PHÁP LUẬT VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

Tiến sĩ Lê Nết - LNT & Partners

1

NỘI DUNG

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025
II. Rủi ro pháp lý cho doanh nghiệp khi giao dịch kinh doanh qua mạng xã hội
III. Doanh nghiệp nên làm gì khi giao dịch kinh doanh qua mạng xã hội
IV. Case study

2

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

I.1. Cấm tuyệt đối hành vi mua bán dữ liệu cá nhân

Điều 7 Luật Bảo vệ dữ liệu cá nhân 2025:
"[...]
5. Sử dụng dữ liệu cá nhân của người khác, cho người khác sử dụng dữ liệu cá nhân của mình để thực hiện hành vi trái quy định của pháp luật.
6. Mua, bán dữ liệu cá nhân, trừ trường hợp luật có quy định khác.
7. Chiếm đoạt, cố ý làm lộ, làm mất dữ liệu cá nhân."

Điều 7 Luật Bảo vệ dữ liệu cá nhân 2025 quy định về việc **cấm mua, bán dữ liệu cá nhân,** trừ trường hợp luật có quy định khác. Điều này là cần thiết để ngăn chặn tình trạng rao bán thông tin cá nhân tràn lan trên mạng, hoặc việc nhân viên tổ chức lợi dụng dữ liệu để lừa đảo, chiếm đoạt tài sản hoặc thực hiện các hành vi khác trái quy định pháp luật.

3

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

I.2. Xử lý vi phạm (Điều 8 Luật Bảo vệ dữ liệu cá nhân 2025)

- Mức phạt tiền tối đa đối với hành vi mua, bán dữ liệu cá nhân là 10 lần khoản thu có được từ hành vi vi phạm hoặc 3 tỷ VNĐ, tùy theo mức nào cao hơn.
- Mức phạt tiền tối đa đối với hành vi vi phạm quy định chuyển dữ liệu cá nhân xuyên biên giới là 5% doanh thu của năm trước liền kề của chủ thể vi phạm hoặc 3 tỷ VNĐ, tùy theo mức nào cao hơn.
- Mức phạt tiền tối đa đối với các hành vi vi phạm khác, mức phạt tiền tối đa là 3 tỷ VNĐ.
- Các mức phạt trên được áp dụng đối với tổ chức. Mức phạt tiền tối đa đối với hành vi do cá nhân thực hiện bằng một phần hai mức phạt tiền đối với tổ chức.

4

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

I.3. Mạng xã hội không được yêu cầu cung cấp hình ảnh, video chứa nội dung về giấy tờ tùy thân làm yếu tố xác thực

Điều 29 Luật Bảo vệ dữ liệu cá nhân 2025 quy định về trách nhiệm của tổ chức, cá nhân cung cấp dịch vụ mạng xã hội, dịch vụ truyền thông trực tuyến:

1. Thông báo rõ ràng nội dung dữ liệu cá nhân thu thập; không thu thập trái phép và ngoài phạm vi đã thỏa thuận;
2. Không được yêu cầu cung cấp hình ảnh, video chứa nội dung đầy đủ hoặc một phần giấy tờ tùy thân làm yếu tố xác thực tài khoản;
3. Cung cấp lựa chọn cho phép người dùng từ chối thu thập và chia sẻ tệp dữ liệu (gọi là cookies);
4. Cung cấp lựa chọn "không theo dõi" hoặc chỉ được theo dõi hoạt động sử dụng mạng xã hội khi có sự đồng ý của người dùng;
5. Không nghe lén, nghe trộm hoặc ghi âm cuộc gọi và đọc tin nhắn văn bản khi không có sự đồng ý của chủ thể dữ liệu cá nhân, trừ trường hợp pháp luật có quy định khác;
6. Công khai chính sách bảo mật, giải thích rõ cách thức thu thập, sử dụng và chia sẻ dữ liệu cá nhân; , cho phép người dùng quản lý dữ liệu, bảo vệ dữ liệu khi chuyển ra nước ngoài và xử lý vi phạm nhanh chóng.

5

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

I.3. Mạng xã hội không được yêu cầu cung cấp hình ảnh, video chứa nội dung về giấy tờ tùy thân làm yếu tố xác thực

- Từ 01/1/2026, nền tảng mạng xã hội không được sử dụng CCCD/hộ chiếu hoặc các loại giấy tờ tùy thân khác dưới dạng ảnh/video làm yếu tố xác thực tài khoản người dùng.
- Nền tảng mạng xã hội không được nghe lén, nghe trộm, ghi âm cuộc gọi, đọc tin nhắn văn bản khi không có sự đồng ý của người dùng.

6

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

I.4. Dữ liệu cá nhân có phải tài sản không?

Theo Khoản 1 Điều 2 Nghị định 13/2023/NĐ-CP: **Dữ liệu cá nhân** là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể.

Theo Điều 105 Bộ luật Dân sự 2015, **tài sản** được định nghĩa là vật, tiền, giấy tờ có giá và quyền tài sản, bao gồm cả bất động sản và động sản hiện có hoặc hình thành trong tương lai.

Hiện **không có quy định pháp luật nào** khẳng định dữ liệu cá nhân có phải là tài sản hay không.

7

I. Một số điểm đáng chú ý của Luật bảo vệ dữ liệu cá nhân 2025

Dữ liệu cá nhân có phải tài sản không?

ỦNG HỘ	PHẢN ĐỐI
1. Dữ liệu cá nhân mang lại lợi nhuận lớn thông qua quảng cáo, phân tích thị trường, phát triển sản phẩm.	1. Dữ liệu cá nhân gắn với quyền riêng tư, có thể dẫn đến vi phạm quyền cá nhân.
2. Có thể định giá và chuyển nhượng giữa các doanh nghiệp, tương tự tài sản thương mại.	2. Giá trị dữ liệu thay đổi theo ngữ cảnh và mục đích sử dụng, gây khó khăn trong việc định giá chuẩn.
3. Một số quốc gia/học giả đề xuất xây dựng quyền sở hữu dữ liệu cá nhân để thương mại hóa minh bạch.	3. Cá nhân vẫn giữ quyền kiểm soát dù đã chia sẻ dữ liệu – khác với tài sản thông thường.
4. Giống như quyền sở hữu trí tuệ, dữ liệu cá nhân có thể được pháp luật bảo vệ như tài sản vô hình.	4. Việc coi dữ liệu là tài sản có thể thúc đẩy hành vi thu thập, mua bán trái phép dữ liệu.
	5. GDPR nhấn mạnh quyền kiểm soát và bảo vệ chứ không phải quyền sở hữu dữ liệu.

