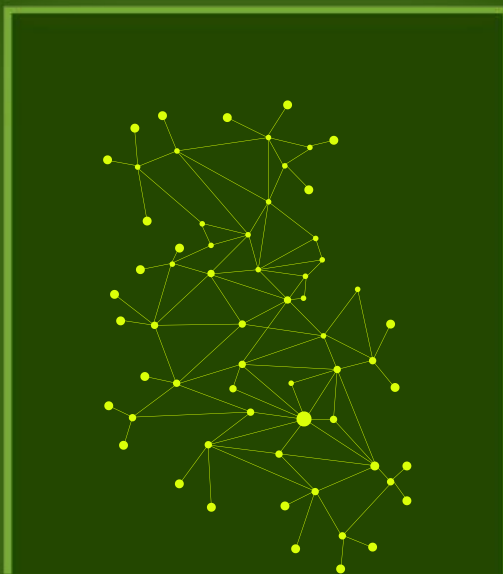
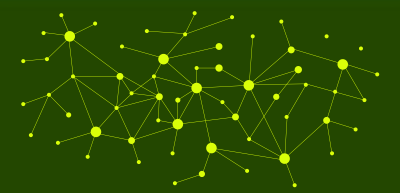




DPO TALK New Sanctions and Data Security Law **DPO Actions**

 8:30 AM - 12:00 PM

 Wed, 30 September, 2026

 **Mars Conference Hall**
La Vela Saigon Hotel, 280 Nam Ky Khoi Nghia, Xuan Hoa ward, HCMC



EVENT HIGHLIGHTS



Reference & Disclaimer

This material is intended solely for attendees of the event **“DPO Talk: New Sanctions and Data Security Law - DPO Actions”** and is provided for internal discussion and reference purposes only. The content should be read together with the accompanying speaking information to fully reflect the session’s context.

It shall not constitute, and should not be construed as, any professional, legal, or regulatory advice. Data Protectify makes no representation or warranty, express or implied, regarding their suitability of the information herein and assumes no responsibility or liability for any reliance placed on it or actions taken based on it.

Any reproduction, distribution, disclosure, adaptation, or use for any other purposes is strictly required a prior written consent from Data Protectify.





SECTION 1

VIETNAM DATA & TECH REGULATORY LANDSCAPE





Personal Data Protection Law

Effective Date:

01/01/2026



Decree No. 356/2025/ND-CP guiding the Personal Data Protection Law

Effective Date:

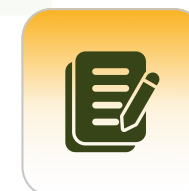
01/01/2026



Decree No. 330/2026/ND-CP on administrative penalties in the field of cybersecurity and personal data protection

Effective Date:

19/08/2026



Decision No. 778/QD-BCA-A05 announcing newly issued and abolished administrative procedures in the field of personal data protection under the state management of the Ministry of Public Security

Effective Date:

09/02/2026





Data Law

Effective Date
01/07/2025



Decree No. 169/2025/ND-CP
*on science, technology and
innovation activities and data
products and services*

Effective Date
01/07/2025



Decree No. 347/2026/ND-CP
*amending and supplementing a
number of articles of Decree No.
169/2025/ND-CP and other Decrees*

Effective Date
15/09/2026



Decree No. 314/2026/ND-CP
on Data Platform

Effective Date
25/09/2026



Decree No. 165/2025/ND-CP
guiding the Data Law

Effective Date
01/07/2025



Decree No. 363/2026/ND-CP
*on Administrative penalties for
violations in the data sector*

Effective Date
11/11/2026



Decision No. 20/2025/QD-TTg
*promulgating the List of Important
Data and Core Data*

Effective Date
01/07/2025



Decision No. 804/QD-TTg
*promulgating the List of Datasets for
Artificial Intelligence Development in
Essential Sectors*

Effective Date
06/05/2026





Law on Artificial Intelligence

Effective Date:

01/03/2026



Decree No. 142/2026/ND-CP *guiding the Law on Artificial Intelligence*

Effective Date:

01/05/2026



Decision No. 804/QD-TTg *promulgating the List of Datasets for Artificial Intelligence Development in Essential Sectors*

Effective Date:

06/05/2026



Decision No. 33/2026/QD-TTg *promulgating the List of High-Risk Artificial Intelligence Systems*

