

HERMAN, HENRY & DOMINIC (EZLAW), thuộc hiệp hội luật sư quốc tế LAWYERS ASSOCIATED WORLDWIDE, là một đội ngũ giàu kinh nghiệm gồm các luật sư và chuyên gia pháp lý làm việc tại Sài Gòn và Hà Nội. Với phương châm “Local Expertise & Global Standard”, chúng tôi cung cấp đầy đủ dịch vụ cho các công ty và nhà đầu tư trong và ngoài nước, tại nhiều lĩnh vực khác nhau. Tìm hiểu thêm về chúng tôi tại: <https://ezlawfirm.org/>

Ngày: 29 tháng 6 năm 2023

Người nhận: Quý Khách hàng, Đồng nghiệp, và những Người quan tâm

**TRÍCH YẾU: TÓM TẮT NGHỊ ĐỊNH SỐ 13/2023/NĐ-CP VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN**

Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (“**Nghị Định 13**”) sẽ có hiệu lực thi hành kể từ ngày 01/07/2023, và được áp dụng cho các cơ quan, tổ chức, cá nhân trong và ngoài nước liên quan đến việc xử lý dữ liệu cá nhân tại Việt Nam.

Trong quá trình xây dựng và soạn thảo Nghị Định 13, các nhà làm luật đã tham khảo các tiêu chuẩn và quy định quốc tế về quyền riêng tư và bảo vệ thông tin và dữ liệu cá nhân, ví dụ như Công ước của Hội đồng châu Âu về bảo vệ cá nhân liên quan đến tự động xử lý thông tin và dữ liệu cá nhân, Hướng dẫn của Liên hợp quốc về các tệp thông tin và dữ liệu cá nhân được vi tính hóa, Luật của Tổ chức các quốc gia Hoa Kỳ về bảo vệ thông tin và dữ liệu cá nhân, và Quy định bảo vệ dữ liệu chung của châu Âu.

Mặt khác, Nghị Định 13 có một số nội dung khác biệt so với các tiêu chuẩn, quy định trên. Những chính sách và hoạt động của các công ty có hoạt động tại Việt Nam, cho dù phù hợp với một hoặc một số tiêu chuẩn, quy định quốc tế, sẽ không mặc định là phù hợp với Nghị Định 13.

Do đó, các công ty trong và ngoài nước có hoạt động liên quan đến việc xử lý dữ liệu cá nhân tại Việt Nam cần lập tức nghiên cứu và triển khai thực hiện các công việc cần thiết để tuân thủ Nghị Định 13.

Tại Bài viết này<sup>1</sup>, chúng tôi sẽ:

- (i) tóm tắt một số nội dung quan trọng của Nghị Định 13, kèm theo khuyến nghị cho các công ty có hoạt động xử lý dữ liệu cá nhân tại Việt Nam; và
- (ii) đưa ra các lưu ý và đánh giá liên quan đến một số nội dung cần chú ý hoặc cần được hướng dẫn cụ thể hơn tại Nghị Định 13.

[Xem tiếp trang sau]

<sup>1</sup> Lưu ý: Bài viết này chỉ mang tính chất tham khảo và không phải là lời khuyên pháp lý cụ thể. Các thông tin được cung cấp trong Bài viết này không bao gồm mọi nội dung, khía cạnh của Nghị Định 13 và pháp luật liên quan. Bài viết này không được dùng để thay thế cho việc tư vấn pháp lý chính thức từ một luật sư chuyên nghiệp.