8

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

I.4. Dữ liệu cá nhân có phải tài sản không?

433/435 đại biểu Quốc hội đã biểu quyết tán thành thông qua Luật Bảo vệ dữ liệu cá nhân, trong đó cấm các hành vi mua bán dữ liệu cá nhân => gián tiếp thừa nhận dữ liệu cá nhân không phải tài sản.

Tham khảo kinh nghiệm quốc tế cho thấy, dữ liệu cá nhân không được công nhận là tài sản, một số quốc gia (như Mỹ, Thái Lan, Singapore, Malaysia…) chỉ công nhận về quyền kiểm soát của chủ thể đối với việc sử dụng dữ liệu cá nhân của mình như thế nào.

Tuy nhiên, dữ liệu cá nhân có giá trị kinh tế và có thể coi là nguồn tài nguyên đặc biệt trong nền kinh tế số, nên một số quan điểm đề xuất coi dữ liệu cá nhân là tài sản phi truyền thống hoặc tài nguyên chiến lược để tăng cường bảo vệ và quản lý.

9

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

I.5. Ý nghĩa của việc bỏ từ "đồng thời" trong định nghĩa về Bên kiểm soát và xử lý dữ liệu trong Luật Bảo vệ dữ liệu cá nhân 2025?

- **Điều 2.11 Nghị định 13/2023/NĐ-CP:** "Bên Kiểm soát và xử lý dữ liệu cá nhân là tổ chức, cá nhân đồng thời quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân."
- **Điều 2.9 Luật bảo vệ dữ liệu cá nhân 2025**: "Bên kiểm soát và xử lý dữ liệu cá nhân là cơ quan, tổ chức, cá nhân quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân."

10

I. Một số điểm đáng chú ý của Luật Bảo vệ dữ liệu cá nhân 2025

Việc Luật Bảo vệ dữ liệu cá nhân 2025 bỏ từ "đồng thời" trong định nghĩa về Bên kiểm soát và xử lý dữ liệu cá nhân (so với Nghị định 13/2023/NĐ-CP) nhằm:

- Tách bạch vai trò rõ ràng hơn giữa Bên kiểm soát dữ liệu cá nhân (quyết định mục đích và phương tiện xử lý) và Bên xử lý dữ liệu cá nhân (thực hiện xử lý thay mặt cho Bên kiểm soát dựa trên hợp đồng hoặc ủy quyền riêng biệt).
- Phân công rõ trách nhiệm và vai trò khi có nhiều bên tham gia xử lý dữ liệu; giúp doanh nghiệp linh hoạt thuê ngoài hoặc hợp tác mà vẫn đảm bảo kiểm soát dữ liệu, nâng cao khả năng kiểm tra, giám sát, và chịu trách nhiệm riêng biệt đối với quá trình xử lý dữ liệu.

11

LNT & PARTNERS VIAC TRUNG TÂM TRỌNG TÀI QUỐC TẾ VIỆT NAM

II. Rủi ro pháp lý cho doanh nghiệp khi giao dịch kinh doanh qua mạng xã hội

12

II. Rủi ro pháp lý cho doanh nghiệp khi giao dịch kinh doanh qua mạng xã hội

II.1. Thu thập trái phép dữ liệu cá nhân

II.2. Không kiểm soát được dữ liệu bị rò rỉ

II.3. Bị mạo danh, lừa đảo

13

II. Rủi ro pháp lý cho doanh nghiệp khi giao dịch kinh doanh qua mạng xã hội

II.1. Thu thập trái phép dữ liệu cá nhân

Nhân viên tư vấn qua Zalo, Messenger

- tự ý xin thông tin cá nhân,
- không cung cấp link chính sách bảo mật,
- không có cơ chế đồng ý minh bạch,
- không chứng minh được khách hàng đã "đồng ý rõ ràng và tự nguyện" theo luật.

--> Vi phạm Điều 9, Điều 11 Luật Bảo vệ dữ liệu cá nhân 2025.

14

II. Rủi ro pháp lý cho doanh nghiệp khi giao dịch kinh doanh qua mạng xã hội

II.2. Không kiểm soát được dữ liệu bị rò rỉ:

Dữ liệu khách hàng bị lưu trên điện thoại cá nhân của nhân viên, bị mất máy hoặc chụp lại chia sẻ cho bên thứ ba.
--> Vi phạm Điều 7. Luật Bảo vệ dữ liệu cá nhân 2025: "Cố ý chiếm đoạt, làm lộ, mất dữ liệu cá nhân; Thu thập, xử lý, chuyển giao dữ liệu cá nhân trái quy định của pháp luật".

15

II. Rủi ro pháp lý cho doanh nghiệp khi giao dịch kinh doanh qua mạng xã hội

II.3. Bị mạo danh, lừa đảo:

Các tài khoản mạng xã hội dễ tạo lập, thay đổi, khả năng mượn danh, mạo danh cao, nội dung trao đổi có thể bị xóa hoặc ẩn, và tên chủ tài khoản cũng rất dễ để thay đổi.

16

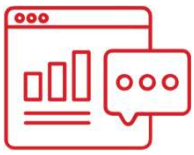
III. Doanh nghiệp nên làm gì khi giao dịch kinh doanh qua mạng xã hội

17

III. Doanh nghiệp nên làm gì khi giao dịch kinh doanh qua mạng xã hội

Có quy định nội bộ về hành vi tiếp cận, xử lý và bảo vệ dữ liệu cho toàn bộ nhân viên, quy định rõ loại thông tin nào được thu thập.

Không nên thu thập dữ liệu cá nhân (CCCD, địa chỉ, email, lịch sử mua hàng...) qua chat nếu không có cơ chế đồng ý minh bạch.