Effective Date:

15/08/2026



Decision No. 1671/QD-TTg *approving the National Strategy on Artificial Intelligence through 2030, with a vision toward 2045*

Effective Date:

28/08/2026





Law on Cybersecurity

Effective Date
01/07/2026



Decree No. 327/2026/ND-CP *

Effective Date
19/08/2026



Decree No. 329/2026/ND-CP
on the cybersecurity protection force

Effective Date
19/08/2026



Decree No. 330/2026/ND-CP
on administrative penalties in the field of cybersecurity and personal data protection

Effective Date
19/08/2026



Decree No. 331/2026/ND-CP
on cybersecurity protection for information systems

Effective Date
19/08/2026



Decree No. 332/2026/ND-CP
on business activities involving cybersecurity products and services

Effective Date
19/08/2026



Decree No. 333/2026/ND-CP
detailing certain articles and implementation measures of the Cybersecurity Law

Effective Date
19/08/2026



Decree No. 328/2026/ND-CP
on preventing and combating fake news and false information

Effective Date
05/10/2026

**Decree No. 327/2026/ND-CP on prevention and handling of information and acts using information technology, computer networks, telecommunications networks and electronic means to infringe upon national security, social order and safety in cyberspace*
- Internal -





Law on Digital Transformation

Effective Date:

01/07/2026



Decree No. 224/2026/ND-CP *guiding the Law on Digital Transformation*

Effective Date:

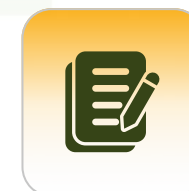
01/07/2026



Decision No. 433/QD-TTg *approving the Digital Transformation Scheme for Small and Medium-Sized Enterprises for 2026–2030*

Effective Date:

16/03/2026



Decision No. 1266/QD-TTg *approving the National Digital Transformation Strategy for 2026–2030, with orientations toward 2045*

Effective Date:

14/07/2026





Law on
Electronic Transactions

Effective Date:

01/07/2024



Draft Law on
Electronic Identification and
Authentication

Draft



Decree No. 69/2024/ND-CP
*on electronic identification and
authentication*

Effective Date:

01/07/2024



Decree No. 320/2026/ND-CP
*amending and supplementing a
number of articles of Decree No.
69/2024/ND-CP on electronic
identification and authentication*

Effective Date:

28/09/2026





BANKING

Law on Credit Institutions

Effective Date
01/07/2024

Decree No. 117/2018/ND-CP

on confidentiality and provision of customer information by credit institutions and foreign bank branches

Effective Date
01/11/2018

Circular No. 09/2020/TT-NHNN

on information system security in banking operations

Effective Date
01/01/2021

Circular No. 50/2024/TT-NHNN

on safety and security for the provision of online services in the banking sector

Effective Date
01/01/2025

Circular No. 15/2023/TT-NHNN

on credit information activities of the State Bank of Vietnam

Effective Date
01/01/2025

Circular No. 77/2025/TT-NHNN

amending Circular No. 50/2024/TT-NHNN on security and confidentiality in online banking services

Effective Date
01/03/2026

Circular No. 46/2026/TT-NHNN

amending and supplementing a number of articles of Circular No. 15/2023/TT-NHNN on credit information activities of the State Bank of Vietnam

Effective Date
01/11/2026

Draft Circular

on Safety, Risk Management and Deployment Conditions for the Application of Artificial Intelligence in the Banking Sector

Draft





E-COMMERCE

Law on E-Commerce

Decree No. 248/2026/ND-CP
guiding the Law on E-Commerce

Effective Date
01/07/2026

Effective Date
01/07/2026



HEALTH

Decree No. 102/2025/ND-CP
on health data management

Circular No. 13/2025/TT-BYT
*on the use and management of
electronic medical records*

Effective Date
01/07/2025

Effective Date
21/07/2025



TELECOMMUNICATIONS

Law on
Telecommunications

Effective Date
01/07/2024

Decree No. 163/2024/ND-CP
guiding the Law on Telecommunications

Effective Date
24/12/2024

Decree No. 174/2026/ND-CP
*on penalties for administrative violations in the fields of
postal services, telecommunications, radio frequencies,
electronic transactions and information technology*

Effective Date
01/07/2026





CONSUMER



Law on Protection of Consumer Rights

Effective Date
01/07/2024



Decree No. 98/2020/ND-CP

on penalties for administrative violations in commercial activities, production and trading of counterfeit and banned goods, and protection of consumers' rights

Effective Date
15/10/2020



Decree No. 17/2022/ND-CP

amending and supplementing a number of articles of decrees providing for administrative penalties in the fields of chemicals and industrial explosives; electricity, hydropower dam safety, economical and efficient use of energy; commercial activities, manufacture and trade in counterfeit and prohibited goods, protection of consumer rights; petroleum activities, and petroleum and gas business.

