**Principles on Processing of Personal Data under the new Decree 13/2023/ND-CP**

**Introduction**

On 17 April 2023, after a thorough drafting and revising procedure, the Government had promulgated the first-ever Decree No. 13/2023/ND-CP on Personal Data Protection (“**PDPD**”), with the aim to provide a comprehensive and uniform approach to personal data safeguards in Vietnam. As the PDPD encompasses mostly on the requirements applicable to businesses involving in the personal data processing activities, we shall take a closer look at its key implications for this particular subject.

1. **Parties involved in processing Personal Data**

Under the PDPD, there are 05 groups[[1]](#footnote-1) of parties involved in the processing of personal data, accordingly:

1. Data Subject: Refers to an individual to whom the data relates;
2. Personal Data Controller: Refers to an organization or individual that decides purposes and means of processing personal data (“**Data Controller**”);
3. Personal Data Processor: Refers to an organization or individual that processes data on behalf of the Personal Data Controller via a contract or agreement (“**Data Processor**”);
4. Personal Data Controller-Processor: Refers to an organization or individual that performs both the Controller and Processor roles, jointly decides purposes and directly processes personal data; and,
5. Third Party: Refers to an organization or individual other than the aforementioned parties, and is permitted to process personal data.

In general, exclusive of the Data Subject, the PDPD imposes equal applicable organizational and technical measures to each of the latter four regulated parties to ensure the security and integrity of the personal data, as such parties can be held liable for any damages resulted from the processing. Notwithstanding, the responsibilities of the Data Controller and the Data Processor (and correspondingly, the Data Controller-Processor) are governed under a more stringent and specified manner.

In regards to the abovementioned measures, the Data Controller is obligated to have those reviewed and updated periodically. It is also required to record a log of processing activities, and only working with Data Processor that has implemented appropriate security measures[[2]](#footnote-2). On the other hand, Data Processor must have a contract with the Data Controller before receiving and processing any personal data. After completing the processing, Data Processor shall have to delete and return all data to the Data Controller[[3]](#footnote-3). It is crucial for businesses to understand and identify their roles, to fully comply with the regulations.

1. **Principles of processing Personal Data**

The PDPD outlines eight principles[[4]](#footnote-4) for businesses to conduct activities in compliance. These principles are in much compatibility with the principles listed under the EU’s General Data Protection Regulation No. 2016/679 (“**GDPR**”), namely:

1. Lawfulness: The personal data shall be processed as prescribed by law;
2. Transparency: The Data Subject must be informed of the processing activities;
3. Purpose Limitation: The personal data shall be processed only for the purposes registered and declared by the processing-involved parties;
4. Data Minimization: The collected personal data shall be appropriate for the scope and purposes of processing;
5. Accuracy: The personal data shall be updated and supplemented for the processing purposes;
6. Integrity and Confidentiality: The personal data shall be protected and secured during the processing against any violations or damages;
7. Storage Limitation: The personal data shall be stored only for a period appropriate with the processing purposes; and
8. Accountability: The Data Controller and Data Controller-Processor must comply with the above principles and demonstrate their compliance.

Regarding the “Data Minimization” principle, the PDPD explicitly introduces the additional principle on prohibition of sale or purchase of personal data under any manner.

1. **Consent of the Data Subject**

Consent of the Data Subject is the most crucial basis and will be applied in all activities of data processing. The consent by a Data Subject will be valid only when[[5]](#footnote-5):

1. The consent is voluntarily given, without being forced or deceived; and,
2. Be made based on the Data Subject’s full understanding of: the type of personal data to be processed; the purpose of the personal data processing; the entities permitted to process personal data; and the Data Subject’s rights and obligations.

The consent must be expressed clearly and specifically in written instrument, by voice, by ticking the consent box, by text message, by selecting consent technical settings, or via other forms applicable[[6]](#footnote-6). The PDPD further stipulates that such forms of consent must be able to be printed, copied in writing, either in electronic or verifiable format[[7]](#footnote-7).

Furthermore, consent for data use must be bound to a single purpose[[8]](#footnote-8). In case of processing the data for multiple purposes, the Data Controller and Data Processor must list out all purposes so that the Data Subject can acknowledge and decide whether to give consent to the stated purposes. Additionally, the Data Subject may provide a partial or conditional consent[[9]](#footnote-9).

It must be noted that the Data Subject's silence or lack of response does not constitute a consent[[10]](#footnote-10).