## I. MỘT SỐ NỘI DUNG QUAN TRỌNG CỦA NGHỊ ĐỊNH 13

Vấn đề	Nội dung Nghị Định 13	Khuyến nghị
<p>Khái niệm dữ liệu cá nhân</p>	<p>"<i>Dữ liệu cá nhân</i>" là các 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 đó dữ liệu cá nhân được phân chia thành dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.<sup>2</sup></p> <p>"<i>Dữ liệu cá nhân cơ bản</i>" bao gồm: thông tin định danh (ví dụ: họ tên, quốc tịch, hình ảnh cá nhân, giới tính, số định danh cá nhân...), cookies, lịch sử duyệt web, và thông tin khác gắn liền với một con người hoặc giúp xác định một người cụ thể.<sup>3</sup></p> <p>"<i>Dữ liệu cá nhân nhạy cảm</i>" bao gồm: quan điểm chính trị, tôn giáo, tình trạng sức khỏe và đời tư (trừ nhóm máu), chủng tộc, dữ liệu di truyền, xu hướng tình dục, dữ liệu về tội phạm, dữ liệu khách hàng của tổ chức tín dụng, dịch vụ trung gian thanh toán, dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị và các dữ liệu cá nhân nhạy cảm khác.<sup>4</sup></p>	<p>Khuyến nghị việc phân loại các loại dữ liệu cá nhân để xây dựng biện pháp bảo vệ phù hợp.</p> <p>Doanh nghiệp và/hoặc các bên có liên quan tới xử lý dữ liệu cá nhân phải áp dụng các biện pháp quản lý, kỹ thuật để bảo vệ dữ liệu cá nhân.<sup>5</sup> Đối với dữ liệu cá nhân nhạy cảm, các chủ thể này phải chỉ định nhân sự/bộ phận bảo vệ dữ liệu cá nhân và thông tin đến cơ quan nhà nước chuyên trách.<sup>6</sup> Ngoài ra, chủ thể dữ liệu phải được thông báo rằng dữ liệu cần xử lý là dữ liệu cá nhân nhạy cảm.<sup>7</sup> Việc thông báo này chỉ được miễn trừ trong một số trường hợp nhất định, ví dụ khi chủ thể dữ liệu đã biết và đồng ý trước, khi cần công khai dữ liệu theo luật định, khi cơ quan nhà nước xử lý dữ liệu phục vụ hoạt động của mình hoặc vì lý do an ninh.<sup>8</sup></p>
<p>Khái niệm xử lý dữ liệu cá nhân</p>	<p>"<i>Xử lý dữ liệu cá nhân</i>" là một hoặc nhiều hoạt động tác động tới dữ liệu cá nhân. Các hoạt động này có thể là thu thập, ghi, phân tích, xác nhận, lưu trữ, chỉnh sửa, công khai, kết hợp, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, cung cấp, chuyển giao, xóa, hủy dữ liệu.<sup>9</sup></p> <p>Hoạt động xử lý dữ liệu cá nhân được thực hiện bằng phương tiện điện tử nhằm đánh giá, phân tích, dự đoán hoạt động của một con người cụ thể là xử lý dữ liệu tự động,<sup>10</sup> và cũng phải tuân thủ các quy định về xử lý dữ liệu theo Nghị Định 13.</p>	<p>Khuyến nghị việc kiểm tra, rà soát và cập nhật các chính sách nội bộ, các điều khoản chung với người tiêu dùng để bảo đảm tuân thủ quy định về xử lý dữ liệu cá nhân tại Nghị Định 13.</p>

<sup>2</sup> Điều 2.1 của Nghị Định 13.

<sup>3</sup> Điều 2.3 của Nghị Định 13.

<sup>4</sup> Điều 2.4 của Nghị Định 13.

<sup>5</sup> Điều 26 của Nghị Định 13.

<sup>6</sup> Điều 28.2 của Nghị Định 13.

<sup>7</sup> Điều 11.8 và 28.3 của Nghị Định 13

<sup>8</sup> Điều 28.3 của Nghị Định 13.

<sup>9</sup> Điều 2.7 của Nghị Định 13.

<sup>10</sup> Điều 2.13 của Nghị Định 13.

