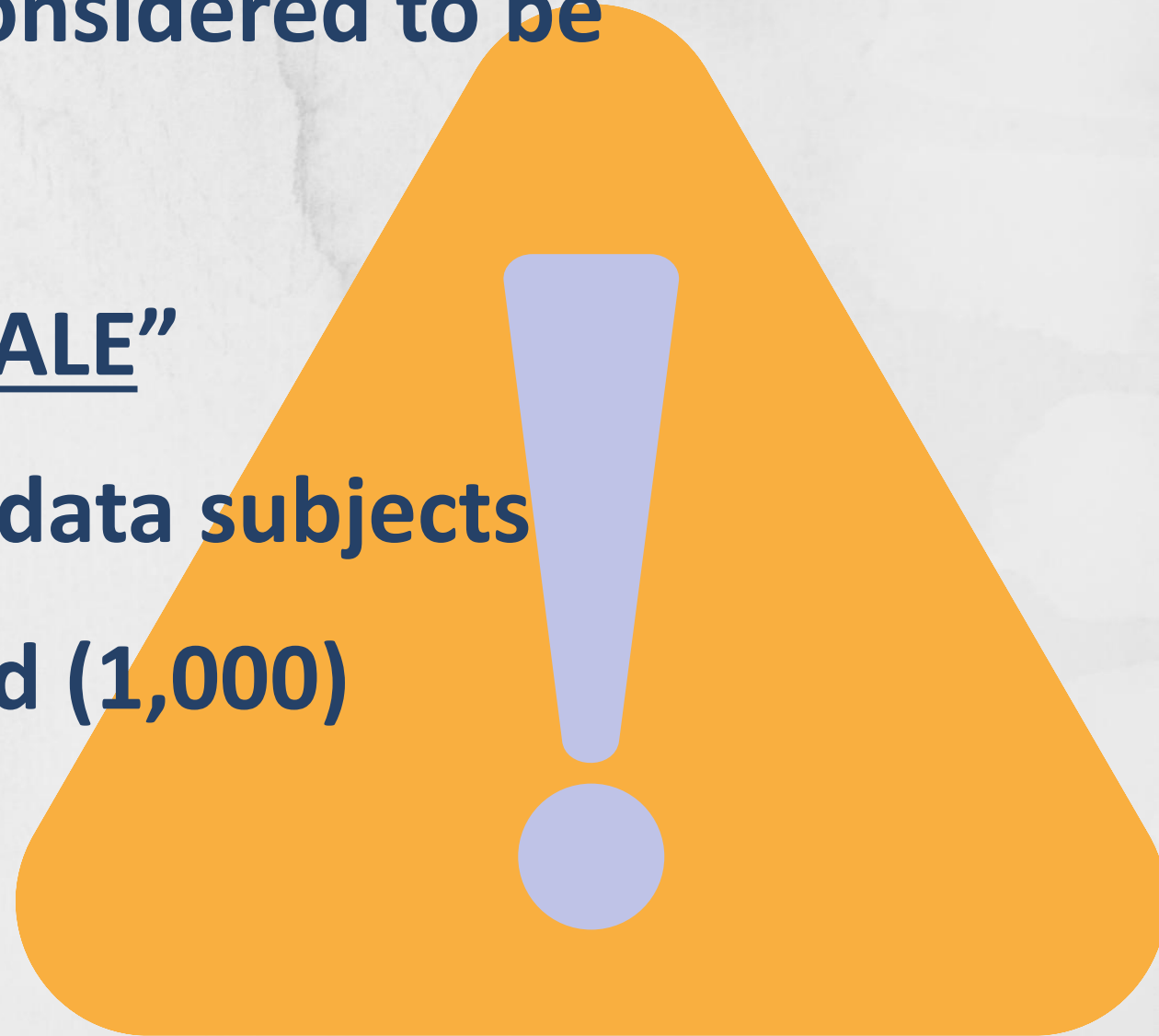
**includes information about an
individual's physical or mental health,
political opinions, religious beliefs,
any information related to the commission or
alleged commission of an offense and biometric data.**



**A personal data breach is considered to be
of**

“SIGNIFICANT SCALE”

**if the number of affected data subjects
exceeds one thousand (1,000)**



An employee loses a laptop
containing personal data of
customers.