Effective Date
31/01/2022



Decree No. 24/2025/ND-CP

amending and supplementing a number of articles of Decree No. 98/2020/ND-CP and related Decrees

Effective Date
21/02/2025



CHILDREN



Law on Children

Effective Date
01/06/2017



Decree No. 56/2017/ND-CP guiding Law on Children

Effective Date
01/07/2017





SECTION 2

SANCTION FOR PERSONAL DATA PROTECTION VIOLATIONS



THE ADMINISTRATIVE SANCTIONING LIFECYCLE



OVERVIEW OF KEY SANCTIONING PRINCIPLES

01

ADMINISTRATIVE VIOLATION

A non-compliance of state-management rules that is not a crime but is sanctionable by law.

Fault-based

Non-compliance

Not a crime

Expressly sanctionable

One violation, one penalty

Art. 2.1, 3.1(d) LAVH

02

COMPLETED & ONGOING VIOLATION

COMPLETED

End
before detection

ONGOING

Still occurring
when detected

A violation ends when the **obligation is fulfilled**, or on the **actual end date confirmed by the authority**.

Art. 8.1 D118, Art. 3.2-3.3 D330

03

LIMITATION PERIOD

01 YEAR

Completed

from the end of the violation

Ongoing

from detection

Art. 6.1 LAVH, Art. 3.1 D330

04

APPLICABLE REGULATIONS

BY TIME

Time of commission: Decrees in force when violation occurred

Spanning several regulations:

- **Completed:** Decree in force at its end
- **Ongoing:** Decree in force at detection