Nên thiết lập link đăng ký có check box đồng ý và dẫn đến chính sách bảo mật, thay vì yêu cầu gửi trực tiếp trong tin nhắn.

Cài chế độ cung cấp chat box tự động về đồng ý thu thập dữ liệu cá nhân khi bắt đầu các cuộc trò chuyện qua mạng xã hội

18

IV. Case Study

19

Case study 1: Vi phạm việc thu thập và sử dụng dữ liệu cá nhân trong kinh doanh, bán thuốc qua nền tảng mạng xã hội

Một nhà thuốc online phục vụ khách hàng qua zalo chính thức của nhà thuốc. Khách hàng tiến hành đặt hàng và mua thuốc qua zaloi. Sau khi đơn hàng thành công, 1 tháng sau, một số số điện thoại cá nhân của một người xưng là "nhân viên nhà thuốc" sử dụng để liên lạc trực tiếp, nhắc nhở khách về việc mua thuốc khi hết thuốc và dặn dò khách hàng lưu số để được hỗ trợ việc mua thuốc sau này.

Câu hỏi: Doanh nghiệp cho phép nhân viên tư vấn và chăm sóc khách hàng qua số điện thoại và zalo cá nhân của nhân viên có thể tiềm ẩn những rủi ro gì?

20

Case study 1: Vi phạm việc thu thập và sử dụng dữ liệu cá nhân trong kinh doanh, bán thuốc qua nền tảng mạng xã hội

Rủi ro vi phạm nghĩa vụ bảo vệ dữ liệu cá nhân:

- Không có sự đồng ý từ khách hàng cho mục đích nhắc nhở hay tư vấn này.
- Không có link chính sách bảo mật hay hướng dẫn về quyền riêng tư liên quan đến dữ liệu cá nhân.
- Dữ liệu cá nhân được lưu giữ trên diện thoại cá nhân của nhân viên mà không có biện pháp bảo vệ phù hợp.

Rủi ro trong quan hệ với khách hàng:

- Khách hàng cảm thấy bị xâm phạm quyền riêng tư, lo ngại thông tin cá nhân bị sử dụng không đúng mục đích.
- Có thể bị khách hàng khởi kiện, khiếu nại về việc làm rò rỉ thông tin cá nhân.

Rủi ro về quản trị nội bộ:

- Không kiểm soát được chất lượng tư vấn của nhân viên;
- Không kiểm soát được tính xác thực thông tin do nhân viên thu thập;

21

Case study 1: Vi phạm việc thu thập và sử dụng dữ liệu cá nhân trong kinh doanh, bán thuốc qua nền tảng mạng xã hội

Khuyến nghị cho doanh nghiệp:

- Trước khi xử lý dữ liệu cá nhân, cần lấy được sự đồng ý của khách hàng về mục đích, phạm vi xử lý dữ liệu.
- Công khai chính sách bảo mật, cách thức xử lý dữ liệu cá nhân; cần có các điều khoản cụ thể liên quan đến việc bảo vệ quyền riêng tư trên các nền tảng mạng xã hội.
- Đào tạo và nâng cao nhận thức cho toàn bộ nhân viên, đặc biệt những người có quyền truy cập, xử lý dữ liệu cá nhân của khách hàng.
- Xây dựng quy trình thuận tiện để người dùng có thể truy cập, chỉnh sửa, hoặc yêu cầu xóa dữ liệu cá nhân khi cần thiết và xử lý kịp thời các trường hợp vi phạm, báo cáo theo yêu cầu pháp luật.

22

Case study 2: Nhân viên Samsung Hàn Quốc làm rò rỉ dữ liệu mật qua ChatGPT

23

Case study 2: Nhân viên Samsung làm rò rỉ dữ liệu mật qua ChatGPT

Ít nhất ba trường hợp nhân viên của Samsung đã nhập các dữ liệu nhạy cảm và dữ liệu mật của công ty vào ChatGPT:
(i) nhân viên kỹ thuật của Samsung sao chép mã nguồn bị lỗi từ cơ sở dữ liệu bán dẫn để nhờ ChatGPT tìm cách khắc phục;
(ii) nhân viên khác vì tò mò đã tải lên mã bí mật của thiết bị lỗi để xem trí tuệ nhân tạo có phát hiện ra;
(iii) nhân viên thuộc khối văn phòng thậm chí đưa toàn bộ nội dung cuộc họp lên nền tảng của OpenAI, nhờ chatbot soạn thành biên bản tóm tắt. Các dữ liệu này sau đó được lưu trữ trên máy chủ của OpenAI và Samsung không thể truy xuất hoặc thu hồi lại.

Hậu quả là các bí mật thương mại và thông tin nội bộ của Samsung bị rò rỉ ra bên ngoài, tiềm ẩn nguy cơ bị đối thủ khai thác, mất lợi thế cạnh tranh. Samsung buộc phải ban hành lệnh cấm nhân viên sử dụng các công cụ AI tạo sinh như ChatGPT trên thiết bị làm việc và cá nhân để tránh rủi ro tiếp tục rò rỉ dữ liệu.

24

Case study 2: Nhân viên Samsung làm rò rỉ dữ liệu mật qua ChatGPT

Tại Việt Nam, vụ việc trên có thể cấu thành vi phạm Điều 7 Luật Bảo vệ dữ liệu cá nhân 2025 (nghiêm cấm làm lộ, mất dữ liệu cá nhân).

Bài học rút ra:

- Có chính sách nghiêm ngặt và đào tạo kỹ càng về việc sử dụng công cụ AI.
- Thiết lập các biện pháp kỹ thuật để ngăn chặn và kiểm soát luồng dữ liệu cá nhân trong nội bộ, không để nhân viên tự ý gửi dữ liệu lên các dịch vụ bên ngoài.
- Phát triển các giải pháp AI nội bộ hoặc hợp tác với các bên cung cấp dịch vụ có cam kết bảo mật cao để bảo vệ thông tin công ty.
- Có quy trình phòng ngừa, cảnh báo khi phát hiện rủi ro rò rỉ, tránh tổn thất lan rộng.