~~YES~~
NO

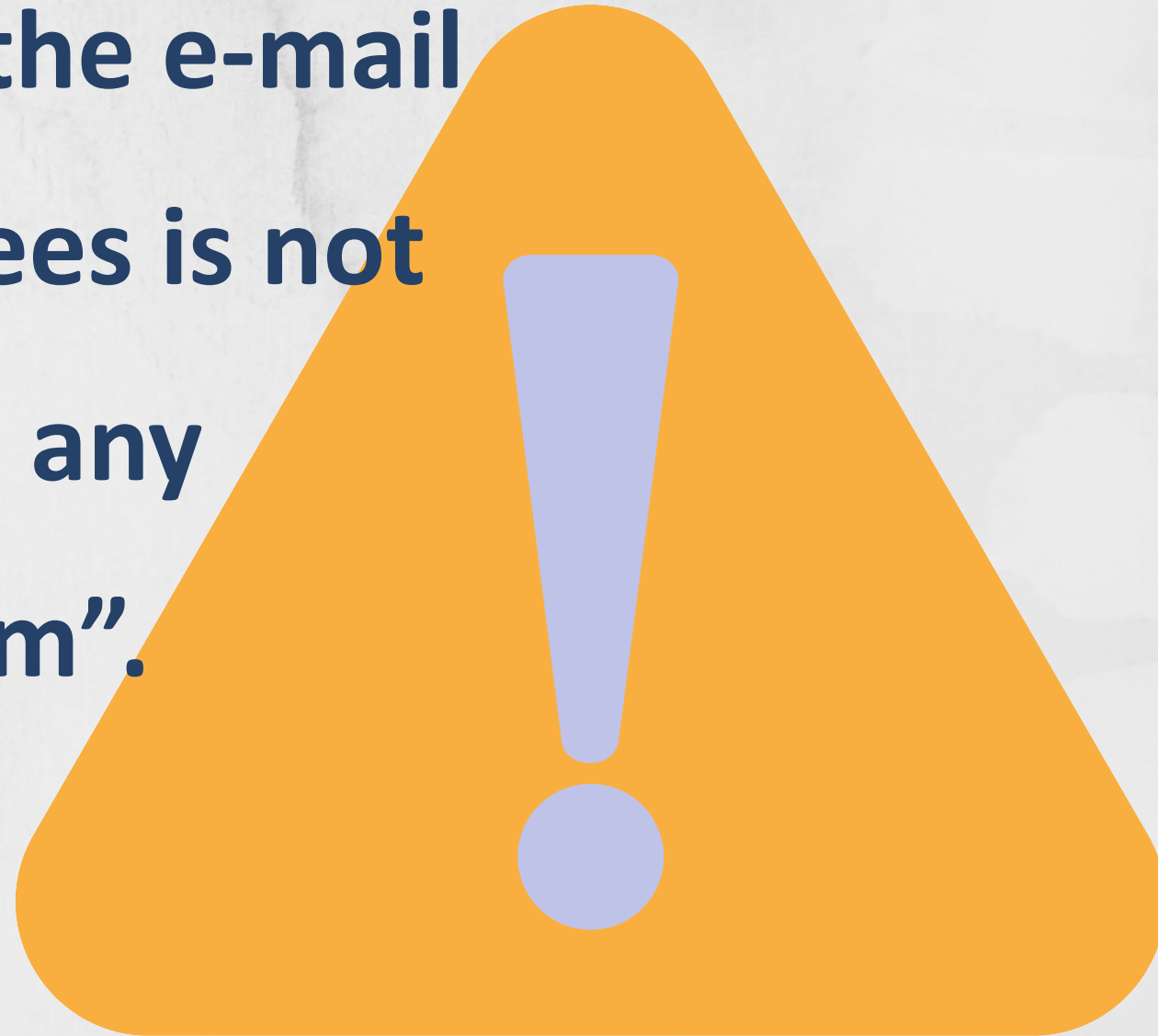
Is this Data Breach?

Theft of an encrypted laptop
containing the **email addresses** of
200 employees of an organisation

Should I notify Commissioner?



**NO, the disclosure of the e-mail
addresses of employees is not
likely to result in any
“significant harm”.**



Received notification of
unauthorised log in to company
work account?

YES ~~**NO**~~

Is this Data Breach?



Data controllers must notify the Commissioner within 72 hours if a breach:

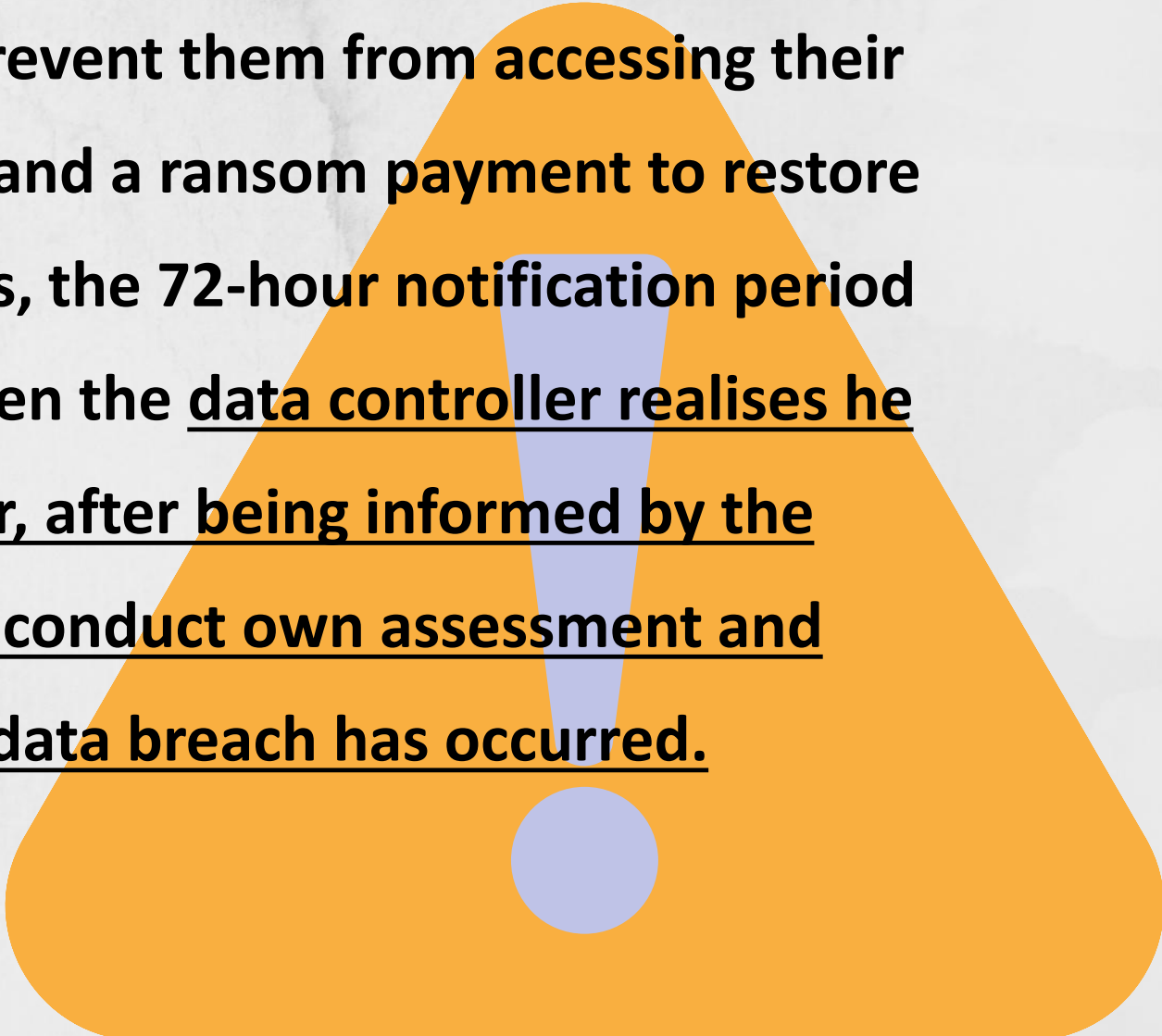
- Causes or is likely to cause significant harm
or
- Affects more than 1,000 people
- Notification can be made via the official website, email, or hand in hard copy.