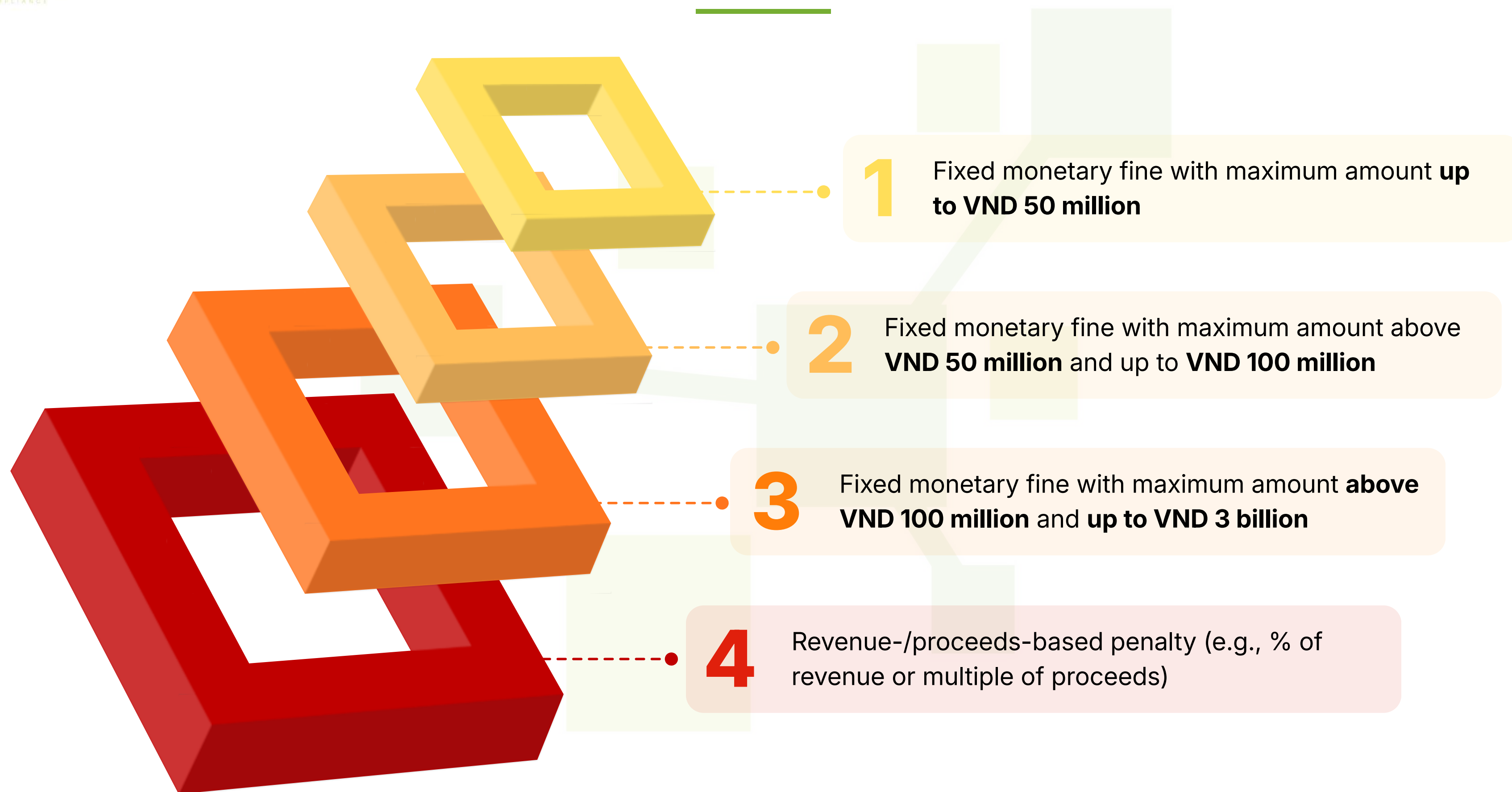
BY SECTOR

Violations not cover by Decree 330: sectoral decree shall apply
