QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG HOẠT ĐỘNG CỦA TỔ CHỨC TÍN DỤNG TẠI VIỆT NAM

NGUYỄN VĂN MINH
Đoàn Luật sư Thành phố Hồ Chí Minh
Ho Chi Minh City Bar Association
Email: nvminhls@gmail.com

Tóm tắt

Bài viết phân tích một số tác động của quy định về bảo vệ dữ liệu cá nhân (DLCN) liên quan đến nghĩa vụ bảo vệ DLCN của khách hàng trong hoạt động của các tổ chức tín dụng, trên cơ sở tham chiếu đến Quy định chung về bảo vệ DLCN của Liên minh châu Âu (General Data protection Regulation of European Union, GDPR) và đưa ra một vài khuyến nghị nhằm tuân thủ tốt hơn, góp phần hoàn thiện quy định về bảo vệ DLCN tại Việt Nam.

Từ khóa: *dữ liệu cá nhân, bảo vệ dữ liệu cá nhân, quyền riêng tư, GDPR, tổ chức tín dụng, TCTD, ngân hàng*

Abstract

The article analyzes certain impacts of personal data protection regulations related to the obligations of credit institutions to safeguard customers' personal data. This analysis references the General Data protection Regulation (GDPR) of the European Union and offers recommendations for better compliance, aiming to contribute to the improvement of personal data protection regulations in Vietnam.

Keywords: *personal data, personal data protection, privacy right, GDPR, credit institutions, CI, bank*
Ngày nhận bài: 30/11/2023 **Ngày duyệt đăng: 09/05/2024**

1. Tìm hiểu chung về dữ liệu cá nhân

1.1. Định nghĩa về dữ liệu cá nhân

Thuật ngữ dữ liệu cá nhân (DLCN) lần đầu tiên được định nghĩa cụ thể trong Nghị định số 13/2023/NĐ-CP, theo đó DLCN có thể là thông tin ở dạng điện tử hoặc phi điện tử, và quan trọng là phải gắn liền hoặc giúp xác định một cá nhân. Quy định này tương đồng với Điều 4(1) Quy định chung về Bảo vệ Dữ liệu cá nhân của Liên minh châu Âu (*General Data protection Regulation, GDPR*), theo đó cá nhân được xác định có thể trực tiếp hoặc gián tiếp thông qua các yếu tố như họ tên, số định danh, dữ liệu vị trí, hoặc các yếu tố thể chất, sinh lý, di truyền, tâm lý, văn hóa. Nếu thông tin không liên quan hoặc không giúp xác định cá nhân, nó có thể không được coi là DLCN.[1] Điều này nhấn mạnh tầm quan trọng của việc bảo vệ dữ liệu cá nhân trong bối cảnh công nghệ phát triển mạnh mẽ.

1.2. Thông tin khách hàng tại tổ chức tín dụng là dữ liệu cá nhân cơ bản hay nhạy cảm

Nghị định số 13/2023/NĐ-CP phân chia DLCN thành hai loại DLCN cơ bản và DLCN nhạy cảm tại khoản 3 và khoản 4 Điều 2, dựa trên mức độ

1 Nguyễn Quỳnh Trang, "Pháp luật về bảo hộ dữ liệu cá nhân trong bối cảnh phát triển trí tuệ nhân tạo và các công nghệ số mới nổi khác", *Tạp chí Pháp luật và thực tiễn*, số 50, 2022.

riêng tư và tác động đến cá nhân khi DLCN của họ được sử dụng hoặc xử lý. DLCN nhạy cảm được giải thích 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 đến quyền và lợi ích hợp pháp của cá nhân". Điều đáng chú ý là các thông tin trong danh mục DLCN cơ bản thường được thu thập, sử dụng rộng rãi trong các giao dịch thông thường tại ngân hàng. Một ví dụ là thông tin khách hàng tại các tổ chức tín dụng (TCTD), như liệt kê tại điểm h khoản 4 Điều 2 của Nghị định số 13/2023/NĐ-CP, bao gồm thông tin định danh, tài khoản, giao dịch, và tài sản, thuộc danh mục DLCN nhạy cảm. Từ đây, có hai điểm cần làm rõ:

Thứ nhất, khi đối chiếu với Nghị định số 117/2018/NĐ-CP về việc giữ bí mật thông tin khách hàng, thông tin định danh như họ tên, ngày sinh, quốc tịch, địa chỉ, dù là DLCN cơ bản, lại được liệt kê trong danh mục DLCN nhạy cảm tại Nghị định số 13/2023/NĐ-CP. Câu hỏi đặt ra là liệu thông tin khách hàng tại TCTD, dù cơ bản, cũng nên được bảo vệ như DLCN nhạy cảm?