25

Case study 3:

- Nếu nhân viên kinh doanh của công ty đi ra ngoài kết nối với khách hàng, xin thông tin cá nhân của khách hàng và lưu trên hệ thống Customer Relationship Management (CRM), vậy làm sao để lưu trữ sự đồng ý của khách hàng là cho phép công ty lưu trữ thông tin cá nhân?

- Bản thân form đăng ký này là đang thu thập dữ liệu cá nhân, vậy đang có chính sách bảo mật thế nào và chưa có chỗ nào để người đăng ký đồng ý việc thu thập dữ liệu cá nhân?

26

Điều 9 Luật Bảo vệ dữ liệu cá nhân 2025, Điều 11.3 Nghị định 13/2023/NĐ-CP, "Sự đồng ý của chủ thể dữ liệu cá nhân được **thể hiện bằng phương thức rõ ràng, cụ thể, có thể in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được."**

Để lưu vào cơ sở dữ liệu của công ty cần có bằng chứng rõ ràng:

- **Email hoặc tin nhắn đồng thuận:** Có email hoặc tin nhắn xác nhận đồng ý từ khách hàng. Nếu không có, gửi email recap sau cuộc gặp để bên kia xác nhận thông tin.
- **Bản điện tử:** tích vào checkbox, ký điện tử, ký số, xác nhận OTP trên form đăng ký điện tử.
- **Văn bản giấy:** ký trực tiếp trên form đồng ý về việc thu thập/ xử lý dữ liệu cá nhân.
- **Hệ thống CRM**: có trường lưu trữ bằng chứng về sự đồng ý
- Dữ liệu được nhân viên thu thập thiếu bằng chứng về sự đồng ý không được phép nhập vào hệ thống Công ty.

27

Bản thân form đăng ký này là đang thu thập dữ liệu cá nhân, vậy đang có chính sách bảo mật thế nào và chưa có chỗ nào để người đăng ký đồng ý việc thu thập dữ liệu cá nhân?

Form đăng ký là nơi thu thập dữ liệu cá nhân nên bắt buộc phải có chính sách bảo mật rõ ràng và phần cho người dùng đồng ý việc thu thập, sử dụng dữ liệu. Nếu không có phần đồng ý và link chính sách bảo mật, form vi phạm quy định về sự đồng ý minh bạch trong luật bảo vệ dữ liệu cá nhân. Doanh nghiệp cần bổ sung checkbox đồng ý, cung cấp link chính sách bảo mật, và cam kết bảo vệ thông tin để đảm bảo tuân thủ pháp luật và tạo niềm tin cho khách hàng.

28

LNT
& PARTNERS
Innovative Legal Solutions

29

LNT & PARTNERS

INNOVATIVE LEGAL SOLUTIONS

TỔNG QUAN VỀ CÔNG TY

70+ Chuyên gia tư vấn

11 Luật sư thành viên

2 Văn phòng

12+ Lĩnh vực hoạt động

30

LUẬT SƯ THÀNH VIÊN


Bùi Ngọc Hồng


Hoàng Nguyễn Hạ Quyên


Lê Nết


Nguyễn Anh Tuấn


Trần Thái Bình


Nguyễn Xuân Thủy


Vũ Thanh Minh


Nguyễn Công Phú


Dương Bá Ánh Duyên


Lương Trung Vân Nhi

Các Luật sư thành viên của chúng tôi có ít nhất 15 năm kinh nghiệm pháp lý. Không chỉ là những chuyên gia về luật Việt Nam, đội ngũ luật sư LNT & Partners cũng có kinh nghiệm làm việc phong phú với nhiều vụ việc có liên quan đến hệ thống pháp luật lớn khác bao gồm Nhật Bản, Hàn Quốc, các nước Đông Nam Á, Châu Âu và Mỹ.

Tại LNT & Partners, chúng tôi tự hào về khả năng dung hòa giữa các quy định pháp luật và mong muốn của khách hàng, khả năng mở rộng các mối quan hệ trong cộng đồng pháp luật và doanh nghiệp vì lợi ích khách hàng và khả năng dành được niềm tiên của khách hàng. Chúng tôi có khả năng cung cấp cái nhìn sâu sắc về pháp lý và diễn giải về các chính sách và pháp luật của địa phương.

31

LĨNH VỰC HOẠT ĐỘNG

- Chống Độc Quyền / Cạnh Tranh
- Thị Trường Vốn
- Quản Trị Doanh Nghiệp
- Đầu Tư Nước Ngoài
- Sở Hữu Trí Tuệ
- M&A
- Bất động sản
- Tài Chính & Ngân Hàng
- Tuân Thủ Pháp Luật
- Lao Động
- Phá Sản & Tái Cấu Trúc
- Giải quyết tranh chấp
- Dự án
- Thuế

32

NGÀNH NGHỀ HOẠT ĐỘNG

- Ngân Hàng
- Giáo Dục
- Hàng Tiêu Dùng Nhanh
- Khách sạn, nghỉ dưỡng & du lịch
- Bảo Hiểm
- Dược Phẩm
- Bất động sản
- Phân Phối & Bán Lẻ
- Năng Lượng & Tài Nguyên
- Chăm Sóc Sức Khỏe & Khoa Học Đời Sống
- Cơ Sở Hạ Tầng
- Sản Xuất
- Góp Vốn Tư Nhân
- Công Nghệ, Truyền Thông & Viễn Thông

33

GIẢI THƯỞNG VÀ XẾP HẠNG

INNOVATIVE LEGAL SOLUTIONS

Chuyên môn trong các lĩnh vực của LNT & Partners đã nhận được đánh giá cao từ các tổ chức trong khu vực và quốc tế như **Legal 500, Financial Times, IFLR1000, Chambers, asialaw Profiles, Benchmark Litigation và Asian Legal Business.**

ALB SE ASIA
Thomson Reuters

Công ty Luật Việt Nam của Năm 2019, 2022, 2023, 2024, 2025
Công ty Luật Việt Nam của Năm trong Hàng không, Y tế và Chăm sóc sức khỏe, Dịch vụ Ngân hàng và Tài chính, Trọng tài, Xây dựng 2015, 2021, 2022