Overlap*: The nature of the breach decides

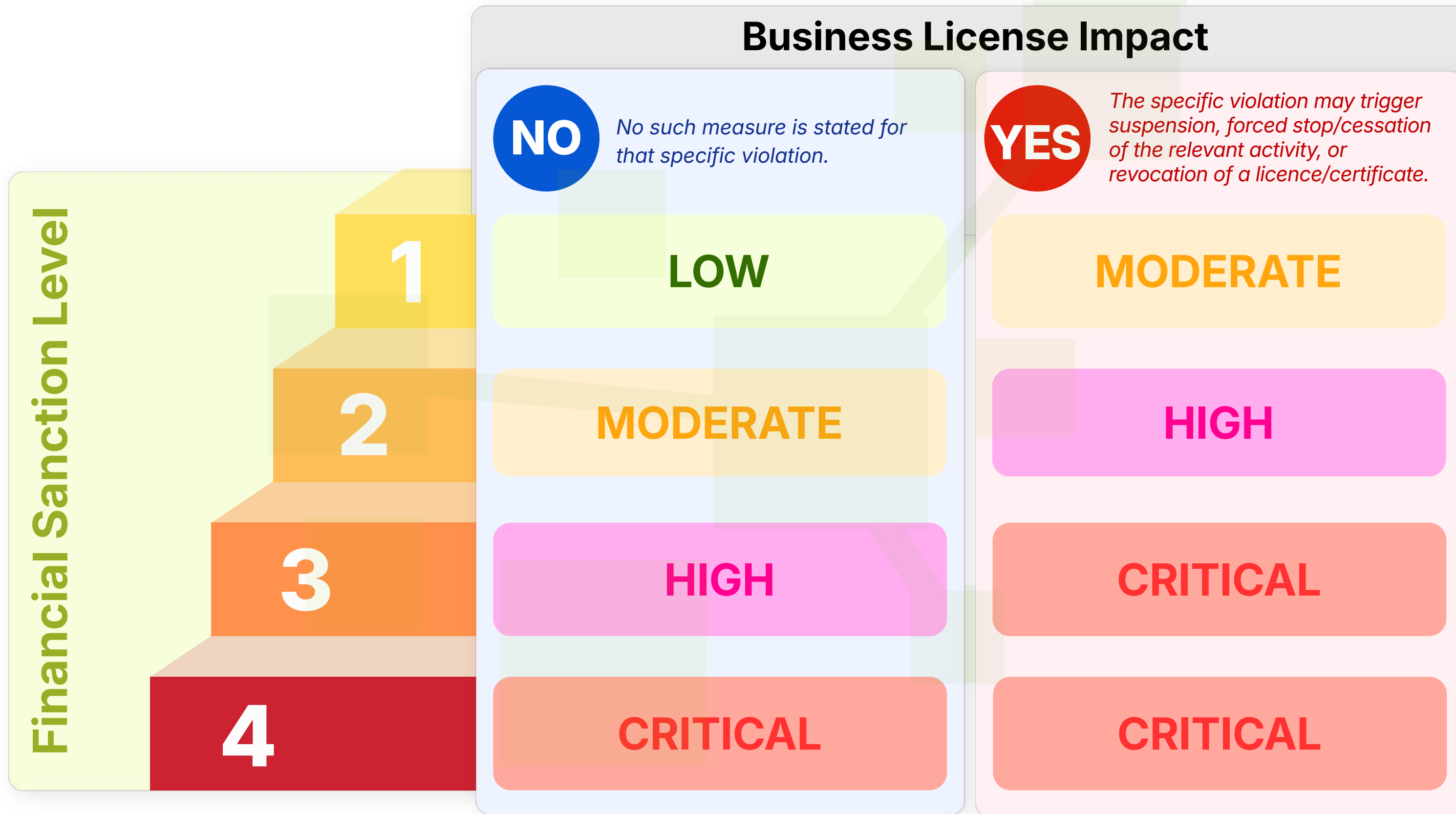
Art. 58 LPLD; Art. 1.2-1.3 D330; Art. 7.1-7.2 D118