Thứ hai, điểm h khoản 4 Điều 2 của Nghị định số 13/2023/NĐ-CP còn liệt kê cả thông tin về tổ chức là bên bảo đảm tại TCTD vào danh mục DLCN nhạy cảm, mặc dù Nghị định này chỉ áp dụng cho dữ liệu cá nhân. Điều này gây ra sự khó hiểu, vì việc mở rộng phạm vi DLCN bao gồm thông tin của tổ chức có thể ảnh hưởng đến các TCTD trong việc tuân thủ các quy định bảo mật và xử lý dữ liệu nhạy cảm.

2. Tư cách của các bên trong quá trình xử lý dữ liệu cá nhân của khách hàng

2.1. Phân biệt Bên kiểm soát dữ liệu cá nhân và Bên xử lý dữ liệu cá nhân

"Bên kiểm soát DLCN"[2] được định nghĩa là tổ chức, cá nhân quyết định mục đích và phương tiện xử lý DLCN. Hiểu theo cách khác, Bên kiểm soát DLCN là đối tượng trực tiếp xác lập các mối quan hệ, thỏa thuận với chủ thể dữ liệu về mục đích, cách thức thu thập, sử dụng DLCN của chủ thể dữ liệu. Ví dụ, khi một cá nhân mở tài khoản thanh toán tại ngân hàng, cá nhân đó phải cung cấp thông tin và giấy tờ cần thiết. Ngân hàng được coi là Bên kiểm soát DLCN vì quyết định mục đích sử dụng DLCN (mở tài khoản, giao dịch thanh toán) và phương tiện xử lý (thu thập dữ liệu bằng điện tử hoặc phi điện tử).

"Bên xử lý DLCN"[3] được định nghĩa 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. Điểm mấu chốt phân biệt giữa Bên kiểm soát DLCN và Bên xử lý DLCN nằm ở quyền quyết định. Bên xử lý DLCN không trực tiếp xác lập mối quan hệ với chủ thể dữ liệu hoặc, nếu có, chỉ thực hiện thay mặt và theo ủy quyền của Bên kiểm soát

2 Xem thêm khoản 9 Điều 2 Nghị định số 13/2023/NĐ-CP.

3 Khoản 10 Điều 2 Nghị định số 13/2023/NĐ-CP.

DLCN. Bên xử lý không quyết định mục đích, phương tiện xử lý DLCN mà chỉ thực hiện trong phạm vi hợp đồng hoặc thỏa thuận với Bên kiểm soát, giới hạn ở các công việc mà Bên kiểm soát đồng ý. Điều này cũng đã được đại diện Bộ Công an giải đáp trong Hội nghị phổ biến, hướng dẫn Nghị định số 13/2023/NĐ-CP tổ chức tại Hà Nội vào ngày 07/06/2023.[4] Theo đó, đối với trường hợp một bên là đại lý bảo hiểm trong mối quan hệ với khách hàng (bên mua bảo hiểm) thì đại lý bảo hiểm mặc dù là bên tiếp xúc, thu thập thông tin của khách hàng đầu tiên nhưng chỉ là Bên xử lý DLCN, bởi vì đại lý bảo hiểm chỉ đang giữ vai trò nhận ủy quyền, thay mặt doanh nghiệp bảo hiểm[5] (là Bên kiểm soát DLCN) thực hiện thu thập thông tin trong giao dịch với khách hàng.

Theo định nghĩa tại Nghị định 13/2023/NĐ-CP, Bên xử lý DLCN phải trực tiếp xác lập hợp đồng hoặc thỏa thuận với Bên kiểm soát DLCN. Điều này dẫn đến trường hợp, nếu một bên thực hiện hoạt động tương tự như Bên xử lý DLCN nhưng không có hợp đồng hoặc thỏa thuận với Bên kiểm soát DLCN, thì không được coi là Bên xử lý DLCN. Ví dụ, các ngân hàng thường thuê nhà thầu cung cấp giải pháp công nghệ thông tin để xử lý dữ liệu khách hàng khi mở tài khoản trực tuyến. Nhà thầu này được xác định là Bên xử lý DLCN. Tuy nhiên, nếu nhà thầu thuê thêm nhà thầu phụ tham gia xử lý dữ liệu, việc xác định tư cách của nhà thầu phụ như một bên thứ ba sẽ gặp khó khăn.

