Vendor Liability and Data Processing Agreements under Vietnam's Personal Data Protection Framework

RUSSIN & VECCHI – 2026

Le Ton Viet
Senior Associate
Hanoi Office

LTViet@russinvecchi.com.vn

SUMMARY

01	Data Controller is ultimately liable for any breach occurring during data processing activities.
02	The Data Processing Agreement (DPA) is a tool for vendor management and sets out the vendor's obligations and responsibilities.
03	DPA should cover scope of processing, specified purposes, security obligations, breach notifications and indemnification.
04	There are operational risks that should be considered when drafting a DPA.
05	Audit and self-assessment should be utilized to confirm that vendor adopts the appropriate measures to protect personal data.

LTVIET@russinvecchi.com.vn

Summary of current regulations

The Precursor:
Decree 13/2023/ND-CP
(Status: Repealed Jan 1, 2026)

The Current Framework:
Law No. 91/2025/QH15 and
Decree 356/2025/ND-CP
(Status: In effect Jan 1, 2026)

- The new Law on Personal Data Protection and Decree 356 have been in effect for 6+ months.

- The new regulations and the previous Decree 13 share a number of similarities but the new rules significantly raise the compliance bar.

ROLE OF THE ENTITY / VENDOR

Data Controller

Determines the purposes for which and the manner in which personal data is processed

Data Processor

Processes personal data for and on behalf of the Data controller and in accordance with an agreement

Third Party

Any party -- that is not the Data processor or the Data subject--who engages in some processing activities

VENDOR

Vendors usually assume the role of a Data Processor and in certain cases, they can also act as a Data Controller.

LIABILITY OF DATA CONTROLLER

Data Flow

Liability Flow

- The Data Controller is directly accountable to the MPS and to the Data Subjects, regardless of where the technical breach occurs.

- Under Law 91 and Decree 356, the Controller must prove that the Data Subject has given valid consent for a vendor's specific processing activities.

DATA PROCESSING AGREEMENTS (DPA)

- There are no specific requirements on the contents of a DPA.
- A DPA or any other arrangement between a Controller and a Processor needs to cover:
  - **Scope and Duration**: Clearly defined data categories and processing timelines.
  - **Specified Purpose**: Strict alignment with consent obtained from the data subject.
  - **Security Obligations**: Commitment to technical and organizational measures.
  - **Breach Protocol**: Cooperation between data controller and processor for notifications.
  - **Termination**: A defined procedure for data return or destruction.

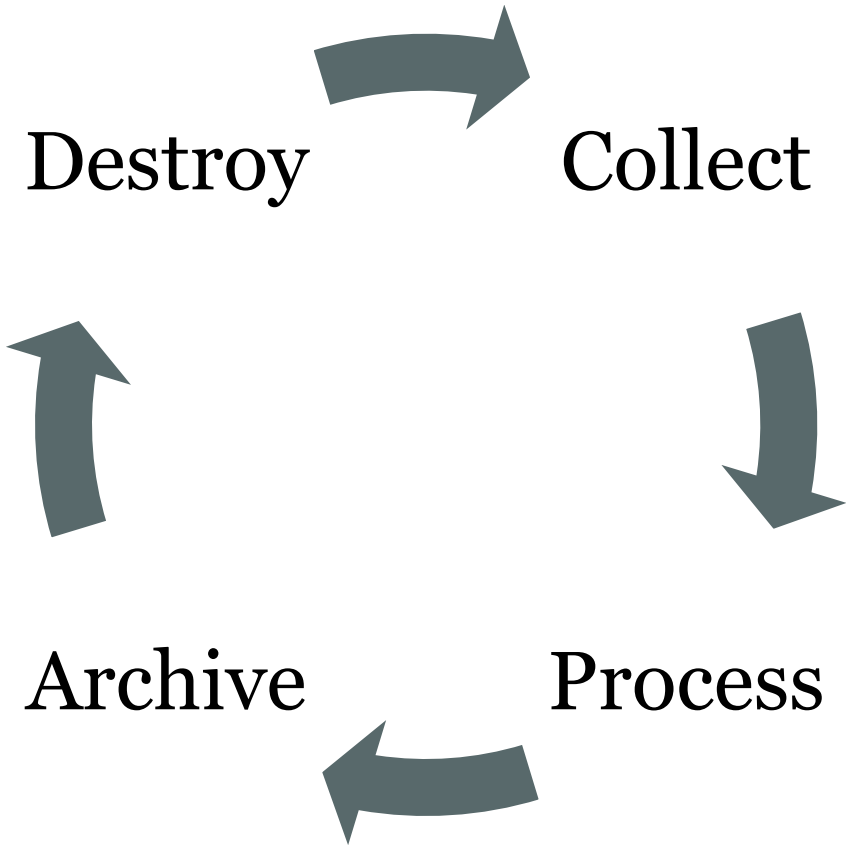
Purpose Limitation

- Clearly defined scope of data processing activities.
- Avoid allowing vendors to include generic purposes in the DPA such as market research, service improvements, etc. If these purposes are allowed, the DPA must require the vendor to anonymize the relevant personal data. Anonymization must be conducted in accordance with Law 91.
- Processing conducted outside of the defined scope must be agreed in writing and is subject to consent of the data subjects.