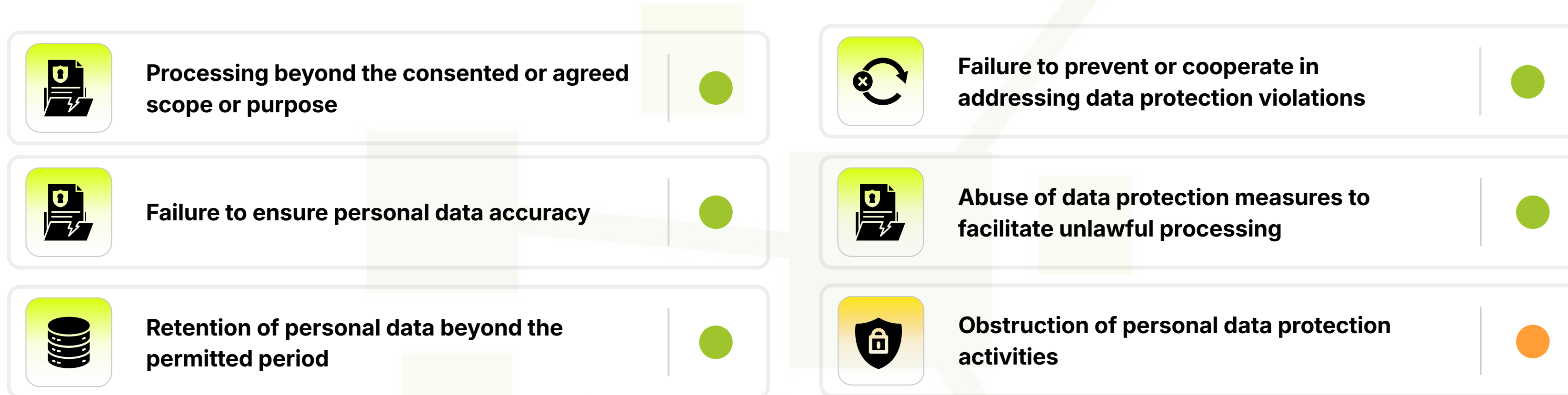
FINANCIAL SANCTION LEVEL



RISK MATRIX



A. DATA PROTECTION PRINCIPLES & PROHIBITED ACTS



● Low ● Moderate ● High ● Critical

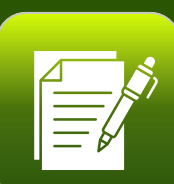


A. DATA PROTECTION PRINCIPLES & PROHIBITED ACTS



● Low ● Moderate ● High ● Critical



 Processing personal data without valid consent, unless legally permitted	●	 Failure to obtain separate consent for each processing purpose	●
 Conditioning or denying services based on consent to unrelated processing purposes	●	 Failure to record, retain or demonstrate evidence of consent	●
 Use of pre-ticked, default or misleading consent mechanisms	●	 Failure to notify data subjects of sensitive personal data processing	●
 Unclear or unverifiable consent regarding the data subject, timing or consent scope	●	 Continued processing despite a withdrawal, restriction or stop request/order	●
 Consent obtained without sufficient transparency or informed basis	●	 Treating silence or non-response as consent	●

● Low ● Moderate ● High ● Critical



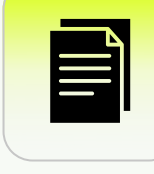
C. DATA SUBJECT RIGHTS (DSRS)

	Failure to establish clear DSR processes, procedures and forms	●
	Unclear internal roles and responsibilities for DSR handling	●
	Failure to inform data subjects of procedures for exercising their rights	●
	Failure to provide a timely or complete initial response to a valid DSR	●
	Failure to provide reasons for DSR refusal or extension	●
	Failure to stop or restrict processing following withdrawal, restriction or objection	●
	Failure to rectify or provide personal data within the applicable timeframe	●
	Failure to erase personal data or restrict processing within the applicable timeframe	●

● Low ● Moderate ● High ● Critical



C. DATA SUBJECT RIGHTS (DSRS)

	Failure to meet deadlines for withdrawal, restriction or objection requests	●
	Failure to meet deadlines for access, rectification or data provision requests	●
	Failure to meet deadlines for erasure requests	●
	Failure to meet deadlines for requested data protection measures	●
	Obstruction of consent withdrawal or processing restriction rights	●
	Failure to stop processing after a valid withdrawal or restriction request	●
	Failure to cascade stop-processing request to processors or third parties	●
	Unauthorized rectification by a processor or third party	●
	Intentional delay or failure to correct known false or fabricated personal data	●

● Low ● Moderate ● High ● Critical



D. PERSONAL DATA COLLECTION



Collection of personal data beyond the defined scope or purpose, or without the data subject's prior consent as required by law



Collection, storage or creation of personal data repositories from transferred data for purposes beyond those consented to by the data subject



Unlawful use of technological or technical measures to collect basic personal data of fewer than 500 data subjects or sensitive personal data of fewer than 100 data subjects



Unlawful use of technological or technical measures to collect basic personal data of 1,000 to fewer than 5,000 data subjects or sensitive personal data of 200 to 1,000 data subjects



Unlawful use of technological or technical measures to collect basic personal data of 5,000 or more data subjects or sensitive personal data of 1,000 or more data subjects



Unlawful use of technological or technical measures to collect basic personal data of 500 to fewer than 1,000 data subjects or sensitive personal data of 100 to fewer than 200 data subjects



Unlawful collection involving sensitive personal data



Low Moderate High Critical



E. PERSONAL DATA PROVISION



Refusal to provide personal data to the data subject upon a valid request



Provision of personal data to another agency, organization or individual without the data subject's consent, unless otherwise permitted by law



Provision of sensitive personal data to another agency, organization or individual without the data subject's consent, unless otherwise permitted by law



● Low ● Moderate ● High ● Critical



F. PUBLIC DISCLOURE OF PERSONAL DATA

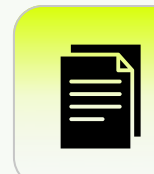
	Public disclosure of personal data without a specific purpose or legal basis for disclosure	Low
	Public disclosure beyond the scope or categories of personal data necessary for the stated purpose	Low
	Public disclosure of personal data that does not accurately reflect the original data source	Low
	Failure to adequately control and monitor public disclosure to ensure compliance with the defined purpose, scope and applicable law	Low

	Failure to implement measures preventing unauthorized access, use, disclosure, copying, modification, deletion, destruction or other unlawful processing of publicly disclosed personal data	Low
	Public disclosure of personal data that infringes the data subject's lawful rights or interests	Low
	Public disclosure of personal data without the data subject's consent, unless otherwise permitted by law	Low