Theo GDPR, các nhà thầu phụ được coi là Bên đồng xử lý DLCN (*sub-processor*) theo Điều 28(2). GDPR quy định rằng Bên xử lý DLCN không được hợp tác với bên khác mà không có sự cho phép trước bằng văn bản của Bên kiểm soát DLCN. Phạm vi của bên thứ ba được giới hạn trên cơ sở cho phép trực tiếp từ Bên kiểm soát hoặc Bên xử lý DLCN, không bao gồm sự cho phép gián tiếp hoặc quy định pháp luật địa phương.

Pháp luật Việt Nam, theo Nghị định 13/2023/NĐ-CP, không quy định rõ việc được phép xử lý DLCN phải dựa trên cơ sở nào. Tác giả cho rằng có thể hiểu rộng rằng sự cho phép này có thể đến từ chủ thể dữ liệu, Bên kiểm soát DLCN, Bên xử lý DLCN, hoặc từ quy định pháp luật. Tuy nhiên, Nghị định chưa đề cập đến chế định Bên đồng xử lý DLCN như GDPR, tạo khoảng trống pháp lý trong thực tiễn xử lý dữ liệu. Vì thế, tác giả bài viết đưa ra một số gợi ý cách xác định tư cách Bên thứ ba như sau:

– Bên được Bên kiểm soát DLCN *gián tiếp đồng ý* việc xử lý DLCN thông qua một hợp đồng giữa Bên kiểm soát DLCN và Bên xử lý DLCN, ví dụ như Bên xử lý DLCN thỏa thuận với Bên kiểm soát DLCN rằng họ được quyền cung cấp DLCN cho công ty mẹ, công ty liên kết, nhà thầu phụ

4 Bộ Công an, *Tài liệu Hội nghị phổ biến, hướng dẫn Nghị định số 13/2023/NĐ-CP ngày 17 tháng 04 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân*, 2023, tr. 51.

5 Khoản 5 Điều 4 Luật Kinh doanh bảo hiểm năm 2022: *"5. Hoạt động đại lý bảo hiểm là một hoặc một số hoạt động theo ủy quyền của doanh nghiệp bảo hiểm…"*.

(*sub-contractor*) của Bên xử lý DLCN;

- Bên tiếp nhận thông tin theo hợp đồng (không mang tính chất ủy quyền xử lý DLCN) với Bên kiểm soát DLCN;

- Bên tiếp nhận thông tin không theo hợp đồng với Bên kiểm soát DLCN, ví dụ như TCTD thỏa thuận với khách hàng rằng TCTD được quyền tiết lộ thông tin cho Bên thứ ba là công ty mẹ, công ty liên kết của TCTD đó; hoặc bên tiếp nhận thông tin này có thể xuất phát từ quy định của pháp luật, ví dụ như cơ quan nhà nước, tổ chức, cá nhân có thẩm quyền;

- Bên được chính chủ thể dữ liệu trực tiếp đồng ý việc xử lý DLCN nhưng không phải là Bên kiểm soát DLCN, Bên xử lý DLCN, ví dụ như bên được khách hàng là chủ thể dữ liệu ủy quyền thay mặt giao dịch với TCTD.

Tuy vậy, Nghị định này vẫn còn thiếu sự hướng dẫn rõ ràng cách xác định tư cách của các bên.