Vấn đề	Nội dung Nghị Định 13	Khuyến nghị
<p>Khái niệm về các bên có vai trò trong việc xử lý dữ liệu cá nhân</p>	<p>"<i>Bên kiểm soát dữ liệu cá nhân</i>" là tổ chức hoặc cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân.<sup>11</sup> (sau đây gọi là "<b>Bên kiểm soát</b>")</p> <p>"<i>Bên xử lý dữ liệu cá nhân</i>" 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.<sup>12</sup> (sau đây gọi là "<b>Bên xử lý</b>")</p> <p>"<i>Bên kiểm soát và xử lý dữ liệu cá nhân</i>" là tổ chức, cá nhân đồng thời quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân, có trách nhiệm của cả hai chủ thể trên.<sup>13</sup> (sau đây gọi là "<b>Bên kiểm soát và xử lý</b>")</p> <p>"<i>Bên thứ ba</i>" là tổ chức hoặc cá nhân không là chủ thể dữ liệu, đồng thời không thuộc các chủ thể nêu trên nhưng được phép xử lý dữ liệu cá nhân.<sup>14</sup></p>	<p>Khuyến nghị việc đánh giá lại trách nhiệm tuân thủ của từng bên có vai trò trong việc xử lý dữ liệu cá nhân theo Nghị Định 13 và phân chia trách nhiệm cho từng bên liên quan.</p>
<p>Quyền của chủ thể dữ liệu</p>	<p>Chủ thể dữ liệu có các quyền:<sup>15</sup> (i) quyền được biết; (ii) quyền đồng ý; (iii) quyền truy cập; (iv) quyền rút lại sự đồng ý; (v) quyền xóa dữ liệu; (vi) quyền hạn chế xử lý dữ liệu; (vii) quyền cung cấp dữ liệu; (viii) quyền phản đối xử lý dữ liệu; (ix) quyền khiếu nại, tố cáo, khởi kiện; (x) quyền yêu cầu bồi thường thiệt hại; và (xi) quyền tự bảo vệ.</p> <p>Bên kiểm soát /bên kiểm soát và xử lý phải bảo đảm các quyền của chủ thể dữ liệu.<sup>16</sup> Mọi yêu cầu của chủ thể dữ liệu, bao gồm hạn chế, phản đối xử lý dữ liệu, cung cấp dữ liệu, chỉnh sửa dữ liệu và xóa dữ liệu, phải được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu.<sup>17</sup></p>	<p>Khuyến nghị việc kiểm tra, rà soát và cập nhật các chính sách nội bộ, các điều khoản chung với người tiêu dùng để bảo đảm quyền yêu cầu của người dùng và phản ứng kịp thời với yêu cầu đó.</p>
<p>Sự đồng ý của chủ thể dữ liệu</p>	<p>Bên kiểm soát/bên kiểm soát và xử lý phải có sự đồng ý của chủ thể dữ liệu để được xử lý dữ liệu cá nhân và có trách nhiệm chứng minh dữ liệu được xử lý hợp pháp trong trường hợp có tranh chấp.<sup>18</sup></p> <p>Sự đồng ý của chủ thể dữ liệu chỉ có hiệu lực khi:</p> <p>(a) Chủ thể dữ liệu tự nguyện và biết rõ thông tin về việc xử lý dữ liệu;<sup>19</sup></p>	<p>Khuyến nghị việc kiểm tra, rà soát và cập nhật các chính sách nội bộ, các điều khoản chung với người tiêu dùng để bảo đảm tuân thủ quy định về thể thức chấp thuận của chủ thể dữ liệu theo Nghị Định 13.</p>

<sup>11</sup> Điều 2.9 của Nghị Định 13.

<sup>12</sup> Điều 2.10 của Nghị Định 13.

<sup>13</sup> Điều 2.11 và Điều 40 của Nghị Định 13.

<sup>14</sup> Điều 2.12 của Nghị Định 13.

<sup>15</sup> Điều 9 của Nghị Định 13.

<sup>16</sup> Điều 38.5 và Điều 40 của Nghị Định 13.

<sup>17</sup> Điều 9.6, 9.8, 14.3, 15.2 và 16.5 của Nghị Định 13.

<sup>18</sup> Điều 3.8, 9.2 và 11.1 và 11.10 của Nghị Định 13.

<sup>19</sup> Điều 11.2 của Nghị Định 13.