Ransomware attack happened on 1 May
which is Public Holiday.

Data Controller realised he has lost access to
the data on 4 May after back to work from
holiday.

How to compute 72-hour timeframe?

A ransomware attack is a type of cyberattack in which criminals encrypt the victim's data and prevent them from accessing their system. The criminals then demand a ransom payment to restore the victim's access. In such cases, the 72-hour notification period to the Commissioner begins when the data controller realises he has lost access to the data or, after being informed by the cybercriminal of the breach, conduct own assessment and confirm that a personal data breach has occurred.



How to notify the Commissioner?

i. Completing the notification form available on the official website of the Department of Personal Data Protection (JPDP) at www.pdp.gov.my;

OR

ii. Completing the notification form in Annex B and submitting it to the official e-mail address dbnpdp@pdp.gov.my;

OR

iii. Completing the notification form in Annex B and submitting a hard copy to the Commissioner.

Notification in Phases

Notification is submitted by Data Controller within the prescribed seventy-two (72) hours



The Commissioner will issue a confirmation notice to the data controller upon receiving the personal data breach notification



Submit data breach details as soon as practicable and no later than thirty (30) days from the date of the notification made



ANNEX B: DATA BREACH NOTIFICATION FORM



DATA BREACH NOTIFICATION

This notification form is to be used when a data controller wishes to report a data breach to the Personal Data Protection Commissioner ("**Commissioner**").

Please note that the information requested in this notification form is non-exhaustive. The Commissioner may require further details of the incident to facilitate investigation.

Where and to the extent that it is not possible to provide all of the information requested in the notification form, is sufficient to complete the form only to the extent of the information available. Additional information to the Commissioner in phases as soon as practicable not later than thirty (30) days from the date of the initial notification.

PARTICULARS OF DATA CONTROLLER

**When should we notify
the Data Subject?**

A thick red curved line that starts under the word 'Subject' and extends to the right, curving slightly upwards at the end.



Data subjects must be notified within 7 days if a breach

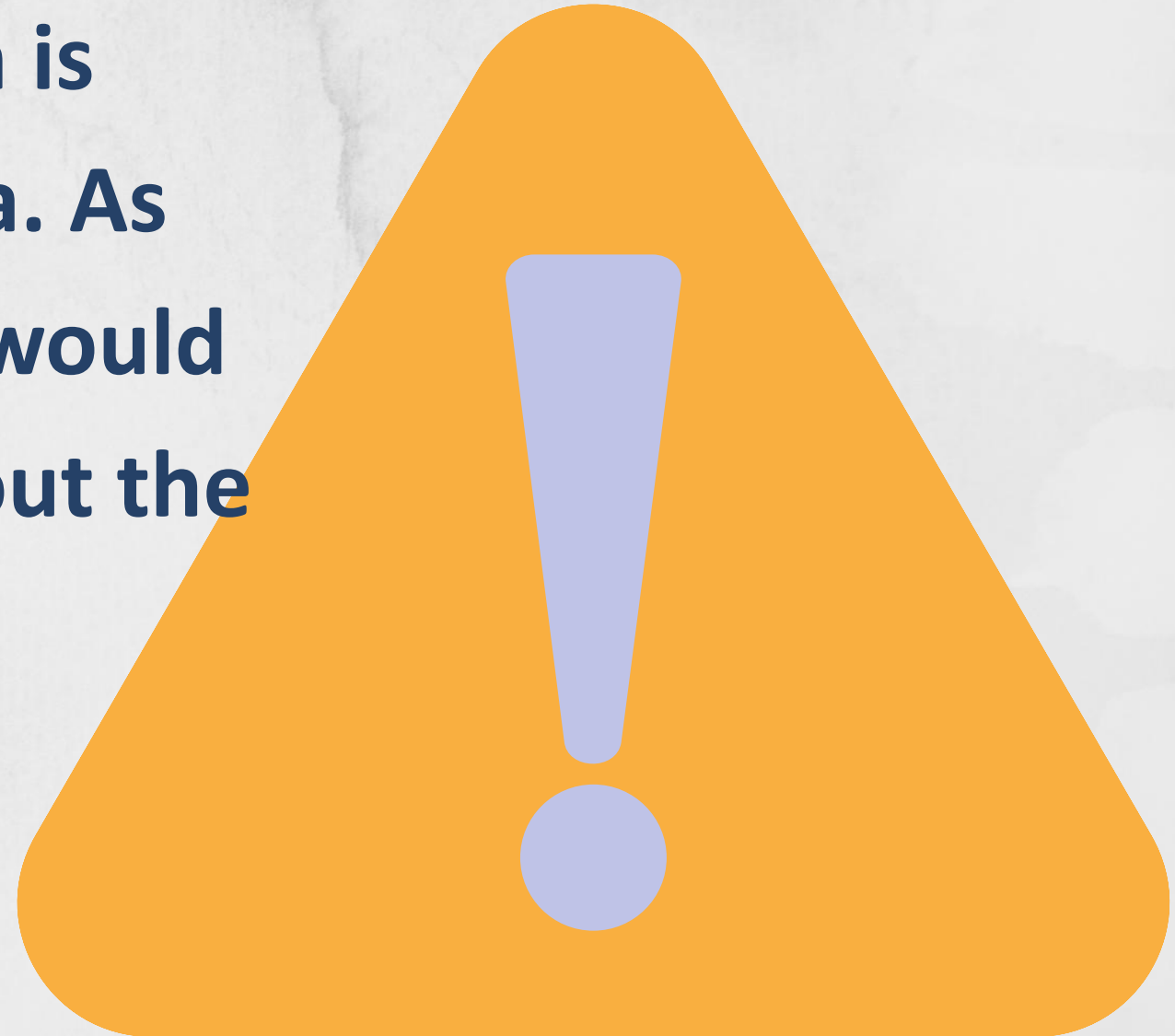
- Causes or is likely to cause significant harm.
- Notification can be made via the direct contact or public communication.