2.2. Bên kiểm soát và xử lý dữ liệu cá nhân

"Bên kiểm soát và xử lý DLCN" được định nghĩa là tổ chức, cá nhân vừa quyết định mục đích, phương tiện, vừa trực tiếp xử lý DLCN. Thực tế, khi một TCTD được xác định là Bên kiểm soát DLCN, thường đồng thời đảm nhận vai trò xử lý DLCN. Theo khoản 7 Điều 2 Nghị định 13/2023/NĐ-CP, xử lý DLCN bao gồm nhiều hoạt động từ thu thập, phân tích, sử dụng, lưu giữ, chuyển giao, mã hóa đến xóa, hủy DLCN, xuất hiện ở mọi giai đoạn trong quan hệ giữa TCTD và khách hàng. Ví dụ, trong mối quan hệ giữa ngân hàng và khách hàng mở tài khoản thanh toán, ngân hàng đóng vai trò là Bên kiểm soát và xử lý DLCN. Các hoạt động như thu thập thông tin (thông qua biểu mẫu, giấy tờ tùy thân), nhận biết khách hàng, cung cấp thông tin cho cơ quan nhà nước, hoặc lưu trữ thông tin theo quy định đều thuộc hoạt động xử lý DLCN. Dù ngân hàng có thể ủy quyền một số công đoạn xử lý cho bên thứ ba, vai trò chính trong toàn bộ quá trình xử lý DLCN vẫn thuộc về ngân hàng.

3. Sự đồng ý của chủ thể dữ liệu (khách hàng)

Sự đồng ý của chủ thể dữ liệu trong quá trình xử lý DLCN cũng đã được nhắc đến tại Điều 38 của Bộ luật Dân sự năm 2015. Nghị định số 13/2023/NĐ-CP đã quy định chi tiết về sự đồng ý của chủ thể dữ liệu với tiêu chuẩn cao hơn. Mặc dù Nghị định 13/2023/NĐ-CP không quy định rõ nghĩa vụ đảm bảo về sự đồng ý của chủ thể dữ liệu thuộc về bên nào, tuy nhiên nghĩa vụ này đang đặt ra cho Bên kiểm soát hoặc Bên kiểm soát và xử lý DLCN.[6] Cần lưu ý rằng Nghị định 13/2023/NĐ-CP có hiệu lực kể từ ngày 01/07/2023, do đó, tác giả cho rằng các yêu cầu về sự đồng ý của chủ thể dữ liệu chỉ được áp dụng đối với DLCN được thu thập từ sau ngày 01/07/2023.[7]

6 Khoản 10 Điều 11 Nghị định số 13/2023/NĐ-CP.
7 Bộ Công an, *tlđd*, tr. 43.

3.1. Nội dung bắt buộc của sự đồng ý

Khoản 2 Điều 11 của Nghị định 13/2023/NĐ-CP quy định sự đồng ý của chủ thể dữ liệu *chỉ có hiệu lực* khi chủ thể dữ liệu tự nguyện và biết rõ bốn nội dung sau: (i) loại DLCN được xử lý, (ii) mục đích xử lý DLCN, (iii) tổ chức, cá nhân được xử lý DLCN và (iv) các quyền, nghĩa vụ của chủ thể dữ liệu. Như vậy, từ ngày 01/07/2023 trở đi, các TCTD sẽ phải có trách nhiệm đảm bảo sự đồng ý của khách hàng là chủ thể dữ liệu với đầy đủ các nội dung trên khi thực hiện thu thập, xử lý DLCN. Tác giả cho rằng với các TCTD đang có giao dịch với số lượng lớn khách hàng, việc chứng minh được khách hàng đã "tự nguyện và biết rõ" các nội dung trên trong trường hợp có tranh chấp xảy ra là tương đối khó khăn.

Hiện nay, Nghị định 13/2023/NĐ-CP chưa có giải thích rõ yếu tố "tự nguyện" khi đưa ra sự đồng ý sẽ được hiểu như thế nào, vì vậy sẽ khá bất lợi cho các khách hàng nếu chỉ dựa vào việc khách hàng đã ký tên hoặc xác nhận dưới hình thức khác vào các điều khoản về sự đồng ý do các TCTD soạn sẵn để đánh giá tính hợp lệ của sự đồng ý. Liên quan đến vấn đề này, Điều 7(4) của GDPR cũng đặt ra một điều kiện quan trọng khá tương đồng với Nghị định 13/2023/NĐ-CP, cụ thể sự đồng ý đó phải được chủ thể dữ liệu đưa ra một cách tự nguyện (*consent is freely given*). Theo đó, Ủy ban Bảo vệ dữ liệu châu Âu (*European Data protection Board - EDPB*) đã giải thích yếu tố "*freely given"* này tại mục 3.1 trong ấn phẩm hướng dẫn về sự đồng ý khi xử lý DLCN vào tháng 05 năm 2020 như sau: Sự đồng ý sẽ trở nên không hợp lệ nếu chủ thể dữ liệu cảm thấy bị ép buộc hoặc nếu không đồng ý sẽ gây ra các hệ quả bất lợi cho họ, như sự đồng ý được lồng ghép vào trong các điều khoản chung của hợp đồng mà chủ thể dữ liệu không được thỏa thuận khác đi sẽ được xem là không hợp lệ, hoặc khi sự đồng ý là điều kiện bắt buộc để cung cấp dịch vụ, thực hiện một hợp đồng.[8]

