30-POINT CHECKLIST

IN-DEPTH ASSESSMENT OF PERSONAL DATA COMPLIANCE

Since Decree No. 13/2023/ND-CP officially took effect in Vietnam, the protection of personal data has become one of the most critical legal requirements for businesses, particularly for entities with large-scale data processing operations, foreign-invested enterprises (FDIs), and multi-sectoral corporate groups.

The following 30-point checklist is designed to assist businesses in self-assessing their compliance level, identifying strengths and gaps, and laying the foundation for further implementation steps such as:

- Data Processing Impact Assessment (DPIA)
- Standardizing internal policies and contracts
- Preventing legal violations and regulatory inspections
- Ensuring compliance not only with Decree 13 but also with international standards such as GDPR, APPI, and industry best practices

Instruction:

- Mark ✅ if your organization fully meets the criterion.
- Mark ❌ if the requirement is not yet met, unclear, or not fully implemented.

If your organization has 5 or more ❌ marks, we recommend conducting an in-depth Data Privacy Audit with legal and technical professionals to mitigate risks.

NO.	EVALUATION CRITERIA	IMPLEMENTED
I. Governance Structure & Internal Responsibilities		
1	Has a designated Data Protection Officer (DPO) or equivalent individual/unit been appointed?	
2	Has an internal personal data protection policy been issued and communicated?	

NO.	EVALUATION CRITERIA	IMPLEMENTED
3	Are the roles and responsibilities of relevant departments documented in writing?	
4	Is there a mechanism for periodic reporting and compliance checks from the DPO to senior management?	
II. Data Inventory – Legal Basis for Processing		
5	Are all types of processed data (including sensitive data) classified and inventoried?	
6	Do consent forms clearly specify data types and purposes?	
7	Is there a mechanism for users to easily withdraw consent, with history recorded?	
8	Is data retention tracked and limited by data category?	
9	Are access rights clearly defined based on roles (role-based access control)?	
10	Is access/edit/delete activity logged (audit trail)?	
11	Is data encrypted in transit and at rest?	
12	Is there an automated data deletion /lifecycle policy in place?	
13	Are backup controls in place to prevent creation of hidden copies (shadow data)?	

NO.	EVALUATION CRITERIA	IMPLEMENTED
14	Is there an access management process for staff termination or role changes?	
	III. Third Parties & Data Transfers	
15	Is there an updated list of third parties involved in data processing?	
16	Do contracts with third parties include data protection clauses (DPA)?	
17	Is a risk assessment conducted prior to sharing/transferring data to partners?	
18	For cross-border data transfers: has a DPIA been conducted or prepared?	
	IV. Data Subject Rights & Legal Risks	
19	Is there a mechanism to receive and process individual requests (access, correction, deletion, etc.)?	
20	Are response templates, logs, and timelines established in accordance with legal requirements?	
21	Is there a complaint handling policy regarding personal data?	
22	Is there a data breach response process with clear reporting timelines (e.g., within 72 hours)?	
23	Has the organization conducted a simulated data breach drill?	
	V. Policies, Contracts & Legal Review	
24	Do employment and outsourcing contracts include personal data protection clauses?	

NO.	EVALUATION CRITERIA	IMPLEMENTED
25	Have employees signed confidentiality agreements on personal data?	
26	Is there a data deletion/destruction policy upon contract termination with vendors?	
27	Have contracts involving personal data been legally reviewed?	
28	Is there a tool or process to update policies in response to legal changes (Vietnam /GDPR)?	
	VI. Third Parties & Data Transfers	
29	Is there an updated list of third parties involved in data processing?	
30	Do contracts with third parties include data protection clauses (DPA)?	

Overall Assessment

SCORE	COMPLIANCE LEVEL
26 – 30	Strong compliance system – ready for DPIA or periodic reporting
18 – 25	Solid foundation – consider conducting a detailed review and upgrading policies/contracts
Dưới 18	Potential risks – urgent assessment and remedial action needed

BOOK A COMPREHENSIVE CONSULTATION TODAY

- Receive a 1-on-1 personal data system assessment with an expert
- Get a consolidated risk report and remediation roadmap
- Support for building a compliance system under Decree 13 & GDPR

OUR ECOSYSTEM

invest

OFFICE LEASING

CFT

LEGAL COMPLIANCE IN BUSINESS

Head Office: R7.01, Transimex Building, 172 Hai Ba Trung Str., Tan Dinh Ward, HCMC, Vietnam.

Branch Office: 330 Nguyen Van Troi Str., Thu Dau Mot Ward, HCMC, Vietnam.

Transaction Office: 101/20 Street 11, Thu Duc Ward, HCMC, Vietnam

---

/cdlaflawfirm