

## BẢN TIN CẬP NHẬT PHÁP LUẬT

Vision & Associates Legal

28/04/2023

### Quy định mới về bảo vệ dữ liệu cá nhân tại Việt Nam

Sau thời gian dài chờ đợi, ngày 17/4/2023, Chính phủ đã ban hành Nghị định số 13/2023/NĐ-CP về Bảo vệ Dữ liệu Cá nhân ("**Nghị định 13**"). Đây là văn bản pháp lý toàn diện đầu tiên quy định về bảo vệ dữ liệu cá nhân tại Việt Nam, đưa ra các yêu cầu mới đối với việc thu thập và xử lý dữ liệu cá nhân. Nghị định 13 sẽ có hiệu lực từ ngày 1/7/2023. Dưới đây là một số nội dung đáng chú ý của Nghị định 13.

#### 1. Phạm vi và đối tượng áp dụng

Nghị định 13 có phạm vi áp dụng rộng, bao gồm cả bên ngoài lãnh thổ Việt Nam và bao trùm gần như tất cả các đối tượng là cá nhân, tổ chức ở Việt Nam và ở nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động xử lý dữ liệu tại Việt Nam.

#### 2. Phân loại dữ liệu cá nhân

Trên cơ sở kế thừa các định nghĩa trước đây về thông tin cá nhân được quy định trong các văn bản pháp luật khác nhau, Nghị định 13 đã phát triển một định nghĩa mới và mở rộng hơn về dữ liệu cá nhân, cụ thể như sau:

*"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."*

Điểm đặc biệt đáng lưu ý là Nghị định 13 đã xác định rất cụ thể thế nào là "*thông tin giúp xác định một con người cụ thể*". Theo đó, "*thông tin giúp xác định một con người cụ thể*" là thông tin thu thập được từ hoạt động của một cá nhân mà khi kết hợp với dữ liệu và thông tin được lưu trữ khác có thể xác định được một con người cụ thể.

Nói một cách tóm tắt, dữ liệu cá nhân được Nghị định 13 phân loại thành hai nhóm chính:

(a) "*dữ liệu cá nhân cơ bản*", bao gồm:

- (i) Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có);
- (ii) Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích;
- (iii) Giới tính;
- (iv) Nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ;
- (v) Quốc tịch;
- (vi) Hình ảnh của cá nhân;
- (vii) Số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế;
- (viii) Tình trạng hôn nhân;
- (ix) Thông tin về mối quan hệ gia đình (cha mẹ, con cái);
- (x) Thông tin về tài khoản số của cá nhân; dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng;
- (xi) Các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể không thuộc dữ liệu cá nhân nhạy cảm dưới đây;

và

(b) "*dữ liệu cá nhân nhạy cảm*", bao gồm:

- (i) Quan điểm chính trị, quan điểm tôn giáo;
- (ii) Tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu;

- (iii) Thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc;
- (iv) Thông tin về đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân;
- (v) Thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân;
- (vi) Thông tin về đời sống tình dục, xu hướng tình dục của cá nhân;
- (vii) Dữ liệu về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;
- (viii) 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;
- (ix) Dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị;
- (x) Dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.

### 3. Phân loại các bên xử lý dữ liệu cá nhân

Nghị định 13 đã đưa ra bốn khái niệm mới về các bên xử lý dữ liệu, bao gồm:

- (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**");
- (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**"); và
- (d) Bên thứ ba là tổ chức, cá nhân ngoài Chủ thể Dữ liệu, Bên Kiểm Soát Dữ liệu, Bên Xử lý Dữ liệu, Bên Kiểm soát và Xử lý Dữ liệu, được phép xử lý dữ liệu cá nhân.

Trong đó, các yêu cầu khắt khe hơn được áp dụng đối với Bên Kiểm soát Dữ liệu và Bên Kiểm soát và Xử lý Dữ liệu.

### 4. Yêu cầu đối với sự đồng ý

Một mặt, Nghị định 13 đã định nghĩa cụ thể "*sự đồng ý*" là sự thể hiện rõ ràng, tự nguyện và khẳng định về việc Chủ thể Dữ liệu cho phép xử lý dữ liệu cá nhân của mình. Cụ thể, sự đồng ý của Chủ thể Dữ liệu phải được thể hiện 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 điều này.

Sự đồng ý của Chủ thể Dữ liệu chỉ có hiệu lực khi họ tự nguyện và biết rõ ràng: (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 đó còn phải được thể hiện ở định dạng có thể được in và sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

Mặt khác, Nghị định 13 cũng quy định các trường hợp ngoại lệ sau đây không cần sự đồng ý của Chủ thể Dữ liệu để xử lý dữ liệu:

- (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. Bên Kiểm soát Dữ liệu, Bên Xử lý Dữ liệu, Bên Kiểm soát và Xử lý Dữ liệu, Bên thứ ba có trách nhiệm chứng minh trường hợp này;
- (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.