EDPB đưa ra một minh họa khá rõ đối với trường hợp một ngân hàng yêu cầu các khách hàng phải đồng ý cho một bên thứ ba được phép sử dụng các thông tin giao dịch thanh toán của khách hàng cho mục đích cá nhân hóa các quảng cáo, tiếp thị.[9] Nếu không đồng ý, khách hàng sẽ bị từ chối cung ứng dịch vụ/ đóng tài khoản hoặc sẽ bị tăng phí dịch vụ. EDPB cho rằng hoạt động xử lý DLCN này là không cần thiết cho việc thực hiện hợp đồng

8 European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, 2020, tr. 7-8; Stephen Breen, Karim Ouazzane, and Preeti Patel (2020), "GDPR: Is your consent valid?", *Business Information Review*, Vol. 37(1), tr. 19-24, https://doi.org/10.1177/0266382120903254.

9 European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, 2020, tr. 11; Patrick Folkert Anton van Erkel, David Nicolas Hopmann, Morten Skovsgaard, Ludovic Terren, "The Role of Consent Form Design Under GDPR: A Survey Experiment", *International Journal of Public Opinion Research*, Vol. 36(1), Spring 2024, https://doi.org/10.1093/ijpor/edad047.

với khách hàng và cho mục đích thông thường của việc cung ứng dịch vụ tài khoản ngân hàng, do đó mặc dù khách hàng đã đồng ý nhưng sự đồng ý này vẫn được xem là không hợp lệ. Một số TCTD sử dụng hai hình thức để lấy sự đồng ý của chủ thể dữ liệu: (i) biểu mẫu về sự đồng ý (*consent form*) với nội dung chi tiết, khách hàng xác nhận trực tiếp; và (ii) điều khoản lồng ghép trong hợp đồng, thỏa thuận, thường ngắn gọn và dẫn chiếu đến chính sách bảo mật trên *website*. Cả hai có thể áp dụng trên giấy hoặc điện tử. Tuy nhiên, hình thức (ii) tiềm ẩn rủi ro hơn, do khó đảm bảo khách hàng hiểu rõ nội dung, đặc biệt khi Nghị định 13/2023/NĐ-CP không coi sự im lặng là đồng ý, buộc TCTD phải chứng minh rõ ràng.

Một ngân hàng thương mại tại Cộng hòa Liên bang Đức đã từng bị phạt 900.000 Euro vì vi phạm Điều 6(1)(f) của GDPR,[10] vì đã có hành vi sử dụng khối lượng lớn dữ liệu của khách hàng (lịch sử giao dịch, tần suất in sao kê, chuyển tiền, thông tin tín dụng) để phân tích thói quen tiêu dùng nhằm phục vụ quảng cáo thương mại. Ngân hàng thuê bên thứ ba hỗ trợ nhưng chỉ có sự đồng ý chung chung từ khách hàng về quảng cáo, không bao gồm việc phân tích dữ liệu chi tiết (*profiling*). Cơ quan Đức cho rằng sự đồng ý này chưa đủ, vi phạm nguyên tắc xử lý dữ liệu cá nhân, đặc biệt khi thực hiện trên quy mô lớn và ảnh hưởng đến các quyền của chủ thể dữ liệu, cũng như vi phạm nguyên tắc cơ bản của xử lý DLCN.[11] Đây cũng là một vấn đề mà các TCTD tại Việt Nam nên lưu ý trong quá trình lấy sự đồng ý của khách hàng, theo đó cần minh bạch cho khách hàng "biết rõ" các mục đích và cách thức mà TCTD xử lý DLCN của họ.

