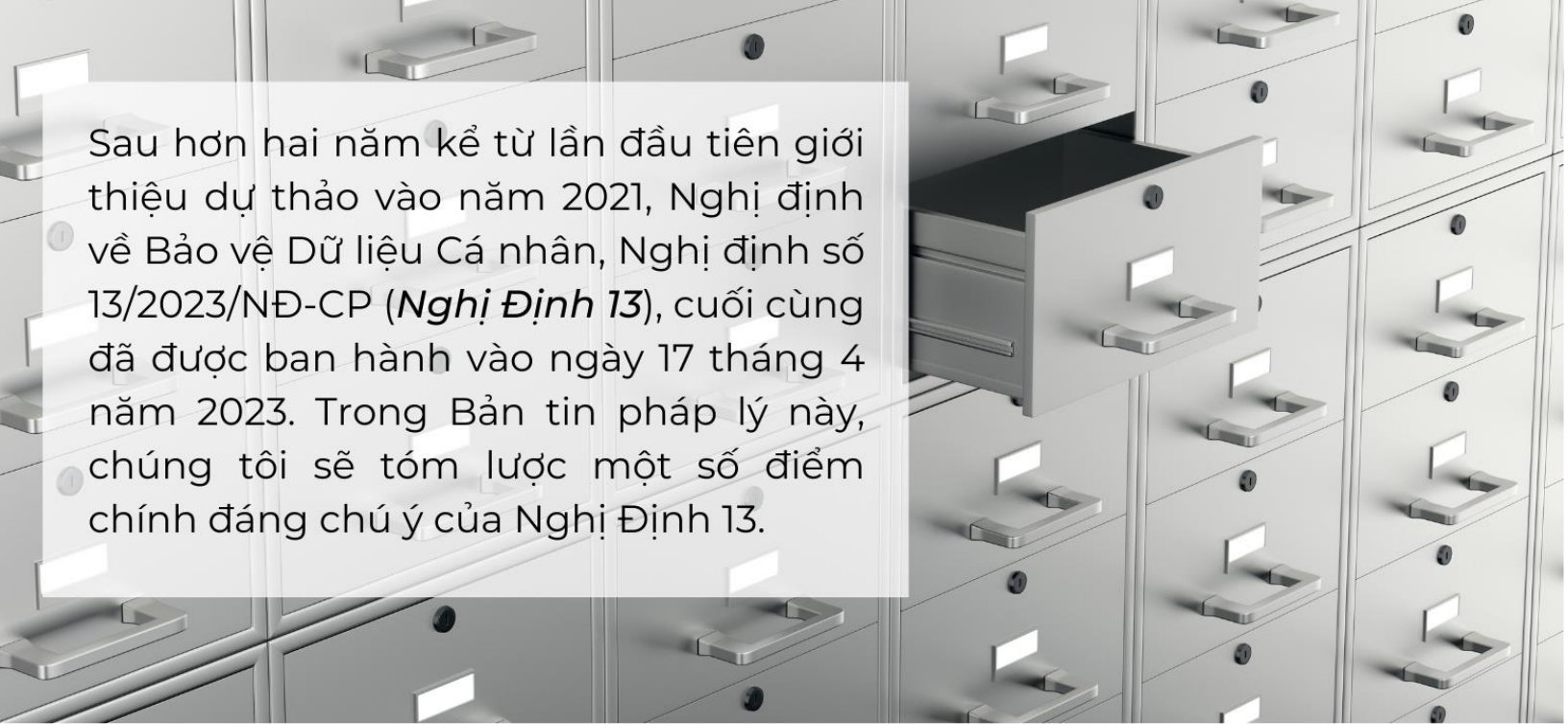


Nghị Định về Bảo vệ Dữ liệu Cá nhân
Bạn đã sẵn sàng?

Bản tin Pháp lý | Tháng 4 năm 2023



Sau hơn hai năm kể từ lần đầu tiên giới thiệu dự thảo vào năm 2021, Nghị định về Bảo vệ Dữ liệu Cá nhân, Nghị định số 13/2023/NĐ-CP (**Nghị Định 13**), cuối cùng đã được ban hành vào ngày 17 tháng 4 năm 2023. Trong Bản tin pháp lý này, chúng tôi sẽ tóm lược một số điểm chính đáng chú ý của Nghị Định 13.