Legal 500 Châu Á – Thái Bình Dương

Công ty Luật hàng đầu trong lĩnh vực Tài chính & Ngân hàng, Doanh nghiệp / Mua bán & Sáp nhập, Giải quyết tranh chấp, Lao động, Dự án & Năng lượng, Thuế, Bất động sản & Xây dựng 2025

Benchmark Litigation Châu Á – Thái Bình Dương

Xếp hạng Tier 1 trong lĩnh vực Tranh chấp Giao dịch và Thương mại, Tranh chấp Năng lượng và xây dựng năm 2025

In-House Community

Công ty Luật Việt Nam của năm trong lĩnh vực Doanh nghiệp và Mua bán & Sáp nhập, Chống độc quyền / Cạnh tranh, Trọng tài Quốc tế, Tranh tụng và Giải quyết tranh chấp, Dự án và Tài chính Dự án, Lao động, Sở hữu trí tuệ, Khoa học đời sống 2018 - 2025

Financial Times

Top 25 Công ty Luật Sáng Tạo Châu Á Thái Bình Dương 2015, 2016, 2019
Đề cử giải thưởng Luật sư sáng tạo Châu Á Thái Bình Dương 2022

34

LNT & PARTNERS

GIẢI THƯỞNG VÀ XẾP HẠNG

INNOVATIVE LEGAL SOLUTIONS

Chuyên môn trong các lĩnh vực của LNT & Partners đã nhận được đánh giá cao từ các tổ chức trong khu vực và quốc tế như **Legal 500, Financial Times, IFLR1000, Chambers, asialaw Profiles, Benchmark Litigation và Asian Legal Business.**

Chambers Global

Xếp hạng trong Chambers Global lĩnh vực Doanh nghiệp / Mua bán & Sáp nhập và Tài chính & Ngân hàng 2023, 2024

Chambers Asia-Pacific

Xếp hạng trong Chambers Asia-Pacific lĩnh vực Doanh nghiệp / Mua bán & Sáp nhập, Tài chính & Ngân hàng, Giải quyết Tranh chấp, Bất động sản, Lao động, Dự án, Cơ sở hạ tầng & Năng lượng 2019 - 2024

asialaw Profiles

Công ty Luật M&A nổi bật tại Việt Nam 2020, 2019, 2016 Công ty Luật được đánh giá cao trong lĩnh vực Tài chính & Ngân hàng, Doanh nghiệp và M&A, Xây dựng, Giải quyết tranh chấp, Thị trường vốn, Dự án và Cơ sở Hạ tầng, Bất động sản 2016 - 2024

The Legal 500 Asia-Pacific

Công ty Luật hàng đầu trong lĩnh vực: Tài chính & Ngân hàng, Doanh nghiệp / M&A, Giải quyết tranh chấp, Lao động, Dự án & Năng lượng, Thuế, Bất động sản & Xây dựng 2018, 2022, 2023, 2024

ALB Thomson Reuters

Nhà tuyển dụng của Năm 2014 – 2016, 2018 – 2023

35

LNT & PARTNERS

Văn phòng Hồ Chí Minh
Tầng 21, Tòa nhà Bitexco Financial Tower
Số 02 Hải Triều, Phường Sài Gòn
Thành Phố Hồ Chí Minh, Việt Nam
Điện thoại: + 84 28 3821 2357
Fax: + 84 28 3910 3733

Văn phòng Hà Nội
Phòng 1203, Tầng 12, Tòa nhà Pacific Place
83B Lý Thường Kiệt, Phường Cửa Nam
Hà Nội, Việt Nam
Điện thoại: + 84 24 3824 8522
Fax: + 84 24 3824 8580

www.LNTpartners.com

www.VietnamLawInsight.com

36

Thông tin của Người tiêu dùng và Rủi ro Pháp lý trong Thương mại xuyên biên giới

Quế Anh Phạm

1

Nội dung chính

- Một số ví dụ liên quan tới thông tin của NTD tại các quốc gia khác trên thế giới
- Thông tin của NTD và các quy định pháp lý liên quan
- Một số lưu ý cho các doanh nghiệp

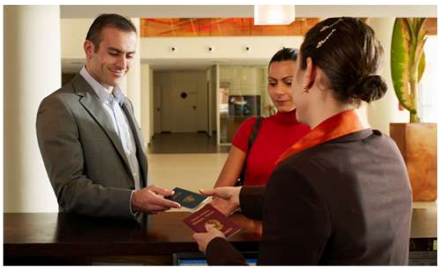
2

Case 1: Khách sạn Marins Playa S.A.

- Năm 2022 – Cơ quan Bảo vệ Dữ liệu Tây Ban Nha (AEPD) phạt khách sạn Marins Playa S.A. 30,000 euro (~900 triệu VND) vì đã scan hộ chiếu của một khách du lịch Hà Lan trên đó có ảnh chụp chân dung và **sử dụng hình ảnh đó để xác minh danh tính của du khách** khi thanh toán dịch vụ, mà không có sự đồng thuận của du khách.
- Khách du lịch người Hà Lan đã khiếu nại tới Cơ quan Bảo vệ Dữ liệu Hà Lan (AP) và cơ quan này đã gửi khiếu nại đó cho AEPD xử lý theo Quy định chung về Bảo vệ Dữ liệu (GDPR) của Liên minh Châu Âu (EU). Sau quá trình điều tra, AEPD quyết định án phạt vì cho rằng:
  - KS có cơ sở pháp lý để scan hộ chiếu của khách bằng công nghệ OCR, nhằm thu thập và cung cấp **thông tin cần thiết** của khách lưu trú cho cảnh sát (theo điều 6(1)c của GDPR)
  - Tuy nhiên KS không có cơ sở pháp lý để xử lý và sử dụng hình ảnh (trên hộ chiếu) của khách để xác minh danh tính (identity verification) khách khi thanh toán dịch vụ do KS không đề cập đến nội dung này trong chính sách về quyền riêng tư (privacy) của mình, cũng không có lợi ích chính đáng (legitimate interest) để làm như vậy. Ngoài ra, Cơ quan Bảo vệ Dữ liệu Hà Lan (AP) cũng chỉ ra một số biện pháp khác ít xâm phạm riêng tư hơn (less intrusive measures) để xác minh danh tính của du khách.
  - Ngoài mức phạt 30,000 euros, khách sạn Marins Playa cũng phải áp dụng các biện pháp cần thiết khác để đảm bảo quyền riêng tư của khách hàng.
- Vì vụ việc này, mùa hè năm 2024, cơ quan AEPD đã tiến hành kiểm tra hàng loạt các khách sạn và cơ sở lưu trú vì hành vi photocopy hoặc scan hộ chiếu của du khách sẽ bị coi là vi phạm GDPR. Án phạt nhỏ nhất được áp dụng là mức 2,000 euros với một cơ sở cung cấp dịch vụ du lịch vì đã photo hộ chiếu của du khách.