An investment firm suffers a cyberattack which results in the theft of customers' personal and financial information.

Should I notify Data Subject?



YES, there is significant harm as financial information is sensitive personal data. As such, the data subjects would need to be informed about the breach.

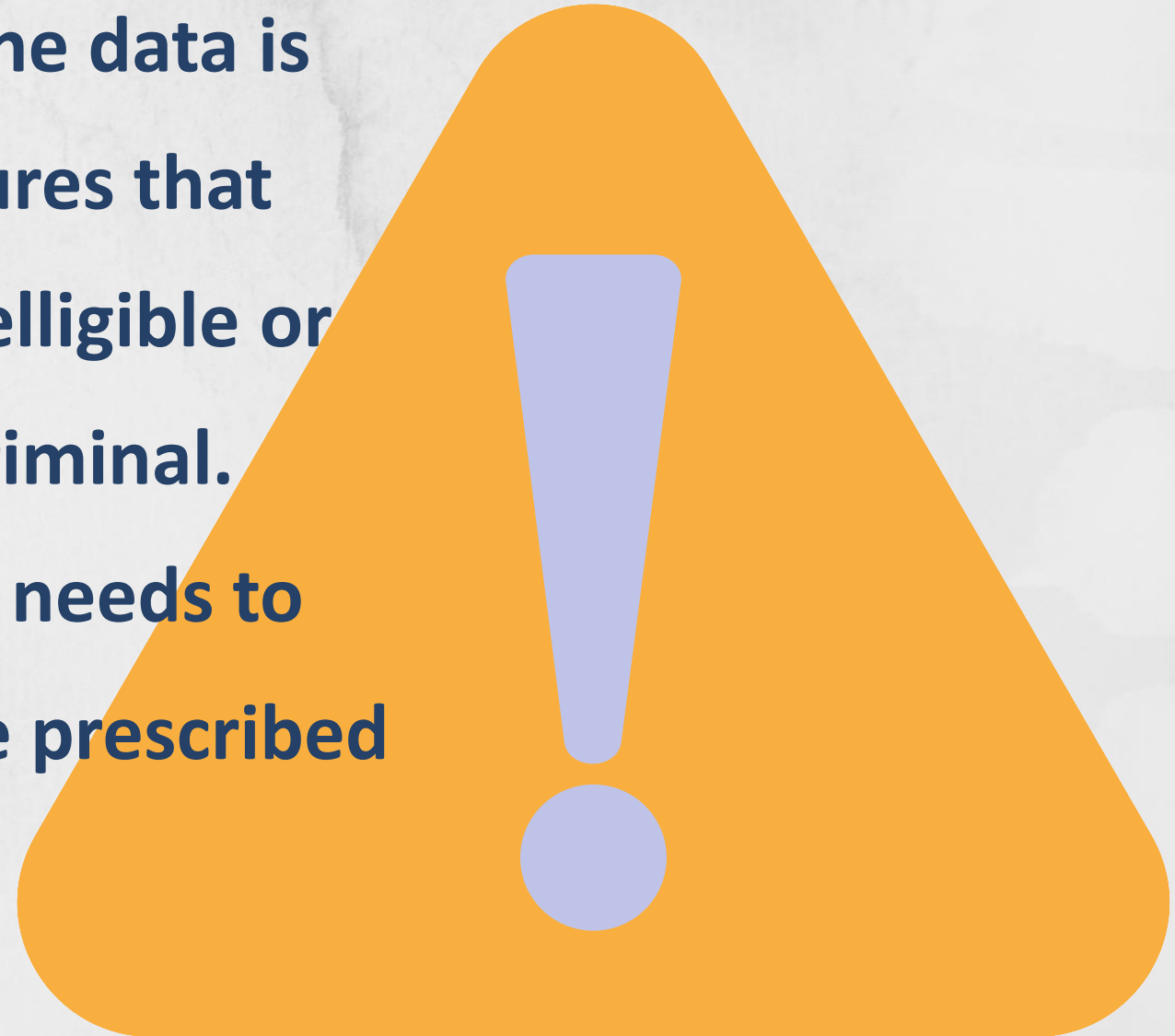


A cybercriminal hacked the server which contains customers' personal and financial data and gained control of the pharmaceutical supplier's server. **However**, the cybercriminal is not able to access the said personal and financial data as the pharmaceutical supplier had implemented two layers of security measures.

Should I notify Data Subject?

A thick red underline is positioned below the text 'Should I notify Data Subject?'. It starts under the first word and extends past the end of the sentence, ending in a small hook-like shape on the right side.

NO, in this situation, the data subjects do not need to be informed as the data is protected by security measures that render the information unintelligible or meaningless to the cybercriminal. However, the data controller needs to inform the Commissioner in the prescribed manner.



Manner of Notification

- a) Direct Notification to Data Subject with details
- b) If direct notification is not practicable or requires a disproportionate effort, alternative means of notification are allowed.



Examples of methods for notifying affected data subjects individually:

- email; ● SMS; ● direct messaging; and ● postal communication.

Examples of public communication:

- notification on the official website; ● notice in printed media; ● social media posts through the data controller's official pages or accounts; and ● automated notifications (push notification)

**Are we required to
lodge police report**



for Data Breach?