Mục lục

- I. Đối tượng điều chỉnh
- II. Sự đồng ý của chủ thể dữ liệu
- III. Dữ liệu cá nhân nhạy cảm
- IV. Sự đồng ý của chủ thể khác
- V. Xử lý dữ liệu trong trường hợp không cần sự đồng ý của chủ thể dữ liệu
- VI. Quyền của chủ thể dữ liệu
- VII. Bảo vệ dữ liệu cá nhân trong kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo
- VIII. Thông báo vi phạm
- IX. Chuyển dữ liệu ra nước ngoài
- X. Các biện pháp đảm bảo bảo vệ dữ liệu cá nhân
- XI. Hiệu lực

I. Đối tượng điều chỉnh

Nghị Định 13 đưa ra các định nghĩa cho một số bên chính có liên quan đến xử lý dữ liệu cá nhân như sau:

- a. Bên kiểm soát dữ liệu cá nhân là tổ chức, cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân (**Bên Kiểm Soát Dữ Liệu Cá Nhân**).
- b. Bên xử lý dữ liệu cá nhân là tổ chức, cá nhân thực hiện việc xử lý dữ liệu thay mặt cho Bên Kiểm Soát Dữ Liệu, thông qua một hợp đồng hoặc thỏa thuận với Bên Kiểm Soát Dữ Liệu (**Bên Xử Lý Dữ Liệu**).
- c. 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 (**Bên Kiểm Soát và Xử Lý Dữ Liệu Cá Nhân**).
- d. Bên thứ ba là tổ chức, cá nhân ngoài Chủ Thể Dữ Liệu, Bên Kiểm Soát và Xử Lý Dữ Liệu Cá Nhân, Bên Xử Lý Dữ Liệu Cá Nhân được phép xử lý dữ liệu cá nhân (**Bên Thứ Ba**).

So với bản dự thảo cuối cùng, Nghị Định 13 đã mở rộng đối tượng áp dụng. Theo đó, Nghị Định 13 công nhận khái niệm “Bên Kiểm Soát Dữ Liệu”, có nội dung tương tự với định nghĩa trong Quy Định Bảo Vệ Dữ Liệu Chung (General Data Protection Regulation) (**GDPR**).

II. Sự đồng ý của chủ thể dữ liệu

Theo Nghị Định 13, trừ một số trường hợp hạn chế, cần phải có sự đồng ý của chủ thể dữ liệu đối với tất cả các hoạt động trong quy trình xử lý dữ liệu cá nhân. Sự đồng ý của chủ thể dữ liệu chỉ có hiệu lực khi chủ thể dữ liệu tự nguyện và biết rõ các nội dung sau đây:

- a. Loại dữ liệu cá nhân được xử lý;
- b. Mục đích xử lý dữ liệu cá nhân;
- c. Tổ chức, cá nhân được xử lý dữ liệu cá nhân; và
- d. Các quyền, nghĩa vụ của chủ thể dữ liệu.

Ngoài ra, sự đồng ý của chủ thể dữ liệu phải được:

- a. Thể hiện rõ ràng, cụ thể bằng văn bản, giọng nói, đánh dấu vào ô đồng ý, cú pháp đồng ý qua tin nhắn, chọn các thiết lập kỹ thuật đồng ý hoặc qua một hành động khác thể hiện được điều này;
- b. Tiến hành cho cùng một mục đích. Khi có nhiều mục đích, Bên Kiểm Soát Dữ Liệu Cá Nhân, Bên Kiểm Soát và Xử Lý Dữ Liệu Cá Nhân liệt kê các mục đích để chủ thể dữ liệu đồng ý với một hoặc nhiều mục đích nêu ra; và
- c. Được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

Nghị Định 13 cho phép đồng ý một phần.

Nghị Định 13 cũng quy định rõ rằng sự im lặng hoặc **không** phản hồi của chủ thể dữ liệu không được coi là sự đồng ý.