3

- Trong nghành du lịch, việc thu thập và xử lý thông tin / dữ liệu cá nhân là không thể thiếu để đảm bảo việc cung cấp dịch vụ.
- Tuy nhiên, sự hiện diện của nhiều bên trung gian (intermediaries) trong quá trình xử lý thông tin khách hàng và cung cấp dịch vụ có thể dẫn đến nhiều rủi ro nếu thông tin /dữ liệu cá nhân không được xử lý đúng chuẩn, gây lộ lọt thông tin.
- Cần có hợp đồng quy định rõ quyền lợi và trách nhiệm giữa các bên liên quan, đặc biệt giữa các nền tảng (đặt phòng ks, đặt vé máy bay, đặt tour, v.v.), bên kiểm soát dữ liệu (data controller – công ty đầu tiên thu thập dữ liệu cá nhân của khách hàng), và bên cung cấp dịch vụ (nhà hàng, khách sạn, công ty vận hành tour, v.v.).
- Các rủi ro thường gặp nhất trong nghành du lịch bao gồm rủi ro về an ninh mạng, thu thập dữ liệu cá nhân của khách hàng hơn mức cần thiết, sử dụng dữ liệu cá nhân mà không có sự đồng ý của khách hàng, và lưu giữ thông tin lâu hơn thời hạn pháp luật cho phép. Ngoài ra, còn cần đảm bảo nhân viên cty không thể tiếp cận và làm lộ lọt / buôn bán dữ liệu nhạy cảm của khách hàng, không sử dụng thông tin cho hoạt động quảng cáo mà không có sự đồng ý của khách hàng, hay các quy định pháp lý khác liên quan tới việc chuyển dữ liệu cá nhân xuyên biên giới, hay việc không kịp thời thông báo cho nhà chức trách về việc lộ lọt thông tin.

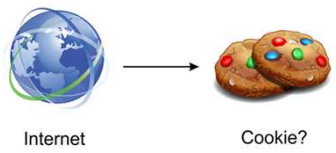


4

Case 2: Công ty Bán lẻ Thời trang Trực tuyến Shein

- Tháng 7 năm 2025 - Công ty bán lẻ thời trang của Trung Quốc mới đây đã bị Ủy ban Quốc gia về Tin học và Tự do (Cnil) – Cơ quan bảo vệ dữ liệu của CH Pháp - đề xuất án phạt 150 triệu Euro về hành vi **sử dụng cookies để theo dõi người dùng** mà **không có sự đồng thuận** của họ. Cơ quan này cũng cáo buộc Shein vẫn tiếp tục theo dõi người dùng (tracking users) kể cả khi họ đã từ chối các cookies của Shein, theo điều tra từ năm 2023.
- Chỉ một tuần trước đó, công ty này cũng vừa bị Cơ quan bảo vệ NTD Pháp phạt 40 triệu euro về hành vi gây nhầm lẫn cho khách hàng trong giảm giá, khuyến mại.
- Song song với đó, Shein cũng đang bị Mạng lưới Hợp tác Bảo vệ NTD (CPC Network) – bao gồm các cơ quan bảo vệ NTD quốc gia của các nước châu Âu và Ủy ban Châu Âu (EC)- yêu cầu ngừng các hành vi vi phạm quyền lợi NTD của mình và cung cấp thông tin để phục vụ điều tra. Shein được xem là một nền tảng trực tuyến cực lớn (Very Large Online Platform) vào tháng 4/2024 theo Đạo luật Dịch vụ Số (Digital Services Act) của Liên minh Châu Âu (EU). Shein bị cáo buộc đã **sử dụng dữ liệu người dùng** thu thập được để thực hiện các hành vi (data-based practices) như:
  - Giảm giá giả mạo nhằm đánh lừa NTD (fake discounts)
  - Tạo áp lực giả tạo để bán hàng (pressure selling)
  - Cung cấp thông tin không đầy đủ, không chính xác, gây nhầm lẫn cho NTD (missing, incorrect and misleading information) về các chính sách đổi trả, hoàn tiền
  - Dán nhãn sản phẩm giả mạo (deceptive product labels)
  - Cung cấp thông tin giả mạo về các hoạt động có tính chất bền vững của Công ty (misleading sustainability claims)
  - Không cung cấp thông tin liên lạc (hidden contact details)
  - Không minh bạch trong hiển thị thông tin về xếp hạng, đánh giá sản phẩm (misleading product rankings, reviews and ratings)

5



- Cookies là các tệp được trang web người dùng truy cập tạo ra. Cookie giúp trải nghiệm trực tuyến của bạn dễ dàng hơn bằng cách lưu thông tin duyệt web. Với Cookies, các trang web có thể duy trì trạng thái đăng nhập của bạn, ghi nhớ tùy chọn trang web và cung cấp nội dung phù hợp với vị trí của người dùng. Như vậy, Cookies thường được sử dụng để lưu lại thông tin của người dùng trên trình duyệt web.
- Có thể chia cookies thành 2 loại, dựa trên nguồn gốc của chúng:
  - Cookies của bên thứ nhất do trang web mà người dùng truy cập tạo ra. Trang web được hiển thị trong thanh địa chỉ.
  - Cookies của bên thứ ba do các trang web khác tạo ra. Các trang web này sở hữu một số nội dung như quảng cáo hoặc hình ảnh mà người dùng thấy trên trang web mình truy cập.
- Ngoài ra, cookies cũng có thể được phân loại thành:
  - Các cookies tối cần thiết (essential cookies) giúp việc truy cập Website của người dùng nhanh hơn, tiện lợi hơn, không quá mất nhiều thời gian đăng nhập lại nhiều lần
  - Các cookies không cần thiết (non-essential cookies) không liên quan đến trải nghiệm (kỹ thuật) của người dùng mà chủ yếu phục vụ cho việc phân tích dữ liệu (analytics) và quảng cáo.
- Chỉ thị về Quyền riêng tư trên không gian mạng (ePrivacy Directive) (2002) và Quy định chung về Bảo vệ Dữ liệu (GDPR) (2018) của EU (Điều 7) có quy định rõ về việc sử dụng cookies cũng như yêu cầu các DN phải có được sự đồng ý rõ ràng của người dùng trước khi tạo và gửi (deploy cookies) tới thiết bị của người dùng.