1. **Processing Personal Data in special cases**
2. Processing Personal Data without consent

Regardless of Section III above, the PDPD also specifies several special cases in which the processing of personal data without consent is permissible, in order to ensure the public interests or to serve the activities of state agencies. Such circumstances are prescribed under Article 17 of the PDPD, when serving the purposes of protecting the life and health of the Data Subject or others; or processing by competent regulatory authorities in the event of a state of emergency regarding national defense, security, social order and safety.

In addition, personal data acquired from audio and video recording activities in public places by the competent agencies and organizations can also be processed[[11]](#footnote-11). However, these instruments shall only be made for the protection of the national security, social order and safety, legitimate rights and interests in accordance with the law. For clarification, if a video or audio is recorded for other purposes, then the Data Subject’s consent is still required before processing. The Data Subject is informed of the recording of such audios and videos.

1. Processing Personal Data of special Data Subjects

In regards to the processing of personal data of persons declared missing or dead, a consent of that person’s family members (e.g., his/her spouse, adult children or parents) must be obtained[[12]](#footnote-12). In the case such person has no family member, it is considered as no consent is given and therefore, the processing could not be carried out.

In regards to the processing of children’s personal data, for children of 7 years old or older, any parties involved in data processing must obtain the consent of both the child and their parents or guardian[[13]](#footnote-13); while for children under 7 years old, it seems that only the consent of their parents or guardian is required. Therefore, it is critical for any processing-involved party to confirm the age of the children prior to conducting any processing activities.

1. Processing Personal Data in marketing and advertising services

Entities that provide marketing and advertising services may only use customers’ personal data collected through their business activities to provide marketing and advertising services with the consent of the Data Subject on the basis that the Data Subject be notified of content, method, form and frequency of marketing and advertising activities provided to them[[14]](#footnote-14).

**Conclusion**

Under the PDPD, the Government has addressed many of the current challenges facing personal data protection in Vietnam. However, the absence of a specific procedure, for example to handle violation complaints remains a concern, which leads to the anticipation that the Government will issue a decree on the enforcement of the regulations. In the interim, businesses are encouraged to cautiously approach and act in compliance with the PDPD.

**ADK VIETNAM LAWYERS**

**Nguyên tắc xử lý Dữ liệu Cá nhân theo Nghị định 13/2023/NĐ-CP**

**Giới thiệu**

Qua quá trình soạn thảo, cân nhắc và sửa đổi kỹ lưỡng, Chính phủ đã ban hành Nghị định đầu tiên về Bảo vệ Dữ liệu Cá nhân số 13/2023/NĐ-CP vào ngày 17 tháng 4 năm 2023 (“**Nghị định 13**”), nhằm mục đích tạo ra khung pháp lý tiếp cận vấn đề bảo vệ dữ liệu cá nhân một cách toàn diện và thống nhất ở Việt Nam. Do nội dung của Nghị định 13 phần lớn quy định về các nguyên tắc áp dụng cho doanh nghiệp liên quan đến hoạt động xử lý dữ liệu cá nhân, bài viết này sẽ cung cấp một cách chi tiết hơn những tác động chính của Nghị định đối với chủ thể doanh nghiệp.

1. **Các chủ thể liên quan tới xử lý Dữ liệu Cá nhân**

Nghị định 13 điều chỉnh 05 chủ thể[[15]](#footnote-15) liên quan tới xử lý dữ liệu cá nhân, tương ứng như sau:

1. Chủ thể Dữ liệu: Là cá nhân được dữ liệu cá nhân phản ánh;
2. Bên Kiểm soát dữ liệu cá nhân: Là tổ chức hoặc cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân (“**Bên Kiểm soát dữ liệu**”);
3. Bên Xử lý dữ liệu cá nhân: Là tổ chức hoặc 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**”);
4. Bên Kiểm soát và xử lý dữ liệu cá nhân: Là tổ chức hoặc cá nhân đồng thời quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân; và,
5. Bên thứ ba: Là tổ chức hoặc cá nhân ngoài các chủ thể nói trên và được phép xử lý dữ liệu cá nhân.