III. Dữ liệu cá nhân nhạy cảm

Khi xử lý dữ liệu cá nhân nhạy cảm, chủ thể dữ liệu phải được thông báo về việc này. Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân gồm:

- a. Quan điểm chính trị, quan điểm tôn giáo;
- b. Tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu;
- c. Thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc;
- d. Thông tin về đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân;
- e. Thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân;
- f. Thông tin về đời sống tình dục, xu hướng tình dục của cá nhân;
- g. Dữ liệu về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;
- h. Thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, các tổ chức được phép khác, gồm: thông tin định danh khách hàng theo quy định của pháp luật, thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch, thông tin về tổ chức, cá nhân là bên bảo đảm tại tổ chức tín dụng, chi nhánh ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán;
- i. Dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị; và
- j. Dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.

IV. Sự đồng ý của các chủ thể khác

Nghị Định 13 quy định 2 (hai) trường hợp ngoại lệ mà hoạt động xử lý dữ liệu cần sự đồng ý từ các chủ thể khác:

- a. Trường hợp chủ thể dữ liệu bị tuyên bố mất tích, đã chết, việc xử lý dữ liệu cá nhân trong trường hợp này phải được sự đồng ý từ các thành viên trong gia đình của người đó (ví dụ, vợ, chồng, cha, mẹ). Nếu chủ thể dữ liệu không có người thân nào, thì được coi là không có sự đồng ý, và do đó, việc xử lý dữ liệu là không được phép.
- b. Trường hợp chủ thể dữ liệu là trẻ em từ đủ 7 tuổi trở lên, thì phải có sự đồng ý của trẻ em và của cha, mẹ hoặc người giám hộ trước khi thực hiện việc xử lý dữ liệu.

V. Xử lý dữ liệu trong trường hợp không cần sự đồng ý của chủ thể dữ liệu

Điều 17 của Nghị Định 13 quy định 5 (năm) trường hợp mà việc xử lý dữ liệu cá nhân có thể được thực hiện mà không cần sự đồng ý của chủ thể dữ liệu, bao gồm:

- a. Trong trường hợp khẩn cấp, cần xử lý ngay dữ liệu cá nhân có liên quan để bảo vệ tính mạng, sức khỏe của chủ thể dữ liệu hoặc người khác;
- b. Việc công khai dữ liệu cá nhân theo quy định của luật;
- c. Việc xử lý dữ liệu của cơ quan nhà nước có thẩm quyền trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật theo quy định của luật;
- d. Để thực hiện nghĩa vụ theo hợp đồng của chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của luật; và
- e. Phục vụ hoạt động của cơ quan nhà nước đã được quy định theo luật chuyên ngành.

Các trường hợp ngoại lệ nêu trên khá tương đồng với quy định của GDPR. Điểm khác biệt đáng chú ý giữa GDPR và Nghị Định 13 là Nghị Định 13 không quy định trường hợp “việc xử lý dữ liệu là cần thiết để phục vụ lợi ích hợp pháp mà bên kiểm soát hoặc bên thứ ba theo đuổi” như là một ngoại lệ đối với yêu cầu về sự đồng ý.

VI. Quyền của chủ thể dữ liệu

Điều 9 của Nghị Định 13 quy định 11 (mười một) quyền của chủ thể dữ liệu, bao gồm:

- a. Quyền được biết;
- b. Quyền đồng ý;
- c. Quyền truy cập;
- d. Quyền rút lại sự đồng ý;
- e. Quyền xóa dữ liệu;
- f. Quyền hạn chế xử lý dữ liệu;
- g. Quyền cung cấp dữ liệu;
- h. Quyền phản đối xử lý dữ liệu;
- i. Quyền khiếu nại, tố cáo, khởi kiện;
- j. Quyền yêu cầu bồi thường thiệt hại; và
- k. Quyền tự bảo vệ.

Các quyền nêu trên khá tương đồng với quy định của GDPR, ngoại trừ việc GDPR không có quy định về quyền tự bảo vệ và quyền

được di chuyển dữ liệu của GDPR không được ghi nhận tại Nghị Định 13.