3.2. Các trường hợp ngoại lệ không cần sự đồng ý của chủ thể dữ liệu

Điều 17 Nghị định 13/2023/NĐ-CP quy định năm trường hợp xử lý dữ liệu cá nhân (DLCN) không cần sự đồng ý của chủ thể dữ liệu, nhưng không có quy định mở về các "trường hợp ngoại lệ khác theo quy định pháp luật". Trong thực tế, nhiều trường hợp xử lý DLCN mà không cần sự đồng ý đã được quy định trong các văn bản pháp luật khác. Ví dụ, Điều 7 Bộ luật Tố tụng dân sự 2015 và điểm c khoản 6 Điều 44 Luật Thi hành án dân sự 2008 (sửa đổi, bổ sung 2014) cho phép cung cấp thông tin về điều kiện thi hành án mà không cần sự đồng ý. Tương tự, Điều 11 Nghị định 117/2018/NĐ-CP quy định các tổ chức tín dụng được cung cấp thông tin khách hàng theo yêu cầu của các cơ quan, tổ chức có thẩm quyền mà không cần sự đồng ý của khách hàng. Đối với người tiêu dùng, khoản 3 Điều 18 Luật Bảo vệ quyền lợi người tiêu dùng 2023 (có hiệu lực từ 01/07/2024) bổ sung ba trường hợp ngoại lệ không cần sự đồng ý khi tổ

10 ComplyCloud & CIT Law Firm, *ComplyCloud EU GDPR Casebook 2023*, 2023, tr. 50.

11 Matthias Artzt, and Tran Viet Dung, "Artificial Intelligence and Data Protection: How to Reconcile Both Areas from the European Law Perspective", *Vietnamese Journal of Legal Sciences*, Sciendo, Vol. 7(2), 2022, https://doi.org/10.2478/vjls-2022-0007, tr. 39-58..

chức kinh doanh sử dụng thông tin. Đáng chú ý, điểm b khoản 3 Điều 18 quy định nếu tổ chức kinh doanh yêu cầu thông tin để bán hoặc cung cấp sản phẩm theo yêu cầu của người tiêu dùng, việc sử dụng thông tin không cần thêm sự đồng ý. Ví dụ, ngân hàng yêu cầu khách hàng cung cấp thông tin để cung cấp dịch vụ ngân hàng không cần thêm sự đồng ý nào khác, trừ khi sử dụng thông tin vào mục đích khác như quảng cáo. Sự không đồng nhất giữa Nghị định 13/2023/NĐ-CP và các quy định pháp luật khác tạo ra "độ chênh" trong áp dụng pháp luật.

4. Các hoạt động mà tổ chức tín dụng cần thực hiện để tuân thủ quy định về bảo vệ dữ liệu cá nhân

Dự thảo Luật BV DLVN (lấy ý kiến từ 24/09/2024 đến 24/11/2024) bổ sung nhiều quy định nổi bật so với Nghị định 13/2023/NĐ-CP. Cụ thể, Điều 49 quy định chi tiết hơn về bảo vệ dữ liệu nhạy cảm, yêu cầu thông báo rõ ràng, biện pháp bảo vệ bổ sung, và đánh giá tín nhiệm dữ liệu. Điều này đòi hỏi các TCTD thực hiện mã hóa, quản lý quyền truy cập, cùng các quy trình giám sát bảo mật.

Điều 11 và Điều 12 yêu cầu TCTD phải thông báo và thu thập sự đồng ý rõ ràng trước khi xử lý dữ liệu nhạy cảm, đảm bảo quyền kiểm soát của khách hàng. Điều 37 yêu cầu TCTD có chuyên gia bảo vệ dữ liệu và tổ chức chuyên trách, đồng thời phải đánh giá tín nhiệm bảo mật theo Điều 41. Đối với dữ liệu chuyển ra nước ngoài, Điều 45 yêu cầu thực hiện đánh giá tác động bảo vệ dữ liệu trước khi chuyển, đảm bảo tiêu chuẩn bảo mật nghiêm ngặt. Ngoài ra, khoản 5 Điều 47 nhấn mạnh việc TCTD phải giám sát, quản lý rủi ro để ứng phó với các hành vi vi phạm, bảo vệ quyền lợi khách hàng. Những quy định này yêu cầu TCTD đầu tư vào bảo mật, đồng thời rà soát và cập nhật quy định nội bộ theo yêu cầu khoản 2 Điều 48 Dự thảo Luật. Các TCTD có thể sửa đổi quy định bảo mật theo Nghị định 13/2023/NĐ-CP để đáp ứng tiêu chuẩn mới, tập trung vào việc lưu trữ, bảo vệ thông tin khách hàng, đặc biệt với dữ liệu nhạy cảm.