6

Case 3: Công ty taxi Taxa 4X35

- Năm 2018 – Cơ quan Bảo vệ Dữ liệu Đan Mạch (Datatilsynet) kiểm tra công ty taxi Taxa 4X35 và nhận thấy công ty này đã lưu giữ dữ liệu cá nhân liên quan tới hơn 9 triệu cuốc xe lâu hơn thời hạn 2 năm theo luật định. Cụ thể, công ty này đã xóa bỏ tên và địa chỉ khách hàng, nhưng giữ lại số điện thoại.
- Taxa cho biết họ chỉ định sử dụng các SĐT này như một dạnh 'số tài khoản'. Nhưng do hệ thống máy tính của công ty không thể chuyển đổi SĐT thành các số TK ngẫu nhiên nên đã chọn sử dụng nguyên các SĐT đó. Datatilsynet không chấp nhận lý do này và tuyên phạt Taxa 1.2tr Kroner (~180,000USD).
- Theo Datatilsynet, Taxa đã vi phạm Điều 5 của GDPR liên quan đến 3 nội dung:
  - **Giới hạn về mục đích** (Purpose Limitation): Cty chỉ được phép thu thập dữ liệu người dùng phục vụ cho một mục đích chính đáng (legitimate purpose) và không được phép xử lý dữ liệu theo phương cách không tương thích với mục đích đó.
  - **Dữ liệu thu thập tối thiểu** (Data Minimization): Dữ liệu cá nhân chỉ được phép thu thập và xử lý ở mức độ vừa đủ, có liên quan và giới hạn ở mức cần thiết so với mục đích xử lý.
  - **Giới hạn về thời hạn lưu trữ** (Storage limitation): Dữ liệu cá nhân được lưu giữ dưới hình thức cho phép xác định danh tính của chủ thể dữ liệu không quá thời gian cần thiết cho mục đích xử lý dữ liệu cá nhân đó.

7

Case 4: Hãng hàng không British Airways

- Năm 2018- Hệ thống dữ liệu của Hãng hàng không British Airways bị tin tặc tấn công, khiến cho thông tin cá nhân của khoảng 430,000 hành khách – bao gồm thông tin truy cập, thông tin về thẻ tín dụng, địa chỉ và hành trình, v.v. - bị lộ lọt.
- Tháng 10 năm 2020, Văn phòng Ủy viên Thông tin (Information Commissioner's Office) - cơ quan có vai trò bảo vệ quyền riêng tư dữ liệu và quyền tự do thông tin ở Vương quốc Anh – tuyên phạt BA 20 triệu bảng Anh do không tuân thủ với GDPR và **không thiết lập các biện pháp an ninh cần thiết để bảo vệ dữ liệu cá nhân** của khách hàng.
- Năm 2022, một vụ kiện tập thể GLO (group litigation order) được cho là gồm trên 22,000 nguyên đơn kiện BA vì **thiệt hại cá nhân do vụ lộ lọt dữ liệu này gây ra** được đưa ra xét xử. BA chọn thỏa thuận bồi thường ngoài tòa án (out of court settlement) cho các bên nguyên đơn, tuy nhiên không nhận trách nhiệm (liability), vì đã ngay lập tức tiến hành các biện pháp cần thiết để vãn hồi an ninh mạng, thông báo cho khách hàng cũng như cung cấp dịch vụ quản trị danh tính và thông tin tín dụng miễn phí.
- Các vụ lộ lọt thông tin cá nhân của khách hàng đang diễn ra ngày càng nhiều. Mới nhất gần đây là vụ SportAdmin bị tin tặc tấn công, gây lộ lọt thông tin của khoảng 1 triệu người dùng tại Thụy Điển (tháng 1/2025) hay vụ VNDirect (tháng 3/2024) tại Việt Nam.

8

Thông tin của NTD

- Theo Khoản 3, Điều 3 Luật BV QL NTD 2025: "*Thông tin của người tiêu dùng* bao gồm thông tin cá nhân của người tiêu dùng, thông tin về quá trình mua, sử dụng sản phẩm, hàng hóa, dịch vụ của người tiêu dùng và thông tin khác liên quan đến giao dịch giữa người tiêu dùng và tổ chức, cá nhân kinh doanh."
- Thông tin của người tiêu dùng có thể bao gồm:
  - **Các nội dung do người dùng tạo ra** (User generated content) như các blog, bình luận, ảnh và video do người dùng đăng tải trên các trang mạng xã hội, các đoạn chat hay emails, v.v.
  - **Các dữ liệu về hoạt động hay hành vi** (activity and behavioural data) như các nội dung tìm kiếm trên mạng, các trang web truy cập, các app sử dụng, các hoạt động mua sắm trực tuyến, giá trị giao dịch và phương thức thanh toán, các thói quen sinh hoạt, sở thích, v.v.
  - **Dữ liệu xã hội** (social data) như danh sách bạn bè (friends) và danh sách liên lạc (contacts) trên các mạng xã hội và các ứng dụng (app) liên lạc
  - **Dữ liệu vị trí** (locational data) như địa chỉ nhà, nơi làm việc, thông tin định vị vị trí địa lý (geolocation) hay GPS, địa chỉ IP, hay khoảng cách tới các cá nhân khác
  - **Thông tin nhân khẩu học** (demographic data) như tuổi, giới tinhs, sắc tộc, thu nhập, tôn giáo, quan điểm chính trị hay thiên hướng tính dục
  - **Thông tin cá nhân** (Individual information) như tên, thông tin tài chính và số tài khoản, thông tin về sức khỏe, số BHXH, hồ sơ tư pháp
  - **Thông tin sinh trắc học** (biometrics) như dấu tay, nhận dạng khuôn mặt, mắt và giọng nói