Vấn đề	Nội dung Nghị Định 13	Khuyến nghị
	<p>(b) Thể thức của sự đồng ý được 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 sao cho chủ thể dữ liệu có thể đồng ý với một phần hoặc có điều kiện kèm theo.<sup>20</sup> Nếu có nhiều mục đích xử lý dữ liệu, chủ thể dữ liệu có thể chọn đồng ý toàn bộ hoặc một phần;<sup>21</sup></p> <p>(c) Sự đồng ý của chủ thể dữ liệu phải 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.<sup>22</sup></p> <p>Lưu ý rằng việc im lặng hoặc không phản hồi sẽ không được xem là sự đồng ý.<sup>23</sup> Cá nhân có quyền rút lại sự đồng ý và trong trường hợp đó, sự đồng ý trước đây xem như là hết hiệu lực.<sup>24</sup></p> <p>Lưu ý việc xử lý dữ liệu trong các trường hợp đặc biệt:</p> <p>(a) Việc xử lý dữ liệu cá nhân của trẻ em phải có sự đồng ý của trẻ em trong trường hợp trẻ em từ đủ 7 tuổi trở lên và có sự đồng ý của cha, mẹ hoặc người giám hộ. Bên kiểm soát/bên xử lý/bên kiểm soát và xử lý/bên thứ ba phải xác minh tuổi của trẻ em trước khi xử lý dữ liệu;<sup>25</sup> và</p> <p>(b) Việc xử lý dữ liệu cá nhân liên quan đến dữ liệu cá nhân của người bị tuyên bố mất tích, người đã chết phải được sự đồng ý của cha, mẹ, vợ, chồng hoặc con thành niên của người đó. Trường hợp không có tất cả những người này thì được coi là không có sự đồng ý.<sup>26</sup></p>	<p>Đồng thời, nên xây dựng cách thức thu thập chấp thuận của chủ thể dữ liệu và bên liên quan trong trường hợp đặc biệt.</p>

<sup>20</sup> Điều 11.3 và 11.7 của Nghị Định 13.

<sup>21</sup> Điều 11.4 của Nghị Định 13.

<sup>22</sup> Điều 11.5 của Nghị Định 13.

<sup>23</sup> Điều 11.6 của Nghị Định 13.

<sup>24</sup> Điều 11.9 và Điều 12 của Nghị Định 13.

<sup>25</sup> Điều 20.2 của Nghị Định 13.

<sup>26</sup> Điều 19 của Nghị Định 13.

Vấn đề	Nội dung Nghị Định 13	Khuyến nghị
Xử lý dữ liệu cá nhân không cần chấp thuận	<p>Việc xử lý dữ liệu cá nhân mà không cần phải có sự đồng ý của chủ thể dữ liệu trong trường hợp:</p> <ul style="list-style-type: none"> <li>(a) để bảo vệ tính mạng, sức khỏe của chủ thể dữ liệu hoặc người khác;<sup>27</sup></li> <li>(b) công khai dữ liệu cá nhân theo quy định của luật;<sup>28</sup></li> <li>(c) thực hiện nghĩa vụ theo hợp đồng cả chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của luật;<sup>29</sup></li> <li>(d) cơ quan nhà nước có thẩm quyền xử lý dữ liệu khi (i) có tình trạng khẩn cấp, (ii) có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức độ ban bố tình trạng khẩn cấp, (iii) phòng, chống tội phạm; hoặc (iv) nhằm phục vụ hoạt động của cơ quan nhà nước đã được quy định theo luật chuyên ngành;<sup>30</sup> hoặc</li> <li>(e) ghi âm, ghi hình và xử lý dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng bởi cơ quan, tổ chức có thẩm quyền nhằm bảo vệ an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân theo quy định của pháp luật.<sup>31</sup> Chủ thể dữ liệu sẽ được thông báo trước khi cơ quan, tổ chức có thẩm quyền thực hiện các hành vi này.</li> </ul>	Khuyến nghị việc kiểm tra, rà soát và cập nhật các chính sách nội bộ, các điều khoản chung với người tiêu dùng để bảo đảm tuân thủ quy định về các trường hợp xử lý dữ liệu cá nhân không cần có sự đồng ý của chủ thể dữ liệu.
Thông báo xử lý dữ liệu cá nhân	<p>Chủ thể dữ liệu phải được thông báo trước khi xử lý dữ liệu.<sup>32</sup> Nội dung thông báo cần bao gồm loại dữ liệu đầu vào, mục đích và cách thức xử lý, thông tin của các bên kiểm soát và/hoặc xử lý liên quan, rủi ro tiềm ẩn trong quá trình xử lý và thời gian xử lý.<sup>33</sup></p> <p>Tuy nhiên, bên kiểm soát/bên kiểm soát và xử lý không cần thông báo nếu chủ thể dữ liệu đã biết rõ và đồng ý với các nội dung trên trước khi cho bên kiểm soát/bên kiểm soát và xử lý tiến hành thu thập dữ liệu cá nhân.<sup>34</sup></p>	<p>Khuyến nghị việc thiết lập, sửa đổi, cập nhật thông báo xử lý dữ liệu trong trường hợp sự đồng ý ban đầu của chủ thể dữ liệu chưa có các nội dung được yêu cầu trong Nghị Định 13.</p> <p>Đồng thời, rà soát và cập nhật các chính sách liên quan đến thông báo xử lý dữ liệu cá nhân theo yêu cầu của Nghị Định 13.</p>

<sup>27</sup> Điều 17.1 của Nghị Định 13.