Một điểm khác biệt đáng chú ý khác là Nghị Định 13 đặt ra một thời hạn nghiêm ngặt để Bên Kiểm Soát thực hiện một số quyền nhất định của chủ thể dữ liệu. Cụ thể, Bên Kiểm Soát được yêu cầu phải thực hiện quyền hạn chế xử lý dữ liệu và quyền phản xử lý dữ liệu trong vòng 72 giờ kể từ khi nhận được yêu cầu của chủ thể dữ liệu. Thời gian hạn chế này chắc chắn sẽ tạo gánh nặng cho Bên Kiểm Soát, đặc biệt khi họ phải xử lý nhiều yêu cầu phức tạp cùng lúc.

VII. Bảo vệ dữ liệu cá nhân trong kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo

Việc xử lý dữ liệu cá nhân của khách hàng để kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo phải được sự đồng ý của khách hàng, trên cơ sở khách hàng biết rõ nội dung, phương thức, hình thức, tần suất của việc giới thiệu, tiếp thị, và quảng cáo sản phẩm.

VIII. Thông báo vi phạm

Theo Điều 23 của Nghị Định 13, tổ chức, cá nhân phải thông báo cho Cục An Ninh Mạng và Phòng, Chống Tội Phạm Sử Dụng Công Nghệ Cao (**Cục ANM&PCTP**) thuộc Bộ Công An khi phát hiện các trường hợp sau:

- a. Phát hiện hành vi vi phạm pháp luật đối với dữ liệu cá nhân;
- b. Dữ liệu cá nhân bị xử lý sai mục đích, không đúng thỏa thuận ban đầu giữa chủ thể dữ liệu và Bên Kiểm Soát, Bên Kiểm Soát và Xử Lý Dữ Liệu hoặc vi phạm quy định của pháp luật;
- c. Không bảo đảm quyền của chủ thể dữ liệu (hoặc không được đảm bảo và bảo vệ đúng) hoặc không được thực hiện đúng; và
- d. Trường hợp khác theo quy định của pháp luật.

Ngôn ngữ của quy định này khá khái quát nhằm bao quát mọi tình huống liên quan đến vi phạm dữ liệu cá nhân. Chúng tôi lưu ý rằng thông báo phải được gửi tới Cục ANM&PCTP trong vòng 72 giờ sau khi phát hiện hành vi vi phạm nêu trên. Trường hợp thông báo sau 72 giờ thì phải kèm theo lý do chậm thông báo.

IX. Chuyển dữ liệu ra nước ngoài

Việc chuyển dữ liệu cá nhân của công dân Việt Nam ra nước ngoài phải đáp ứng những yêu cầu chính sau đây:

- a. Bên chuyển dữ liệu phải lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài gồm những nội dung sau (trong số những nội dung khác): a) sự đồng ý của chủ thể dữ liệu, và b) (các) văn bản thể hiện sự ràng buộc giữa bên chuyển và bên nhận dữ liệu cá nhân;
- b. Bên chuyển dữ liệu phải luôn giữ hồ sơ có sẵn để Cục ANM&PCTP kiểm tra, đánh giá và phải gửi một (1) bản gốc cho Cục ANM&PCTP trong thời gian sáu mươi (60) ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân; và

- c. Bên chuyển dữ liệu phải thông báo bằng văn bản cho Cục ANM&PCTP thông tin về việc chuyển dữ liệu và chi tiết liên lạc của tổ chức, cá nhân phụ trách bằng văn bản sau khi việc chuyển dữ liệu diễn ra thành công.

So với bản dự thảo gần nhất, Nghị Định 13 đã bỏ các yêu cầu về (i) văn bản chứng minh quốc gia nhận dữ liệu có quy định bảo vệ dữ liệu ở mức độ bằng hoặc cao hơn pháp luật Việt Nam; và (ii) văn bản đồng ý từ Ủy Ban Bảo Vệ Dữ Liệu Cá Nhân của Việt Nam, về tổng thể, việc này có thể giảm bớt gánh nặng cho bên chuyển dữ liệu, giúp các chủ thể này hoạt động tự do và linh hoạt hơn.