9

Thông tin của NTD và các Hành vi thao túng

- Các hành vi **thao túng NTD** (manipulative practices) là các hành vi cố ý gây tác động tới quyết định mua sắm, sử dụng hàng hóa dịch vụ của NTD theo các phương pháp được cho là không minh bạch (transparent), công bằng (fair), hay hợp đạo lý (ethical).
- Một số hành vi thao túng thường gặp:
  - Quảng cáo phóng đại, gây nhầm nhẫn
  - Không công bố đầy đủ thông tin
  - Tạo tình trạng khan hiếm hay áp lực hết hàng giả mạo
  - Nhắm vào những nhóm NTD dễ bị tổn thương như trẻ em, người cao tuổi, v.v.
  - Thao túng cảm xúc của NTD, đánh vào niềm vui, nỗi buồn, khát vọng của NTD đúng vào thời điểm thích hợp
  - Sử dụng hiệu ứng đám đông (bandwagon effect)
  - Các thiết kế 'đen' (dark patterns) khác
- Đa phần các hành vi thao túng đều được thực hiện trên cơ sở sử dụng những thông tin / dữ liệu của NTD đã thu thập được.

10

Một số quy định pháp lý có liên quan liên quan đến thông tin của NTD

- Điều 10(1)m Luật BVQL NTD 2023 của Việt Nam: Tổ chức, cá nhân kinh doanh bị nghiêm cấm…Thu thập, lưu trữ, sử dụng, chỉnh sửa, cập nhật, hủy bỏ thông tin của người tiêu dùng trái quy định của pháp luật.
- Trách nhiệm của Tổ chức, cá nhân kinh doanh đối với NTD: *Điều 15 – Bảo vệ TT của NTD; Điều 16 – Xây dựng quy tắc bảo vệ TT của NTD; Điều 17 – Thông báo khi thu thập, sử dụng TT của NTD; Điều 18 – Sử dụng TT của NTD; Điều 19 – Bảo đảm an toàn, an ninh thông tin của NTD; Điều 20 – Kiểm tra, chỉnh sửa, cập nhật, hủy bỏ, chuyển giao, ngừng chuyển giao TT của NTD; Điều 25 (14) - Trong hợp đồng giao kết với người tiêu dùng, hợp đồng theo mẫu, điều kiện giao dịch chung, tổ chức, cá nhân kinh doanh không được … quy định người tiêu dùng phải đồng ý cho tổ chức, cá nhân kinh doanh thu thập, lưu trữ, sử dụng thông tin của người tiêu dùng là điều kiện để giao kết hợp đồng, điều kiện giao dịch chung, trừ trường hợp pháp luật có quy định khác.*
- Đạo luật Thị trường Số (DSA) của Liên minh Châu Âu cấm các hành vi thao túng NTD (manipulative practices) với khung hình phạt lên tới 6% tổng doanh thu toàn cầu.
- Các đạo luật về BV NTD nhiều quốc gia trên thế giới đều có quy định về các hành vi gây nhầm lẫn cho NTD (misleading practices) trong đó bao gồm cả liên quan tới việc thu thập, xử lý, sử dụng, chuyển giao và xóa bỏ dữ liệu.
- Ngoài ra, các quy định pháp lý của các quốc gia khác như GDPR đều có khả năng áp dụng ngoài lãnh thổ quốc gia (extra-territorial applicability).

11

Một số lưu ý cho các DN để tránh rủi ro pháp lý (1)

- Thông tin đầy đủ và chính xác cho NTD về:
  - Lý do cần thu thập dữ liệu
  - Những loại dữ liệu thu thập
  - Phương thức thu thập dữ liệu
  - Mục đích sử dụng dữ liệu
  - Thời hạn lưu trữ dữ liệu
- Chỉ lưu trữ dữ liệu trong thời hạn được công bố và chỉ sử dụng dữ liệu cho mục đích đã công bố và được NTD đồng ý.
- Dữ liệu của NTD phải luôn được bảo đảm an ninh - mọi nơi, mọi lúc.
- Nếu NTD yêu cầu xóa bỏ dữ liệu/thông tin về họ, thông tin phải được xóa hoàn toàn và ngay lập tức.
- Không cung cấp thông tin của NTD cho vợ/chồng, con cái, họ hàng hay bạn bè của họ, trừ phi được NTD đồng ý rõ ràng.
- Không chuyển giao thông tin của NTD cho bên thứ 3 trừ phi có sự đồng ý của NTD hay theo quy định pháp luật.
- Đảm bảo rằng thông tin của NTD, khi chuyển giao cho bên thứ 3, không bị sử dụng vào mục đích gây nhầm lẫn, thiệt hại cho NTD, đặc biệt là nhóm NTD dễ bị tổn thương như trẻ em, người cao tuổi, v.v.

12

Một số lưu ý cho các DN để tránh rủi ro pháp lý (2)

- Thông báo cho NTD ngay lập tức trong trường hợp bị lộ lọt thông tin và có các biện pháp sửa chữa (remedial actions) thích hợp.
- Không tham gia vào các hoạt động mua bán dữ liệu cá nhân trên thị trường.
- Tránh sử dụng thuật ngữ kỹ thuật, pháp lý phức tạp khiến NTD không thể hiểu được trong các chính sách, thông báo về quyền riêng tư, cookie hay quy trình thu thập, xử lý và xóa bỏ dữ liệu / thông tin của NTD.
- Tránh sử dụng các chính sách, thông báo về quyền riêng tư dài dòng, khó hiểu.
- Không giấu, đặt các thông tin quan trọng vào các đường link trỏ tới các văn bản khác hoặc giữa các điều khoản chung.

13

Xin cám ơn quý vị đã chú ý lắng nghe!
Câu hỏi, trao đổi xin gửi về
queanh.pham@gmail.com

14