<sup>28</sup> Điều 17.2 của Nghị Định 13.

<sup>29</sup> Điều 17.4 của Nghị Định 13.

<sup>30</sup> Điều 17.3 của Nghị Định 13.

<sup>31</sup> Điều 18 của Nghị Định 13.

<sup>32</sup> Điều 13.1 của Nghị Định 13.

<sup>33</sup> Điều 13.2 của Nghị Định 13.

<sup>34</sup> Điều 13.4(a) của Nghị Định 13.

Vấn đề	Nội dung Nghị Định 13	Khuyến nghị
Cung cấp dữ liệu cá nhân	<p>Chủ thể dữ liệu có quyền yêu cầu bên kiểm soát/bên kiểm soát và xử lý cung cấp cho bản thân dữ liệu cá nhân của mình.<sup>35</sup></p> <p>Nhìn chung, bên kiểm soát/bên kiểm soát và xử lý chỉ được cung cấp dữ liệu cá nhân cho bên khác theo chấp thuận hoặc ủy quyền của chủ thể dữ liệu.<sup>36</sup></p> <p>Bên kiểm soát/bên kiểm soát và xử lý không được cung cấp dữ liệu cá nhân nếu (i) gây tổn hại tới quốc phòng, an ninh quốc gia, trật tự; (ii) có thể ảnh hưởng tới sự an toàn, sức khỏe thể chất hoặc tinh thần của người khác; hoặc (iii) không có sự đồng ý của chủ sở hữu dữ liệu.<sup>37</sup></p> <p>Việc yêu cầu cung cấp dữ liệu cá nhân được thực hiện thông qua phiếu yêu cầu theo mẫu.<sup>38</sup> Bên kiểm soát/bên kiểm soát và xử lý phải thông báo việc không thể cung cấp dữ liệu cá nhân và/hoặc hướng dẫn cho chủ thể yêu cầu đến cơ quan có thẩm quyền khi dữ liệu cá nhân không thuộc thẩm quyền của mình.<sup>39</sup></p>	Khuyến nghị việc kiểm tra, rà soát và cập nhật các chính sách nội bộ, các điều khoản chung với người tiêu dùng để bảo đảm tuân thủ quy định về cung cấp dữ liệu cá nhân tại Nghị Định 13.
Lưu trữ, xóa, hủy dữ liệu cá nhân	<p>Dữ liệu cá nhân chỉ được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý dữ liệu và phải có biện pháp bảo vệ phù hợp.<sup>40</sup></p> <p>Bên kiểm soát/bên kiểm soát và xử lý xóa dữ liệu cá nhân đối với trường hợp:<sup>41</sup></p> <p>(a) theo yêu cầu của chủ thể dữ liệu khi chủ thể dữ liệu (i) nhận thấy không còn cần thiết cho mục đích thu thập đã đồng ý; (ii) rút lại sự đồng ý; (iii) phản đối việc xử lý dữ liệu và bên kiểm soát/bên kiểm soát và xử lý không có lý do chính đáng để tiếp tục xử lý; (iv) nhận thấy dữ liệu cá nhân được xử lý không đúng với mục đích đã đồng ý hoặc việc xử lý dữ liệu cá nhân là vi phạm quy định của pháp luật; hoặc (v) nhận thấy dữ liệu cá nhân phải xóa theo quy định của pháp luật.</p> <p>(b) không cần có yêu cầu của chủ thể dữ liệu khi (i) xử lý dữ liệu không đúng mục đích hoặc đã hoàn thành mục đích; (ii) việc lưu trữ dữ liệu cá nhân không còn</p>	Khuyến nghị việc kiểm tra, rà soát và cập nhật các chính sách nội bộ, các điều khoản chung với người tiêu dùng để bảo đảm tuân thủ quy định về lưu trữ, xóa, hủy dữ liệu cá nhân tại Nghị Định 13.