4.1. Phân loại dữ liệu cá nhân được xử lý

Trước khi thực hiện xây dựng quy trình nội bộ về bảo vệ DLCN của khách hàng, TCTD cần liệt kê ra được mình đang thu thập, xử lý DLCN của các loại khách hàng nào, bao gồm các khách hàng đã, đang trực tiếp thực thiết lập mối quan hệ với các TCTD và các khách hàng khác mặc dù không trực tiếp thiết lập mối quan hệ với TCTD nhưng gián tiếp có phát sinh hoạt động xử lý DLCN từ các TCTD. Ví dụ như khi các TCTD cho khách hàng vay vốn (bên trực tiếp thực thiết lập mối quan hệ với TCTD), khách hàng thường được yêu cầu cung cấp thông tin của người tham chiếu (bên không trực tiếp thiết lập mối quan hệ với TCTD nhưng gián tiếp có phát sinh hoạt động xử lý DLCN từ TCTD) để TCTD có thể liên hệ trong một số trường hợp nhất

định; Hoặc một số trường hợp một ngân hàng có phát sinh hoạt động xử lý DLCN của khách hàng thuộc quản lý của ngân hàng đối tác, như trong một số hoạt động liên quan đến ngân hàng đại lý, ủy thác, tài trợ thương mại. Từ đó, việc xác định nghĩa vụ của các TCTD tùy theo loại khách hàng cũng sẽ khác nhau.

4.2. Đảm bảo và duy trì sự đồng ý từ khách hàng về xử lý dữ liệu cá nhân

TCTD (trong vai trò là Bên kiểm soát DLCN hoặc Bên kiểm soát và xử lý DLCN) cần đảm bảo và duy trì sự đồng ý hợp lệ về việc xử lý DLCN từ các khách hàng là chủ thể dữ liệu. Nghị định 13/2023/NĐ-CP và Dự thảo Luật BV DLCN không quy định rõ về tần suất lấy sự đồng ý của chủ thể dữ liệu, do đó tác giả cho rằng sự đồng ý này chỉ cần được lấy một lần trước khi thực hiện hoạt động thu thập, xử lý DLCN.

Tuy nhiên, về bản chất, sự đồng ý của khách hàng chỉ có hiệu lực đối với các loại thông tin mà khách hàng đã đồng ý cho các TCTD thu thập, xử lý trước đó và tương ứng với mục đích ban đầu các bên đã thỏa thuận. Đối với các loại thông tin mới phát sinh sau thời điểm đồng ý hoặc có sự thay đổi về mục đích xử lý, cần phải được khách hàng đồng ý bổ sung.

4.3. Thông báo đến các khách hàng về xử lý dữ liệu cá nhân

TCTD phải thông báo việc xử lý DLCN đến khách hàng, đặc biệt DLCN nhạy cảm cần đáp ứng tiêu chí riêng. Theo Nghị định 13/2023/NĐ-CP và Dự thảo Luật BV DLCN, thông báo thực hiện trước khi xử lý, nội dung gồm mục đích, cách thức, thời gian, loại DLCN, tổ chức liên quan, hậu quả rủi ro. Điều 13 Dự thảo yêu cầu thông báo bằng văn bản (in/điện tử), đảm bảo minh bạch, giúp khách hàng hiểu quyền và trách nhiệm. Tham khảo GDPR, tác giả nhận thấy các tổ chức nước ngoài thường gộp việc thông báo này vào mẫu đồng ý về xử lý DLCN (*Notice and consent form*) và yêu cầu chủ thể dữ liệu đồng ý ngay tại thời điểm cung cấp, thu thập thông tin cá nhân. Đây cũng là một thông lệ khá hay mà các TCTD có thể tham khảo để áp dụng khi điều này phù hợp với trường hợp ngoại lệ không cần thông báo lại đến khách hàng.