PDRM

- if involves criminal activity

BNM or SC or MCMC

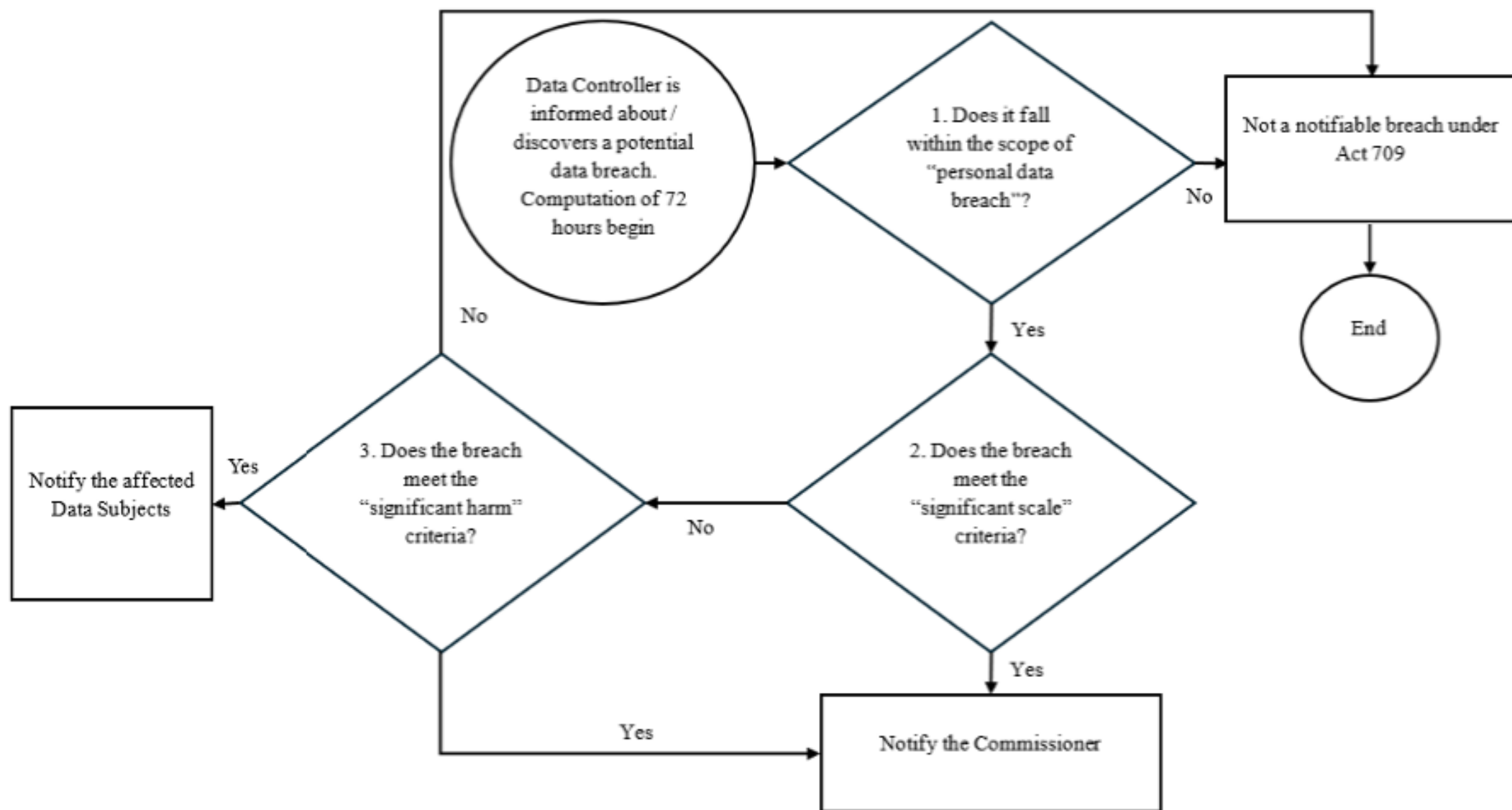
- sectoral cyber incident or data breach notification requirements

National Cyber Security Agency and National Critical Information Infrastructure

- where the data controller is a designated NCII Entity under the Cyber Security Act 2024

Please note that the list above is for reference purposes only. The data controller should conduct an independent assessment to determine the notification requirements under other applicable Malaysian laws and regulations.

**ANNEX A: FLOWCHART OVERVIEW OF THE DATA BREACH NOTIFICATION REQUIREMENT
UNDER THE ACT 709**



What is the scope of the PDPA when the retailer collects information and then pass it on to other suppliers in the network, for e.g., marketing agency.

If a data breach occurs at one of the suppliers, is the retailer liable?



To discharge its liabilities, the retailer must demonstrate that it has exercised all due diligence, including to enter into a data processing agreement with the marketing agency which states clearly the agency's responsibilities to protect personal data.



**Last but not least,
is Data Breach avoidable?**

YES ~~**NO**~~

What is your company's
Data Protection Policy?

Do you have
Data Breach Response Plan?

Have you conducted
Data Risk Assessment?



PUBLIC CONSULTATION PAPER NO. 2/2025:
DATA PROTECTION BY DESIGN GUIDELINE

Start Date: 20 March 2025

End Date: 19 May 2025

Data Protection by Design

(a) Proactive not Reactive;
Preventative not Remedial

(b) Privacy as the Default Setting

(c) Privacy embedded into design

(d) Full functionality – positive sum, not zero sum

(g) Respect for user privacy- keep it user-centric

(f) Visibility and transparency – keep it open

(e) End-to-end security – full lifecycle protection

Data Breach Response Plan

WHEN

- circumstances
- types of risk

WHAT

- action plan
- prevention
- recovery plan

HOW

- risk assessment
- communication plan

PUBLIC CONSULTATION PAPER NO. 1/2025

**DATA PROTECTION IMPACT ASSESSMENT
GUIDELINE**

Start Date: 20 March 2025

End Date: 19 May 2025

Data Protection Impact Assessment (DPIA)