Điều 25 cũng nêu cụ thể các trường hợp Bộ Công an có thể yêu cầu bên chuyển dữ liệu ngừng chuyển dữ liệu cá nhân ra nước ngoài như sau:

- a. Khi phát hiện dữ liệu cá nhân được chuyển được sử dụng vào hoạt động vi phạm lợi ích, an ninh quốc gia của nước Cộng Hòa Xã Hội Chủ Nghĩa Việt Nam;
- b. Bên chuyển dữ liệu ra nước ngoài không hoàn thiện hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài theo yêu cầu của Cục ANM&PCTP; và
- c. Để xảy ra sự cố lộ, mất dữ liệu cá nhân của công dân Việt Nam.

Chúng tôi lưu ý rằng không có biện pháp bảo vệ tương tự được quy định trong trường hợp chuyển dữ liệu ra nước ngoài đối với dữ liệu cá nhân của công dân không phải người Việt Nam đang sinh sống hoặc quá cảnh tại Việt Nam.

X. Các biện pháp đảm bảo bảo vệ dữ liệu cá nhân

Các biện pháp đảm bảo bảo vệ dữ liệu cá nhân phải được thực hiện ngay từ khi bắt đầu và xuyên suốt quá trình xử lý dữ liệu cá nhân. Các biện pháp này bao gồm (i) quản lý do tổ chức, cá nhân có liên quan tới xử lý dữ liệu cá nhân thực hiện; (ii) các biện pháp kỹ thuật do tổ chức, cá nhân có liên quan tới xử lý dữ liệu cá nhân thực hiện; (iii) các biện pháp điều tra và tố tụng được thực hiện bởi cơ quan có thẩm quyền; và (iv) các biện pháp khác theo quy định của pháp luật.

Nghị Định 13 cũng quy định các biện pháp hành động cụ thể đối với từng loại dữ liệu cá nhân. Ở đây, chúng tôi muốn đề cập đến dữ liệu cá nhân nhạy cảm, theo đó, Nghị Định 13 yêu cầu phải chỉ định bộ phận và nhân sự phụ trách bảo vệ dữ liệu cá nhân (**Bộ phận/Nhân sự bảo vệ dữ liệu**) và cung cấp thông tin của họ cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân (được thành lập bởi cơ quan nhà nước có thẩm quyền liên quan).

XI. Hiệu lực

Nghị Định 13 sẽ có hiệu lực thi hành từ ngày 1 tháng 7 năm 2023. Theo đó, tất cả đối tượng có liên quan sẽ phải tuân thủ các quy định của Nghị Định 13 kể từ ngày 1 tháng 7 năm 2023, ngoại trừ quy định về chỉ định cá nhân và bộ phận bảo vệ dữ liệu cá nhân. Chúng tôi lưu ý rằng ngoại lệ này chỉ áp dụng cho trong thời gian

hai (02) năm đầu kể từ khi doanh nghiệp thành lập nếu đáp ứng các điều kiện sau:

- a. Là các doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ, doanh nghiệp vừa, doanh nghiệp khởi nghiệp; và
- b. Các doanh nghiệp này không trực tiếp kinh doanh hoạt động xử lý dữ liệu cá nhân.

Công Ty Luật Frasers | Tháng 4 năm 2023

Tác giả



Dương Thị Mai Hương
Luật Sư Cấp Cao
huong.duong@frasersvn.com

Thành phố Hồ Chí Minh

Số 19.01, tầng 19, Tòa nhà Đức
33 Lê Duẩn, Quận 1,
Thành phố Hồ Chí Minh
Điện thoại: +84 28 3824 2733

Email: legalenquiries@frasersvn.com

Hà Nội

Số 1205, tầng 12, Tòa nhà Pacific Place
83B Lý Thường Kiệt, Quận Hoàn Kiếm,
Hà Nội, Việt Nam
Điện thoại: +84 24 3946 1203

Email: legalenquiries@frasersvn.com

Bài viết này chỉ cung cấp một bản tóm tắt về chủ đề được đề cập, mà không có bất kỳ nghĩa vụ nào do Công ty Luật Frasers chịu trách nhiệm. Bản tóm tắt không nhằm mục đích cũng như không nên dựa vào nó để thay thế cho lời khuyên pháp lý.

@Bản quyền của bài viết thuộc về Công Ty Luật Frasers.