Security Standards

- **Encryption:** Data at rest and data in transit must be encrypted.
- **Access control**: Multi-Factor Authentication and “Least Privilege” access.
- **Logging: S**ystem access logs must be retained for a minimum of 12 months.

DATA RETENTION AND DISPOSAL



- **Right to be forgotten:** Data subjects may request that their data be deleted or may withdraw their consent.
- **Upon Termination**: Data must be returned or destroyed. The parties can agree whether a Certificate of Destruction is required.
- **Retention Conflict:** Can a vendor claim that it must keep data for tax or regulatory purposes?

Operational Risks

1

Cross-border transfer

When a vendor makes a cross-border transfer under the Law on Personal Data Protection, requirements in relation to cross-border transfer of personal data will be triggered

2

Breach Notifications

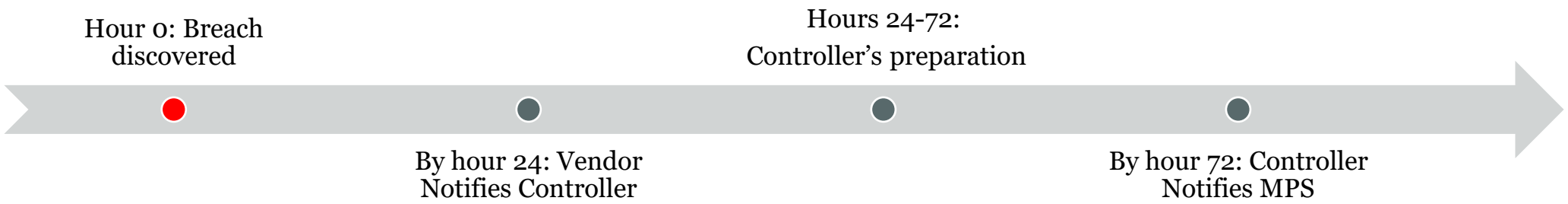
Statutory deadline to file a breach notice with the authority is 72 hours after a breach is discovered.

3

Exercising Data Subjects' Requests

Vendor must have the technical capacity to delete, restrict, or provide data within the statutory windows.

Breach Notification Requirements



- Within 72 hours of discovering a data breach, the Data Controller must notify the Ministry of Public Security (A05). If certain types of personal data are involved, data subjects must also be notified within the same timeframe.

- The following information must be included in the notification:
  - Description of the incident;
  - Potential damages and consequences;
  - Information of the data protection personnel;
  - The measures being taken to mitigate or to rectify the situation.

- Notification provided to the data subjects essentially contains the same information but is presented differently.

Handling of Data Subjects' Requests

Type of Request	Response	Execution
To withdraw consent	2 business days	15 days, or 20 days if there are data processors
To view, edit or adjust personal data	2 business days	10 days, or 15 days if there are data processors
To delete personal data	2 business days	20 days, or 30 days if there are data processors
To perform protective measures	2 business days	15 days

Audit Rights

- Because the Data Controller is ultimately liable for all data processing activities, the Data Controller is also responsible for the Data Processor's compliance.

- Two-tiered audit:
  - Questionnaire: Self-assessment questionnaire answered by Data Processors and in certain cases, SOC2/ISO 27001 certificate should be required;
  - On-site Inspection: Reserved for high-risk vendors or after a breach.

- Data Controller can contractually require Processor to bear the cost of audit if any material non-compliance is discovered.

Audit Questions - Sample

- Is there a particular policy/process in place? (for example, a privacy policy or a vulnerability management policy).

- Has the organization undergone a SOC 2 audit within the past 12 months to assess the effectiveness of its security controls and processes?

- Has a Vulnerability Assessment and Penetration Testing report been created?

- Does the organization segregate its network according to groups of information services, users, and information systems?

- What is the method used to destroy data stored on tapes, hard disks and other electronic media so that it is completely unreadable, unusable and inaccessible for unauthorized purposes?

- Is there a hardening checklist and/or report for firewall, router etc.?

Penalties and Compensations

- Penalties and compensation for violation of Data Processing Agreement still follow the rules for penalties and compensation in a normal commercial/civil contract.

- Liquidated damages or pre-calculated damages may be accepted by the courts but there are still issues.