WHO

HOW

WHEN

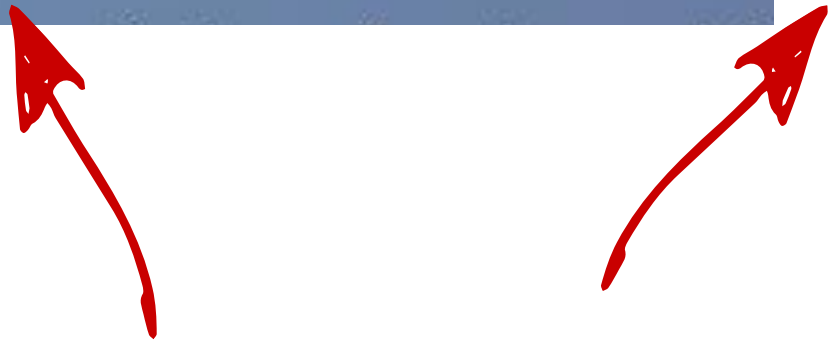
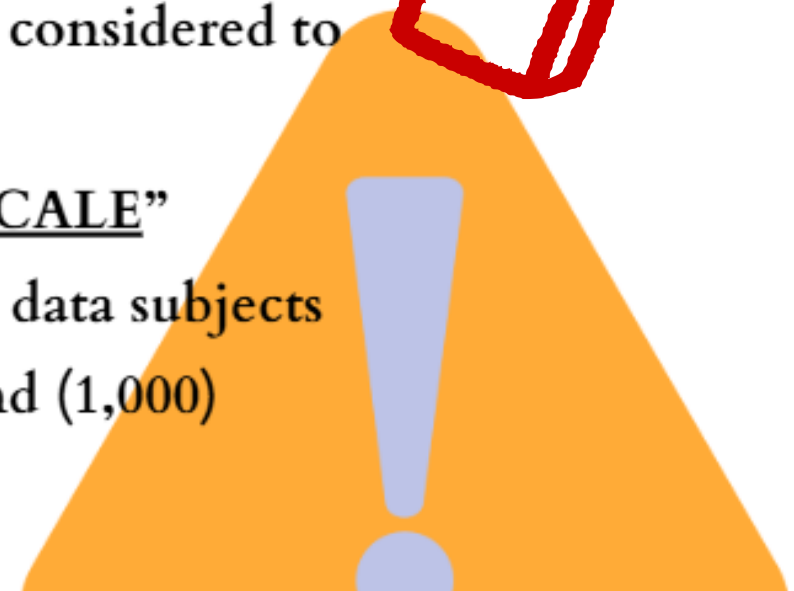
▪ Syarikat yang perlu mendaftar adalah syarikat yang tertakluk dalam golongan pengguna data berikut sahaja:

1. Komunikasi
2. Perbankan & Institusi Kewangan
3. Insuran
4. Kesihatan
5. Pelancongan & Hospitaliti
6. Pengangkutan
7. Pendidikan
8. Jualan Langsung
9. Perkhidmatan
10. Hartanah
11. Utiliti
12. Pajak Gadai
13. Pemberi Pinjam Wang

A personal data breach is considered to
be of

“SIGNIFICANT SCALE”

if the number of affected data subjects
exceeds one thousand (1,000)



D describe the processing operations;

E evaluate the necessity and proportionality of the processing operation in relation to the purposes;

I identify and analyse the specific risks on the protection of personal data for data subjects;

C consider measures to be taken to address the specific risks identified in order to safeguard the protection of personal data; and

A assess the overall residual risk level (e.g., high, medium, low) of the processing operation.

COMING SOON

Tips for Risk Management!



Identification

- “What personal data are we collecting, using, storing and sharing — and where is it?”
- Identify all sources and types of personal data the organization processes, how data is collected and stored, and who accesses it.

Assessment

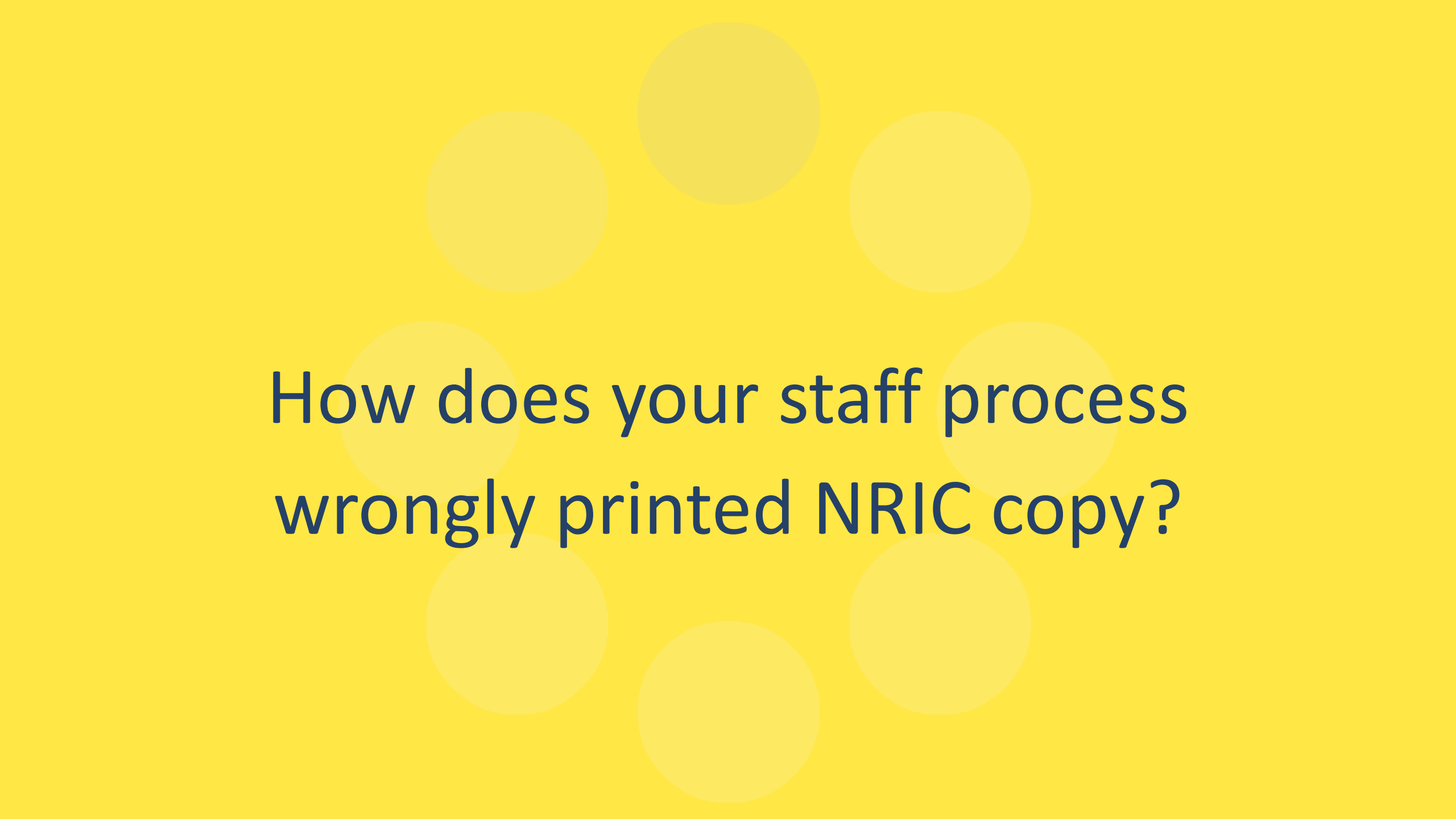
- “What are the risks associated with our handling of this data?”
- Assess the risks of unauthorized access, data leaks, misuse or non-compliance with PDPA.
- Consider are we collecting more data than needed or any risks in our third-party data handling.
- Discuss data breach cases and analyze what went wrong and what risks were overlooked.