Nhìn chung, ngoại trừ Chủ thể Dữ liệu, Nghị định 13 yêu cầu mỗi bên thuộc bốn chủ thể xử lý dữ liệu cá nhân phải thực hiện biện pháp tổ chức và kỹ thuật cùng các biện pháp an toàn để bảo đảm tính bảo mật và tính toàn vẹn của dữ liệu cá nhân, trên cơ sở các chủ thể phải chịu trách nhiệm pháp lý trước Chủ thể Dữ liệu về mọi thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra. Tuy nhiên, trách nhiệm của Bên kiểm soát dữ liệu và Bên Xử lý dữ liệu (và, tương ứng với hai bên nêu trên, Bên Kiểm soát và xử lý dữ liệu cá nhân) được quy định chi tiết và nghiêm ngặt hơn.

Liên quan đến các biện pháp tổ chức, kỹ thuật và an toàn nêu trên, Bên kiểm soát dữ liệu có nghĩa vụ phải rà soát và cập nhật các biện pháp này tùy từng thời điểm khi cần thiết. Đồng thời, phải ghi lại và lưu trữ nhật ký hệ thống quá trình xử lý dữ liệu cá nhân, và chỉ làm việc với Bên Xử lý dữ liệu có các biện pháp bảo vệ phù hợp theo yêu cầu và quy định pháp luật hiện hành[[16]](#footnote-16). Mặt khác, Bên xử lý dữ liệu phải ký kết hợp đồng với Bên kiểm soát dữ liệu trước khi tiếp nhận và xử lý bất kỳ dữ liệu cá nhân nào. Sau khi kết thúc quá trình xử lý, Bên xử lý dữ liệu phải xóa và trả lại toàn bộ dữ liệu cho Bên kiểm soát dữ liệu[[17]](#footnote-17). Yêu cầu đặt ra cho các doanh nghiệp theo Nghị định 13 là phải hiểu và xác định được vai trò của mình trong quá trình xử lý dữ liệu cá nhân để tuân thủ đầy đủ các quy định pháp luật liên quan.

1. **Nguyên tắc xử lý Dữ liệu Cá nhân**

Nghị định 13 đặt ra 08 nguyên tắc[[18]](#footnote-18) để các doanh nghiệp tuân thủ trong quá trình xử lý dữ liệu. Về cơ bản, các nguyên tắc này tương thích với các nguyên tắc được liệt kê trong Quy định bảo vệ dữ liệu chung số 2016/679 của Liên minh Châu Âu (“**Quy định 2016/679**”). Cụ thể:

1. Tính hợp pháp: Dữ liệu cá nhân được xử lý theo quy định của pháp luật;
2. Tính minh bạch: Chủ thể Dữ liệu phải được thông báo và biết về các hoạt động xử lý;
3. Giới hạn mục đích sử dụng: Dữ liệu cá nhân chỉ được xử lý cho các mục đích đã được đăng ký và tuyên bố bởi các bên liên quan đến việc xử lý dữ liệu;
4. Giảm thiểu dữ liệu: Dữ liệu cá nhân được thu thập phải phù hợp với phạm vi và mục đích xử lý;
5. Tính chính xác: Dữ liệu cá nhân phải được cập nhật, bổ sung phù hợp cho mục đích xử lý;
6. Tính toàn vẹn và bảo mật: Dữ liệu cá nhân sẽ được bảo vệ và bảo mật trong quá trình xử lý khỏi mọi vi phạm hoặc thiệt hại;
7. Giới hạn lưu trữ: Dữ liệu cá nhân sẽ chỉ được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý; Và
8. Trách nhiệm giải trình: Bên kiểm soát dữ liệu và Bên xử lý và kiểm soát dữ liệu cá nhân phải tuân thủ các nguyên tắc trên và chứng minh sự tuân thủ các nguyên tắc.

Đối với nguyên tắc “Giảm thiểu dữ liệu”, Nghị định 13 đồng thời đưa vào một nguyên tắc bổ sung về cấm mua, bán dữ liệu cá nhân dưới bất kỳ hình thức nào.

1. **Sự đồng ý của Chủ thể Dữ liệu**

Sự đồng ý của Chủ thể Dữ liệu là cơ sở quan trọng nhất và được áp dụng đối với mọi hoạt động xử lý dữ liệu. Sự đồng ý của Chủ thể dữ liệu sẽ chỉ có hiệu lực khi[[19]](#footnote-19):

1. Sự đồng ý được đưa ra một cách tự nguyện, không bị ép buộc hoặc lừa dối; và,
2. Được đưa ra dựa trên sự hiểu biết đầy đủ của Chủ thể Dữ liệu về các nội dung: loại dữ liệu cá nhân sẽ được xử lý; mục đích xử lý dữ liệu cá nhân; các chủ thể được phép xử lý dữ liệu cá nhân; và các quyền và nghĩa vụ của Chủ thể Dữ liệu.

