CHECK LIST 30 ĐIỂM

ĐÁNH GIÁ CHUYÊN SÂU
TUÂN THỦ DỮ LIỆU CÁ NHÂN

Kể từ khi Nghị định 13/2023/NĐ-CP chính thức có hiệu lực tại Việt Nam, vấn đề bảo vệ dữ liệu cá nhân đã trở thành một trong những yêu cầu pháp lý quan trọng nhất đối với các doanh nghiệp, đặc biệt là các tổ chức có quy mô xử lý dữ liệu lớn, doanh nghiệp có yếu tố nước ngoài (FDI) và các tập đoàn đa ngành.

Checklist 30 điểm dưới đây được thiết kế nhằm giúp doanh nghiệp tự rà soát mức độ tuân thủ, xác định các điểm mạnh, điểm thiếu hụt, và chuẩn bị nền tảng cho các bước triển khai tiếp theo như:

- Đánh giá tác động xử lý dữ liệu (DPIA)
- Chuẩn hóa hợp đồng và chính sách nội bộ
- Phòng ngừa rủi ro vi phạm và thanh tra
- Tuân thủ không chỉ theo Nghị định 13 mà còn tham chiếu các tiêu chuẩn quốc tế như GDPR, APPI và các thông lệ ngành

Cách sử dụng:

- Đánh dấu ✅ nếu tổ chức của bạn đã hoàn toàn đáp ứng tiêu chí
- Đánh dấu ❌ nếu chưa có, chưa rõ, hoặc chưa triển khai đầy đủ

Nếu doanh nghiệp của bạn có từ 5 dấu ❌ trở lên, chúng tôi khuyến nghị nên thực hiện một cuộc đánh giá chuyên sâu (Data Privacy Audit) với chuyên gia pháp lý và kỹ thuật để hạn chế rủi ro

STT	TIÊU CHÍ ĐÁNH GIÁ	ĐÃ THỰC HIỆN
	I. Cấu trúc quản trị & trách nhiệm nội bộ	
1	Đã chỉ định rõ người/bộ phận phụ trách bảo vệ dữ liệu cá nhân (DPO hoặc tương đương)?	
2	Có chính sách nội bộ về bảo vệ dữ liệu cá nhân đã ban hành & phổ biến?	

STT	TIÊU CHÍ ĐÁNH GIÁ	ĐÃ THỰC HIỆN
3	Vai trò, trách nhiệm của các bộ phận liên quan đã được ghi nhận bằng văn bản?	
4	Có cơ chế báo cáo định kỳ & kiểm tra tuân thủ từ DPO lên cấp quản lý?	
	II. Danh mục dữ liệu – Căn cứ xử lý	
5	Có phân loại & thống kê đầy đủ các loại dữ liệu đang xử lý (bao gồm nhạy cảm)?	
6	Biểu mẫu xin đồng ý có nội dung rõ ràng, phân biệt loại dữ liệu và mục đích?	
7	Có cơ chế cho phép rút lại sự đồng ý dễ dàng & ghi nhận lịch sử?	
8	Có theo dõi và giới hạn thời hạn lưu trữ cho từng nhóm dữ liệu?	
9	Có phân quyền truy cập rõ ràng theo vai trò (role-based access)?	
10	Có hệ thống ghi nhận (log) việc truy cập – chỉnh sửa – xoá dữ liệu?	
11	Dữ liệu được mã hoá khi truyền và khi lưu trữ không?	
12	Có chính sách xóa dữ liệu tự động sau khi hết mục đích/thiết lập lifecycle?	
13	Có kiểm soát sao lưu dữ liệu, tránh tạo bản sao ẩn (shadow data)?	

STT	TIÊU CHÍ ĐÁNH GIÁ	ĐÃ THỰC HIỆN
14	Có quy trình quản lý truy cập khi nhân sự nghỉ việc hoặc chuyển vị trí?	
	III. Đối tác & bên thứ ba – Chuyển dữ liệu	
15	Có danh sách cập nhật các bên thứ ba có xử lý dữ liệu?	
16	Các hợp đồng với bên thứ ba có điều khoản ràng buộc bảo vệ dữ liệu (DPA)?	
17	Có đánh giá rủi ro trước khi chia sẻ hoặc chuyển dữ liệu cho đối tác?	
18	Nếu chuyển dữ liệu ra nước ngoài: đã thực hiện hoặc chuẩn bị hồ sơ đánh giá tác động (DPIA)?	
	IV. Quyền của chủ thể dữ liệu & Rủi ro pháp lý	
19	Có cơ chế tiếp nhận & xử lý yêu cầu từ cá nhân (truy cập, chỉnh sửa, xoá...)?	
20	Có biểu mẫu phản hồi, log và thời gian phản hồi theo quy định?	
21	Có chính sách xử lý khiếu nại liên quan đến dữ liệu cá nhân?	
22	Có quy trình xử lý vi phạm dữ liệu, nêu rõ thời hạn báo cáo (72 giờ)?	
23	Đã từng thực hiện mô phỏng xử lý sự cố rò rỉ dữ liệu (data breach drill)?	
	V. Chính sách, hợp đồng & kiểm tra pháp lý	
24	Hợp đồng lao động, hợp đồng thuê ngoài có điều khoản dữ liệu cá nhân chưa?	

STT	TIÊU CHÍ ĐÁNH GIÁ	ĐÃ THỰC HIỆN
25	Nhân viên có ký cam kết bảo mật dữ liệu cá nhân?	
26	Có chính sách xóa/hủy dữ liệu khi chấm dứt hợp đồng với nhà cung cấp?	
27	Đã từng kiểm tra hoặc rà soát pháp lý hợp đồng chứa dữ liệu cá nhân?	
28	Có công cụ hoặc quy trình cập nhật khi có thay đổi pháp luật (VN/GDPR)?	
	VI. Đối tác & bên thứ ba – Chuyển dữ liệu	
29	Có danh sách cập nhật các bên thứ ba có xử lý dữ liệu?	
30	Các hợp đồng với bên thứ ba có điều khoản ràng buộc bảo vệ dữ liệu (DPA)?	

Đánh giá tổng hợp

SỐ ĐIỂM	ĐÁNH GIÁ
26 – 30	Doanh nghiệp có hệ thống tuân thủ mạnh – sẵn sàng mở rộng DPIA hoặc báo cáo định kỳ
18 – 25	Nền tảng tốt – nên rà soát chuyên sâu và nâng cấp hợp đồng, quy trình
Dưới 18	Có rủi ro tiềm ẩn – cần thực hiện đánh giá & hành động khẩn cấp

ĐĂNG KÝ TƯ VẤN CHUYÊN SÂU NGAY HÔM NAY

- Nhận đánh giá hệ thống dữ liệu cá nhân 1-1 cùng chuyên gia
- Nhận báo cáo tổng hợp rủi ro & đề xuất khắc phục
- Hỗ trợ xây dựng hệ thống tuân thủ theo Nghị định 13 & GDPR

HỆ SINH THÁI CỦA CDLAF

invest

VĂN PHÒNG CHO THUÊ

CFT

TUÂN THỦ PHÁP LÝ TRONG DOANH NGHIỆP

Trụ sở: Phòng 7.01, Toà nhà Transimex, 172 Hai Bà Trưng, Phường Tân Định, Thành phố Hồ Chí Minh.

Chi nhánh: 330 Nguyễn Văn Trỗi, Phường Thủ Dầu Một, Thành phố Hồ Chí Minh.

Văn phòng Giao dịch: 101/20 đường 11, Phường Thủ Đức, Thành phố Hồ Chí Minh.

/cdlaflawfirm