Monitor

- “Are our processes working as intended to protect data?”
- Access logs (who accessed what data and when), retention practices (are we keeping data longer than necessary) and employee behavior (emailing personal data without encryption).
- The difference between a company that monitors compliance actively vs. one that ignores signs of weak controls.

Control

- Technical controls: encryption, passwords and access restrictions.
- Policy controls: data retention policies, privacy notices and SOPs.
- Disciplinary actions for non-compliance.

The background is a solid yellow color with several large, semi-transparent yellow circles scattered across it. The text is centered in the middle of the image.

How does your staff process
wrongly printed NRIC copy?



Countdown to 1 June 2025: Is Your Team Ready?

The reinforcement of the Data Protection Officer (DPO) role is coming into effect soon. As we are approaching 1 June 2025, organizations must ensure that their teams are well-prepared to meet data protection compliance requirements.

Last week, we conducted an in-house training session for [Japan Travel Bureau \(Malaysia\) Sdn Bhd](#), a tourism company with global presence - helping their local team to stay updated and equipped with the legal knowledge needed to protect clients' data effectively.

Is your organization ready?
Now is the time to assess, prepare, and empower your team.

Get in touch with us to arrange customized in-house training to meet your industry needs.

[#DataProtection](#) [#DPO](#) [#PDPA](#)



In industries like construction and production, debtor management isn't just an accounting function — it's a legal risk area that businesses cannot afford to ignore. That's why, "Paper trail is your best friend when it comes to protecting your business!"

A proactive legal strategy can make a significant difference — not just in recovering what's owed, but in preventing disputes before they arise.

Photo: A snapshot from our "Lim Kopi with Loyar Batik" session on 24/4, sharing about: Management of Debtors in Production and Construction Industries and Its Common Misconceptions

Look for legal expert for your debt recovery advisory? Please reach out to us for the effective legal strategy.

[#DebtRecovery](#) [#ConstructionLaw](#) [#DebtorManagement](#)



mike.lee@clcolaw.com

CHAN LEE & CO
ADVOCATES & SOLICITORS

thank you

Recent Trends in Disciplinary Actions and Content Creators

Presented By:

Alwin Rajasurya

Slides prepared by:

Kelly Yong

Ragavee Saravanan

Olivia Yeoh

DISCLAIMER

These brief slides have been prepared for ease of reference and sections referred to in the Statute have been paraphrased.

You are advised to refer to the actual wording of the Statute for a complete appreciation of its legal implication.

Professional advice should be sought before making decisions based on this general presentation.



PART 1:

WHAT ARE EMPLOYEES ALLOWED TO DO IN THE RECENT WORLD FULL OF CONTENT CREATORS?

INTRODUCTION

- With the rise of technological advancements, it comes as no surprise that problems in the workplace are also evolving.
- With all employees being in a possession of a mobile phone and the rise of social media, the boundaries between an employee's work and personal has begun to blur, inviting types of misconduct and employment issues that may have never even crossed the minds of employers only a few years ago

Q & A WITH THE FLOOR

EXAMPLES OF NEW ISSUES THAT HAVE ARISEN

- Based on your knowledge and experience, do you think employees should be allowed to do the following?
 - Take pictures of their colleagues and post it to social media without their consent?
 - What if the employees take the picture but does not do anything with it, ie. Post it anywhere?
 - Livestream in the office while taking footage of their environment and colleagues and replying to chat messages?
 - What if they only livestream in the office, but only of themselves, not replying to any of the chat messages, and are paying full attention to their work?

Cont...

- Based on your knowledge and experience, do you think employers should be allowed to do the following?
 - What are you allowed to make your employees do for work?
 - Can you make your employees write articles for work?
 - Can you make your employees make informative tiktok videos for work?
 - Can you make your employees make dance tiktok movies for work?
 - How is being asked to record videos for tiktok different from being asked to write an article?

Cont...

- What happens when an employee refuses to participate?
- Are you allowed to dismiss them based on their refusal to participate in situations where this forms a part of their contract?
- Are you allowed to dismiss them based on their refusal to participate in situations where this does NOT form a part of their contract?
- Is this a matter of an employee's job scope or consent?

CASE STUDIES

Case Study: What can an employee post on their own social media?