Sự đồng ý phải được thể hiện rõ ràng và cụ thể bằng văn bản, bằng giọng nói, bằng cách đánh dấu vào ô đồng ý, bằng tin nhắn văn bản, bằng cách chọn các thiết lập kỹ thuật đồng ý hoặc thông qua các hình thức khác có thể thể hiện được sự đồng ý[[20]](#footnote-20). Nghị định 13 cũng quy định rằng các hình thức đồng ý phải ở định dạng có thể in, sao chép được bằng văn bản, bao gồm định dạng điện tử hoặc định dạng có thể kiểm chứng được[[21]](#footnote-21).

Bên cạnh đó, sự đồng ý sử dụng dữ liệu phải được ràng buộc với một mục đích duy nhất[[22]](#footnote-22). Trong trường hợp dữ liệu được xử lý cho nhiều mục đích, Bên kiểm soát dữ liệu và Bên xử lý dữ liệu phải liệt kê tất cả các mục đích để Chủ thể Dữ liệu có thể xem xét, xác nhận và quyết định đồng ý với các mục đích đã nêu. Chủ thể Dữ liệu có thể đồng ý một phần hoặc đưa ra điều kiện kèm theo[[23]](#footnote-23).

Cần lưu ý rằng việc Chủ thể Dữ liệu im lặng hoặc không phản hồi không cấu thành sự đồng ý[[24]](#footnote-24).

1. **Xử lý Dữ liệu Cá nhân trong một số trường hợp đặc biệt**
2. Xử lý Dữ liệu Cá nhân không có sự đồng ý

Bất kể Mục III nêu trên đưa ra yêu cầu về sự đồng ý của Chủ thể Dữ liệu, Nghị định 13 quy định một số trường hợp đặc biệt được phép xử lý dữ liệu cá nhân mà không có sự đồng ý để bảo đảm lợi ích công cộng hoặc phục vụ hoạt động của các cơ quan Nhà nước. Những trường hợp như vậy được quy định tại Điều 17 của Nghị định, khi phục vụ mục đích bảo vệ tính mạng và sức khỏe của Chủ thể Dữ liệu hoặc cá nhân khác; hoặc được cơ quan Nhà nước có thẩm quyền xử lý trong trường hợp xảy ra tình trạng khẩn cấp về quốc phòng, an ninh, trật tự, an toàn xã hội.

Ngoài ra, dữ liệu cá nhân thu thập được từ hoạt động ghi âm, ghi hình ở nơi công cộng của các cơ quan, tổ chức có thẩm quyền cũng có thể được xử lý mà không có sự đồng ý của Chủ thể Dữ liệu[[25]](#footnote-25). Tuy nhiên, những công cụ này chỉ được ghi lại vì mục đích bảo vệ an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp theo quy định của pháp luật. Để làm rõ, nếu video hoặc âm thanh được ghi lại vì các mục đích khác thì các chủ thể xử lý vẫn cần có sự đồng ý của Chủ thể Dữ liệu trước khi tiến hành hoạt động xử lý. Chủ thể Dữ liệu phải được thông báo về việc ghi âm, ghi hình đó.

1. Xử lý Dữ liệu Cá nhân của các chủ thể dữ liệu đặc biệt

Liên quan đến việc xử lý dữ liệu cá nhân của những người bị tuyên bố mất tích hoặc đã chết, phải có sự đồng ý của các thành viên gia đình của người đó (ví dụ: vợ/chồng, con cái đã thành niên hoặc cha mẹ của người đó)[[26]](#footnote-26) trước khi thực hiện hoạt động xử lý dữ liệu. Trong trường hợp người đó không có thành viên gia đình thì coi như không có sự đồng ý và do đó, không thể xử lý dữ liệu cá nhân của người đó.

Liên quan đến việc xử lý dữ liệu cá nhân của trẻ em, đối với trẻ em từ 7 tuổi trở lên, bất kỳ chủ thể nào tham gia xử lý dữ liệu đều phải có được sự đồng ý của cả trẻ em và cha mẹ hoặc người giám hộ của trẻ em[[27]](#footnote-27); trong khi đối với trẻ em dưới 7 tuổi, dường như chỉ cần có sự đồng ý của cha mẹ hoặc người giám hộ. Do đó, cần phải xác nhận độ tuổi của Chủ thể Dữ liệu là trẻ em trước khi tiến hành bất kỳ hoạt động xử lý nào, để có được sự đồng ý phù hợp và đầy đủ theo luật định.