Low Moderate High Critical



G. PERSONAL DATA DELETION, DESTRUCTION AND ANONYMIZATION

 Failure to inform the data subject of the reasons why a deletion or destruction request cannot be fulfilled	●	 Failure to prevent unauthorized access, copying, appropriation, disclosure or loss of personal data during de-identification	●
 Failure to erase or destroy personal data using secure measures	●	 Failure to erase or destroy personal data where required by law	●
 Failure to prevent unauthorized access to or recovery of erased or destroyed personal data	●	 Failure by the controller to instruct processors or third parties to erase or destroy personal data as required by law	●
 Failure to adequately control or monitor the de-identification of personal data	●	 Failure by the processor to erase or return all personal data to the controller upon termination of the processing contract or arrangement	●

● Low ● Moderate ● High ● Critical



G. PERSONAL DATA DELETION, DESTRUCTION AND ANONYMIZATION



Occurrence of unauthorized access, copying, appropriation, disclosure or loss of personal data during de-identification



Intentional unauthorized recovery of erased or destroyed personal data



Re-identification of personal data after de-identification, unless otherwise permitted by law



● Low ● Moderate ● High ● Critical



H. DATA TRANSFERRING ACTIVITIES



Data transfer agreement failing to define responsibilities for data protection, data subject rights, and cooperation and compliance in the event of a data protection violation



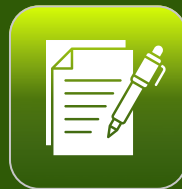
Failure to define an appropriate retention period for transferred personal data, or to erase or destroy such data once the transfer purpose has been fulfilled



Failure to clearly define the roles of controller, processor and third party in personal data transfers



Failure to define and limit the categories of transferred personal data to what is necessary for the transfer purpose



Failure to establish controls for internal data sharing and use, or to prevent personnel from unlawfully sharing personal data with third parties



Transfer of sensitive personal data without appropriate physical security, encryption, anonymization or other security safeguards during transfer



● Low ● Moderate ● High ● Critical



I. ILLEGAL TRADING OF PERSONAL DATA



Provision, sharing or exchange of personal data for financial or other benefits outside permitted cases under Article 17.1 of PDPL



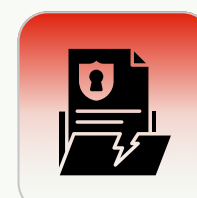
Paid or benefit-based personal data transfer without a transfer agreement



Paid or benefit-based data transfer without a defined purpose or inconsistent with the agreed purpose



Paid or benefit-based data transfer without specific, informed consent for each transfer



Paid or benefit-based data transfer outside the consented transfer purpose or registered business scope



Paid or benefit-based data transfer without anonymizing the personal data when conducting transactions on a data exchange



● Low ● Moderate ● High ● Critical

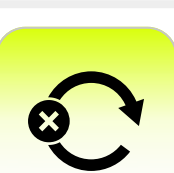
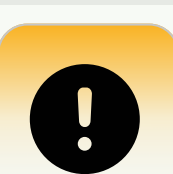
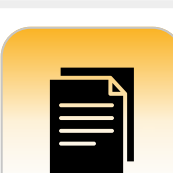


	Failure by the processor to promptly notify the controller or controller-processor of a detected violation	Low
	Failure to formally document a personal data protection violation	Low
	Concealment or misrepresentation of breach details in regulatory reporting	Low
	Detected personal data protection violation	Low
	Processing inconsistent with stated purpose or agreement	Low
	Failure to ensure or properly implement data subject rights	Low
	Failure to notify the data protection authority within 72 hours of a harmful or potentially harmful violation	Moderate
	Failure to contain the violation or remediate its consequences	Moderate
	Failure to cooperate with the competent data protection authority in handling the violation	Moderate

Low Moderate High Critical



K. DATA IMPACT ASSESSMENTS &
CROSS-BORDER TRANSFER

	Failure to submit the DPIA dossier within 60 days of commencing processing	Moderate
	Intentional failure to complete the DPIA dossier as required by the authority	Low
	Failure to perform the required six-month DPIA update	Low
	Failure to perform six-month DPIA update	Low
	Failure to update the DPIA dossier within the required 10-day period	Low
	Falsification, misrepresentation or failure to correct information in the DPIA dossier	Moderate
	Failure to prepare OTIA dossier	Moderate
	Failure to submit the OTIA dossier within 60 days of commencing the transfer	Moderate