Where an employee uses images of the Company with a specific private group of employees — does not constitute misconduct / just termination

- The Court held that using such pictures for promotion and invitation to attend a Union dinner does not constitute exposing the Company's branding to unnecessary adverse publicity risk - *Amm Mashor Mahfiz bin Abdul Wahab v Malaysia Airlines Bhd [2022] 1 ILJ 22*
- While the posting was unauthorised, but the misconduct was **not** serious enough to warrant dismissal

Case Study: Can an Employee run a side business on Social Media if already working at a Company?

Where an employee starts an online business where there is specific clauses that prevents an employee from doing so — may constitute misconduct

- Employee in this case was taking longer lunch breaks to run her business on social media, where Company has managed to establish that her work performance had been hindered, may constitute misconduct - *Nurul Hanisah bt Mohd Isa v Continental Tyre PJ Malaysia Sdn Bhd [2025] ILJU 154*

Case Study: Can an Employee post negative comments about superiors / Company on their personal account?

Employee who posted vulgar complaints and negative comments on her social media about her superior and Company dismissed — court upheld dismissal

- Employee in this case was using vulgar language to describe her Company and her superiors on her personal social media accounts. Although she did not mention the name of the Company, court held that dismissal was fair and just - *Ng Seok May @ Angie Sabrina v Maxis Broadband Sdn. Bhd. [2020] ILJU 42*
- Due process = just dismissal

Case Study: What happens when employers do not go through necessary inquiry before terminating?

Employee who posted vulgar derogatory Facebook comments about his Superior and Company, resulting in dismissal — court found dismissal to be unjust and unfair

- Employee was called to a meeting (treated as a Domestic Inquiry) without show cause letter or notice, where he admitted and apologised, but was dismissed immediately.
- Court found that due to there being no due process and found the dismissal to be unjust and unfair - *Mohd Azizi Sohan v Asian Kitchen (M) Sdn Bhd [2017] 4 ILR 376*
- No fair process = unfair dismissal

Cont...

Reasons for the Court's Decision:

- No fair process – no show cause, hasty inquiry, decision-makers sat in Domestic Inquiry.
- Handbook unclear – only covered misconduct at workplace or during hours.
- Comments = misconduct, but not serious enough for dismissal.

Case Study: Can an Employee be terminated for defamatory comments?

Two long-serving MAS flight stewardesses were dismissed after posting negative/defamatory Facebook comments, and also reporting sick but attended a Union gathering – **Court upheld dismissal**

- Although both employees claimed their medical leaves to be legitimate, the Court still considered them guilty of malingering (misusing medical leave) and considered the defamatory and damaging Facebook posts to be **serious misconduct** - *Farahtina binti Kassim & Anor v Malaysian Airline System Berhad [2018] ILJU 88*

Case Study: Can an Employee be sued over defamatory comments?

Employee who posted several statements in Facebook stages criticising Company and Members of staff — Court upheld that comments were defamatory and ordered Damages

- Employee in this case made defamatory comments towards Company, ie. Saying that the company was **cheating, greedy**. Court considered the statements made to be defamatory and ordered the Employee, who was the Defendant to pay damages - *GS Realty Sdn Bhd v Lee Kong Seng [2018] MLJU 1902*

Case Study: What happens when an Employee leaks CCTV Footage?

An Airport employee who was in charge of monitoring CCTV Footage accidentally leaked a recording showing a van accident — court upheld the decision to terminate the employee

- Although the Employee only shared the video to a WhatsApp group consisting of former employees, it was disseminated and eventually got leaked to social media and news outlets, causing harm to the Company's reputation - *Mohd Azmin Mohd Tamin v Malaysia Airline Berhad [2019] 2 LNS 1093*

Cont...

- Court held:
 - Breach of **trust and confidence** justified termination
 - **No Domestic Inquiry required** since misconduct was admitted by the Claimant himself when issued with a show cause letter

PART 2:

HOW CAN EMPLOYERS
NAVIGATE EMPLOYEES OF A
DIGITAL ERA AND PREVENT
MISCONDUCT BEFORE IT
HAPPENS?

Employer Insights

- **Social media is not private:**
 - Posts, even in “closed” groups, can reach the public and damage the company’s reputation, **employers can take action for messages disseminated in closed groups**
- **No absolute free speech:**
 - Union or personal opinions do not excuse defamatory or damaging posts against the company
- **Handbook & policies:**
 - Clear rules on social media, sick leave, and professional conduct help employers take firm action
- **Fair process:**
 - Even if Domestic Inquiry is skipped, ensure misconduct is well-documented and evidence-based to withstand scrutiny.

Employer's Perspective

- **Trust & confidence** = backbone of employment
- Sharing **confidential info** = serious breach of duty
- Conduct **inside or outside office hours** can justify dismissal
- **No intent or financial loss needed** – reasonable grounds are enough
- Especially relevant for industries with **security, reputation, and content creators**

Employer's Takeaways

- If misconduct is **admitted**, **Domestic Inquiry** not required
- Still ensure process is **fair & documented**:
 - Issue **show cause letter**
 - Record employee's **response/admission**
- Maintain **clear policies** in handbooks:
 - Misuse of confidential info
 - **Social media activity** harming employer
 - Behaviour damaging company's **reputation**
- Strong policies help defend decisions in the **Industrial Court**

Employer Insights

- Always issue a **show cause letter** – state charges clearly, allow time for defence.
- **Domestic Inquiry** must follow **natural justice**: impartial panel, right to respond, proper documentation.
- Ensure **proportionality**:
 - Not all misconduct = dismissal.
 - Consider warnings, suspension, demotion first.
- Document all steps – protects company in Industrial Court.

CONCLUSION

- Prevention is better than cure, prevent problems before they arise
- Review & update **Employee Handbook**:
 - Cover **off-duty conduct & social media activity** harming reputation.
 - Use clear, specific definitions of misconduct.
- Ensure training is conducted and memos are given so that employees are clear of the necessary rules

THANK YOU

For any queries, please contact:

MESSRS ALWIN RAJASURYA

Unit 1305, Amcorp Tower, Amcorp
Trade Centre, 18, Persiaran Barat,
46050 Petaling Jaya, Selangor Darul
Ehsan.

Email: general@arlegal.my

Telephone No.: 03-7613 7605