<sup>35</sup> Điều 14.1 của Nghị Định 13.

<sup>36</sup> Điều 14.2 của Nghị Định 13.

<sup>37</sup> Điều 14.4 của Nghị Định 13.

<sup>38</sup> Điều 14.5 của Nghị Định 13.

<sup>39</sup> Điều 14.8(b) của Nghị Định 13.

<sup>40</sup> Điều 3.7 và Điều 16.6 của Nghị Định 13.

<sup>41</sup> Điều 16.1, Điều 16.7 và Điều 20.3 của Nghị Định 13.

Vấn đề	Nội dung Nghị Định 13	Khuyến nghị
	<p>cần thiết; (iii) bên kiểm soát/bên xử lý/bên kiểm soát và xử lý/bên thứ ba xử lý dữ liệu bị giải thể/không còn hoạt động/tuyên bố phá sản/bị chấm dứt hoạt động kinh doanh; (iv) cha, mẹ hoặc người giám hộ của chủ thể dữ liệu là trẻ em rút lại sự đồng ý cho phép xử lý dữ liệu; (v) theo yêu cầu của cơ quan chức năng có thẩm quyền khi việc xử lý dữ liệu gây ảnh hưởng tới quyền và lợi ích hợp pháp của trẻ em.</p> <p>Bên kiểm soát/bên kiểm soát và xử lý không xóa dữ liệu cá nhân khi (a) pháp luật không cho phép xóa dữ liệu; (b) dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền; (c) dữ liệu cá nhân đã được công khai; (d) dữ liệu cá nhân được xử lý nhằm phục vụ yêu cầu pháp lý, nghiên cứu khoa học, thống kê; (e) trường hợp tình trạng khẩn cấp hoặc khi có nguy cơ đe dọa an ninh, quốc phòng, phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật theo quy định của luật; (f) ứng phó với tình huống khẩn cấp đe dọa đến tính mạng, sức khỏe hoặc sự an toàn của chủ thể dữ liệu hoặc cá nhân khác.<sup>42</sup></p>	
<p>Bảo vệ dữ liệu cá nhân trong tiếp thị, quảng cáo</p>	<p>Về nguyên tắc, Nghị Định 13 quy định chủ thể dữ liệu có quyền phản đối mọi hoạt động xử lý dữ liệu cá nhân, bao gồm cả việc xử lý dữ liệu cho mục đích quảng cáo, tiếp thị.<sup>43</sup></p> <p>Tổ chức/cá nhân kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo phải tuân thủ và có trách nhiệm chứng minh tuân thủ các quy định sau:<sup>44</sup></p> <p>(a) Chỉ sử dụng dữ liệu cá nhân của khách hàng được thu thập qua hoạt động kinh doanh của mình; và</p> <p>(b) 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 giới thiệu sản phẩm.</p>	<p>Khuyến nghị việc kiểm tra, rà soát và cập nhật các chính sách nội bộ, các điều khoản chung với người tiêu dùng để bảo đảm tuân thủ quy định xử lý dữ liệu cá nhân cho mục đích tiếp thị, quảng cáo tại Nghị Định 13.</p>
<p>Đánh giá tác động xử lý dữ liệu cá nhân</p>	<p>Kể từ khi tiến hành xử lý dữ liệu cá nhân, bên kiểm soát /bên kiểm soát và xử lý phải lập và lưu giữ hồ sơ đánh giá tác động xử lý dữ liệu cá nhân. Hồ sơ gốc phải được nộp cho Cục An ninh mạng và Phòng chống Tội phạm Công nghệ cao trong vòng 60 ngày kể từ ngày xử lý dữ liệu cá nhân. Đồng thời, bên kiểm soát/bên kiểm soát và xử lý</p>	<p>Khuyến nghị việc cập nhật các quy trình về lập, nộp và lưu trữ hồ sơ đánh giá tác động xử lý dữ liệu theo quy định tại Nghị Định 13.</p>

<sup>42</sup> Điều 16.2 của Nghị Định 13.

<sup>43</sup> Điều 21.1 của Nghị Định 13.

<sup>44</sup> Điều 21 của Nghị Định 13.