1. Xử lý Dữ liệu Cá nhân trong kinh doanh dịch vụ tiếp thị và quảng cáo

Các chủ thể kinh doanh dịch vụ tiếp thị và quảng cáo chỉ có thể sử dụng dữ liệu cá nhân của khách hàng được thu thập thông qua hoạt động kinh doanh của mình để cung cấp dịch vụ tiếp thị và quảng cáo với sự đồng ý của Chủ thể Dữ liệu, trên cơ sở Chủ thể Dữ liệu được thông báo về nội dung, phương pháp, hình thức và tần suất thực hiện các hoạt động tiếp thị và quảng cáo[[28]](#footnote-28).

**Kết luận**

Nghị định 13 đã tạo ra khung pháp lý giúp Chính phủ giải quyết những thách thức hiện nay đối với việc bảo vệ dữ liệu cá nhân ở Việt Nam. Tuy nhiên, Nghị định chưa hướng dẫn thủ tục cụ thể áp dụng, ví dụ như giải quyết khiếu nại vi phạm việc bảo vệ dữ liệu cá nhân - một vấn đề đáng lo ngại trong hoạt động xử lý dữ liệu. Một nghị định hướng dẫn thi hành Nghị định 13 được dự đoán sẽ được xây dựng và ban hành trong thời gian tới, để thực hiện nghiêm ngặt và có hiệu quả hoạt động bảo vệ dữ liệu cá nhân. Trong giai đoạn hiện tại, các doanh nghiệp cần thận trọng khi thu thập và xử lý dữ liệu cá nhân, và hành động tuân thủ theo nghĩa vụ và trách nhiệm quy định trong Nghị định.

**ADK VIETNAM LAWYERS**

1. Article 2.6, 2.9, 2.10, 2.11, 2.12 of the Decree No. 13/2023/ND-CP on Personal Data Protection (PDPD). [↑](#footnote-ref-1)
2. Article 38 of the PDPD. [↑](#footnote-ref-2)
3. Article 39 of the PDPD. [↑](#footnote-ref-3)
4. Article 3 of the PDPD. [↑](#footnote-ref-4)
5. Article 11.2 of the PDPD. [↑](#footnote-ref-5)
6. Article 11.3 of the PDPD. [↑](#footnote-ref-6)
7. Article 11.5 of the PDPD. [↑](#footnote-ref-7)
8. Article 11.4 of the PDPD. [↑](#footnote-ref-8)
9. Article 11.7 of the PDPD. [↑](#footnote-ref-9)
10. Article 11.6 of the PDPD. [↑](#footnote-ref-10)
11. Article 18 of the PDPD. [↑](#footnote-ref-11)
12. Article 19 of the PDPD. [↑](#footnote-ref-12)
13. Article 20 of the PDPD. [↑](#footnote-ref-13)
14. Article 21 of the PDPD. [↑](#footnote-ref-14)
15. Điều 2.6, 2.9, 2.10, 2.11, 2.12 Nghị định số 13/2023/ND-CP về bảo vệ dữ liệu cá nhân (“**Nghị định 13**”). [↑](#footnote-ref-15)
16. Điều 38 Nghị định 13. [↑](#footnote-ref-16)
17. Điều 39 Nghị định 13. [↑](#footnote-ref-17)
18. Điều 3 Nghị định 13. [↑](#footnote-ref-18)
19. Điều 11.2 Nghị định 13. [↑](#footnote-ref-19)
20. Điều 11.3 Nghị định 13. [↑](#footnote-ref-20)
21. Điều 11.5 Nghị định 13. [↑](#footnote-ref-21)
22. Điều 11.4 Nghị định 13. [↑](#footnote-ref-22)
23. Điều 11.7 Nghị định 13. [↑](#footnote-ref-23)
24. Điều 11.6 Nghị định 13. [↑](#footnote-ref-24)
25. Điều 18 Nghị định 13. [↑](#footnote-ref-25)
26. Điều 19 Nghị định 13. [↑](#footnote-ref-26)
27. Điều 20 Nghị định 13. [↑](#footnote-ref-27)
28. Điều 21 Nghị định 13. [↑](#footnote-ref-28)