● Low ● Moderate ● High ● Critical



K. DATA IMPACT ASSESSMENTS & CROSS-BORDER TRANSFER

	Failure to complete the OTIA dossier within 30 days of an authority request	●
	Failure to periodically update the OTIA dossier or update it upon required changes	●
	Failure to keep the OTIA dossier available for regulatory inspection	●
	Failure to notify the recipient's data protection contact details after the transfer	●
	Failure to control onward transfers by the overseas recipient	●
	Failure to establish a binding cross-border data transfer agreement	●
	Cross-border transfer without valid consent or required notice	●
	Insufficient security safeguards during or after cross-border transfer	●

● Low ● Moderate ● High ● Critical

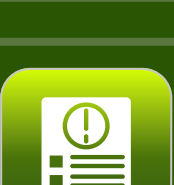


K. DATA IMPACT ASSESSMENTS & CROSS-BORDER TRANSFER

	Obstruction of or failure to cooperate with cross-border transfer inspections	●		Cross-border breach affecting 10,000–99,999 Vietnamese data subjects	●
	Continuation of cross-border transfers despite an authority stop order	●		Cross-border breach affecting 100,000–999,999 Vietnamese data subjects	●
	Failure to report and contain a violation or data breach involving the overseas recipient	●		Mass cross-border data breach or transfer in breach of a stop order causing national security harm	●

● Low ● Moderate ● High ● Critical



	Failure to enter into a confidentiality agreement with DPO	Low
	Failure to provide required training for DPO	Low
	DPO appointment or data protection unit establishment document lacks required functions, duties and authority	Low
	Appointment of data protection personnel who fail to meet qualification or experience requirements	Low
	Appointment of data protection personnel without required legal and professional training	Low
	Failure to formally appoint data protection personnel or establish a data protection unit	Low

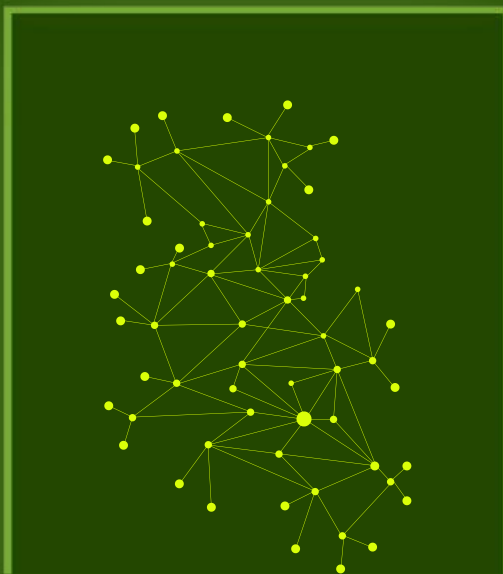
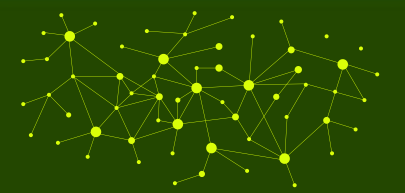


M. PERSONAL DATA PROTECTION SERVICES

	Provision of personal data protection services without required qualifications	
	Provision of services beyond the agreed contractual scope	
	Failure to delete or destroy personal data upon contract completion	
	Failure to prepare a compliant service capability profile	
	Failure to maintain the required minimum number of qualified personnel	
	Provision of services without a service contract and data processing agreement	
	Failure to disclose service provider information to data subjects and relevant parties	
	Misuse of service access for unauthorized personal data processing	

 Low  Moderate  High  Critical





Get in Touch With Us For Tailored Solutions!

At **Data Protectify**, we prioritize your privacy and data protection compliance needs. Our comprehensive data and privacy solutions are designed to help businesses navigate the complexities of data and tech regulations. We offer tailored solutions that assess your current practices, implement necessary policies, data protection controls and conduct ongoing monitoring to ensure adherence to privacy requirements.

Our dedicated DPO team provides you with practical solutions and insights that empower you to sustain robust data & technology standards, enhance risk culture, and build digital trust across the market.



www.dataprotectify.vn



+84-39662-6694



contact.us@dataprotectify.vn