#### **5. Đánh giá Tác động Xử lý Dữ liệu Cá nhân (ĐGTĐXLDLCN)**

Nghị định 13 yêu cầu Bên Kiểm soát Dữ liệu, Bên Xử lý Dữ liệu, và Bên Kiểm soát và Xử lý Dữ liệu phải lập và lưu trữ hồ sơ ĐGTĐXLDLCN của mình ("**Hồ sơ Xử lý Dữ liệu**") bằng văn bản, hồ sơ này phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an ("**BCA**"). Hồ sơ ĐGTĐXLCN này được xác lập theo mẫu quy định tại Phụ lục ban hành kèm theo Nghị định 13 kể từ thời điểm bắt đầu xử lý dữ liệu cá nhân.

Ngoài ra, bản chính Hồ sơ Xử lý Dữ liệu phải được gửi đến Cục An ninh Mạng và Phòng, chống Tội phạm Sử dụng Công nghệ Cao trực thuộc Bộ Công an ("**Cục An ninh Mạng**") trong thời hạn 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.

Bên Kiểm soát Dữ liệu, Bên Kiểm soát và Xử lý Dữ liệu, và Bên Xử lý Dữ liệu phải cập nhật, bổ sung Hồ sơ Xử lý Dữ liệu theo mẫu quy định tại Phụ lục ban hành kèm theo Nghị định 13 khi có thay đổi về nội dung hồ sơ đã gửi cho Cục An ninh Mạng.

#### **6. Thông báo xử lý dữ liệu cá nhân**

Nghị định 13 yêu cầu Bên Kiểm soát Dữ liệu và Bên Kiểm soát và Xử lý Dữ liệu phải thông báo cho Chủ thể Dữ liệu về việc xử lý dữ liệu cá nhân của họ. Thông báo phải có các nội dung theo luật định, được thực hiện một lần trước khi tiến hành đối với hoạt động xử lý dữ liệu cá nhân và phải được thể hiện ở định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

#### **7. Thông báo vi phạm quy định bảo vệ dữ liệu cá nhân**

Nghị định 13 cũng yêu cầu trong trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân, tổ chức, cá nhân phải thông báo cho Cục An ninh Mạng. Tuy nhiên, khác với quy định hiện hành yêu cầu phải thông báo "trong vòng 5 ngày" nói chung và "trong vòng 24 giờ" trong lĩnh vực thương mại điện tử nói riêng, Nghị định 13 cho phép thời hạn thông báo vi phạm quy định bảo vệ dữ liệu cá nhân là 72 giờ đối với Bên Kiểm soát Dữ liệu, Bên Kiểm soát và Xử lý Dữ liệu. Trường hợp thông báo sau 72 giờ thì phải kèm theo lý do thông báo chậm, muộn.

#### **8. Yêu cầu khắt khe hơn đối với việc chuyển dữ liệu ra nước ngoài**

Nghị định 13 đặt ra các yêu cầu mới đối với việc chuyển dữ liệu ra nước ngoài, vốn là vấn đề không được điều chỉnh trước khi Nghị định này được ban hành. Cụ thể, trong trường hợp dữ liệu dự định được chuyển ra nước ngoài, bên xử lý dữ liệu chuyển dữ liệu ra nước ngoài, bao gồm cả Bên thứ ba, phải thực hiện các nghĩa vụ sau:

- (a) Lập và lưu giữ hồ sơ Đánh giá Tác động Chuyển Dữ liệu Cá nhân Ra Nước ngoài ("**Hồ sơ Chuyển Dữ liệu**") theo mẫu quy định. Hồ sơ này phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của BCA;
- (b) Nộp 01 bản chính Hồ sơ Chuyển Dữ liệu cho Cục An ninh Mạng trong thời hạn 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân để Cục An ninh Mạng đánh giá và có thể yêu cầu hoàn thiện nếu phát hiện hồ sơ nói trên chưa đầy đủ và không đúng quy định;
- (c) Thông báo bằng văn bản cho Cục An ninh Mạng 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; và
- (d) Cập nhật, bổ sung hồ sơ Chuyển Dữ liệu khi có sự thay đổi về nội dung hồ sơ đã gửi cho Cục An ninh Mạng trong thời hạn 10 ngày kể từ ngày yêu cầu.

**9. Cử nhân viên bảo vệ dữ liệu**

Các bên xử lý dữ liệu cá nhân nhạy cảm phải chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân, chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân và trao đổi thông tin về bộ phận và cá nhân phụ trách bảo vệ dữ liệu cá nhân với Cục An ninh Mạng. Trường hợp bên xử lý dữ liệu là cá nhân thì trao đổi thông tin của cá nhân thực hiện.

**10. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân**

Nghị định 13 chỉ định Cục An ninh Mạng là Cơ quan chuyên trách về bảo vệ dữ liệu cá nhân, có trách nhiệm giúp BCA thực hiện quản lý Nhà nước về bảo vệ dữ liệu trên phạm vi toàn quốc tại Việt Nam.