4.4. Xác lập thỏa thuận về xử lý dữ liệu cá nhân của khách hàng với các bên liên quan

Khoản 1 Điều 39 của Nghị định 13/2023/NĐ-CP quy định trách nhiệm Bên xử lý DLCN "Chỉ tiếp nhận DLCN sau khi có hợp đồng hoặc thỏa thuận về xử lý dữ liệu với Bên kiểm soát DLCN". Dự thảo Luật BVDLCN tại Điều 59 yêu cầu hợp đồng hoặc thỏa thuận phải ghi rõ các nội dung liên quan đến quy trình xử lý, bảo mật, thời gian lưu trữ, và các biện pháp bảo vệ cụ thể để bảo đảm an toàn cho DLCN. Bên xử lý dữ liệu chỉ được tiếp nhận và xử lý dữ liệu theo hợp đồng đã ký kết, chịu trách nhiệm trả lại hoặc xóa dữ liệu sau khi hoàn tất. Do đó, các TCTD cần xác lập thỏa

thuận về xử lý DLCN của khách hàng, cho dù TCTD đang đóng vai trò là Bên xử lý DLCN hay Bên kiểm soát DLCN. Theo tác giả, yêu cầu này là hợp lý nhằm góp phần ngăn chặn tình trạng mua bán, truyền tải trái phép thông tin cá nhân, qua đó có thể phân định được trách nhiệm của từng bên khi tham gia vào quá trình xử lý DLCN. Do hai văn bản này không nêu rõ thỏa thuận về xử lý DLCN là một thỏa thuận riêng hay dưới dạng một điều khoản, phụ lục đính kèm theo hợp đồng khác giữa các bên, vì vậy tác giả cho rằng các bên có thể lựa chọn hình thức của thỏa thuận này tùy theo từng hoàn cảnh, miễn là thỏa thuận đó phân định được rõ quyền và nghĩa vụ của mỗi bên liên quan đến việc xử lý DLCN.

4.5. Lập hồ sơ đánh giá tác động gửi về Bộ Công an

TCTD cần lập hồ sơ đánh giá tác động xử lý DLCN và hồ sơ đánh giá tác động chuyển DLCN ra nước ngoài (nếu có phát sinh việc chuyển DLCN ra nước ngoài) theo yêu cầu tại Điều 24, Điều 25 của Nghị định 13/2023/NĐ-CP gửi về Bộ Công an theo mẫu chi tiết được đăng tải công khai trên website cổng thông tin quốc gia về bảo vệ DLCN (https://baovedlcn.gov.vn). Điều 44 của Dự thảo Luật BVDLCN cũng yêu cầu hồ sơ đánh giá tác động phải được hoàn thành và gửi về Bộ Công an trong các trường hợp quan trọng, chẳng hạn như xử lý dữ liệu nhạy cảm, chuyển dữ liệu ra nước ngoài, hoặc các hoạt động xử lý có quy mô lớn. Điều này giúp củng cố tính minh bạch và tăng cường trách nhiệm của các tổ chức trong việc bảo vệ DLCN. ●

Tài liệu tham khảo

[1] Matthias Artzt, and Tran Viet Dung, "Artificial Intelligence and Data Protection: How to Reconcile Both Areas from the European Law Perspective", *Vietnamese Journal of Legal Sciences*, Sciendo, Vol. 7(2), 2022, https://doi.org/10.2478/vjls-2022-0007

[2] Bộ Công an, *Tài liệu Hội nghị phổ biến, hướng dẫn Nghị định số 13/2023/NĐ-CP ngày 17 tháng 04 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân*, 2023

[3] Stephen Breen, Karim Ouazzane, and Preeti Patel (2020), "GDPR: Is your consent valid?", *Business Information Review*, Vol. 37(1), https://doi.org/10.1177/0266382120903254

[4] ComplyCloud & CIT Law Firm, *ComplyCloud EU GDPR Casebook 2023*, 2023

[5] Patrick Folkert Anton van Erkel, David Nicolas Hopmann, Morten Skovsgaard, Ludovic Terren, "The Role of Consent Form Design Under GDPR: A Survey Experiment", *International Journal of Public Opinion Research*, Vol. 36(1), Spring 2024, https://doi.org/10.1093/ijpor/edad047

[6] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, 2020

[7] Nguyễn Quỳnh Trang, "Pháp luật về bảo hộ dữ liệu cá nhân trong bối cảnh phát triển trí tuệ nhân tạo và các công nghệ số mới nổi khác", *Tạp chí Pháp luật và thực tiễn*, số 50, 2022 [trans: Nguyen Quynh Trang, "Law on Personal Data Protection in the Context of Developing Artificial Intelligence and Other Emerging Digital Technologies", *Journal of Law and Practice*, Vol. 50, 2022]