Vấn đề	Nội dung Nghị Định 13	Khuyến nghị
	<p>cũng phải lưu một bộ hồ sơ để Bộ Công an kiểm tra và đánh giá bất kỳ lúc nào.<sup>45</sup></p> <p>Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của bên kiểm soát/bên kiểm soát và xử lý/bên xử lý có một số khác biệt nhỏ, nhưng nhìn chung cần chứa các thông tin như chi tiết liên lạc của bên kiểm soát/bên xử lý, mục đích của việc xử lý dữ liệu cá nhân, loại dữ liệu cá nhân được xử lý, bên nhận dữ liệu cá nhân (bao gồm tổ chức và cá nhân ngoài Việt Nam), thời gian xử lý dữ liệu, thời gian dự kiến để xóa dữ liệu cá nhân, biện pháp được áp dụng để bảo vệ dữ liệu cá nhân và đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu cá nhân.<sup>46</sup></p>	
Chuyển dữ liệu ra nước ngoài	<p>Dữ liệu cá nhân của công dân Việt Nam chỉ có thể được chuyển ra nước ngoài nếu bên chuyển dữ liệu thực hiện đánh giá tác động chuyển dữ liệu ra nước ngoài và tuân thủ các thủ tục luật định.<sup>47</sup></p> <p>Hồ sơ đánh giá tác động phải bao gồm, nhưng không chỉ giới hạn ở một số thông tin như: các bên liên quan, loại dữ liệu được chuyển, biện pháp được áp dụng để bảo vệ dữ liệu và hậu quả tiềm năng của việc chuyển dữ liệu.<sup>48</sup></p> <p>Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an, và một bản chính phải được gửi đến Bộ Công an trong vòng 60 ngày kể từ ngày xử lý dữ liệu.<sup>49</sup> Ngoài ra, bên chuyển dữ liệu phải thông báo cho Bộ Công an bằng văn bản kèm theo một số thông tin sau khi chuyển dữ liệu thành công.<sup>50</sup></p> <p>Bộ Công an có thể yêu cầu bên chuyển dữ liệu dừng việc chuyển dữ liệu ra nước ngoài nếu phát hiện việc chuyển giao này vi phạm an ninh quốc gia hoặc gây rò rỉ dữ liệu, hoặc nếu người chuyển dữ liệu vi phạm nghĩa vụ báo cáo của mình.<sup>51</sup></p>	Khuyến nghị việc cập nhật các quy trình về lập, nộp và lưu trữ hồ sơ đánh giá tác động chuyển dữ liệu ra nước ngoài theo quy định tại Nghị Định 13.

<sup>45</sup> Điều 24.1 và Điều 24.4 của Nghị Định 13.

<sup>46</sup> Điều 24.1 và Điều 24.2 của Nghị Định 13.

<sup>47</sup> Điều 25.1 của Nghị Định 13.

<sup>48</sup> Điều 25.3 của Nghị Định 13.

<sup>49</sup> Điều 25.3 của Nghị Định 13.

<sup>50</sup> Điều 25.4 của Nghị Định 13.

<sup>51</sup> Điều 25.8 của Nghị Định 13.



<b>Vấn đề</b>	<b>Nội dung Nghị Định 13</b>	<b>Khuyến nghị</b>
Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân	Trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân, bên kiểm soát/bên kiểm soát và xử lý thông báo bằng văn bản theo mẫu của Nghị Định 13 cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc chậm nhất 72 giờ sau khi xảy ra hành vi vi phạm. Trường hợp thông báo sau 72 giờ thì phải kèm theo lý do thông báo chậm, muộn. <sup>52</sup>	Khuyến nghị việc rà soát các quy trình nội bộ để bảo đảm phản ứng kịp thời khi xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân.
Nhân sự phụ trách bảo vệ dữ liệu cá nhân	Nghị Định 13 yêu cầu tất cả cơ quan, tổ chức, doanh nghiệp đều phải chỉ định nhân sự/bộ phận phụ trách bảo vệ dữ liệu, bắt đầu từ 1/7/2023. <sup>53</sup> Doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ và vừa, công ty khởi nghiệp không trực tiếp tham gia xử lý dữ liệu cá nhân có thể lựa chọn miễn trừ quy định này trong vòng 2 năm kể từ khi thành lập. <sup>54</sup>	Khuyến nghị việc bổ nhiệm nhân sự/chỉ định bộ phận phụ trách bảo vệ dữ liệu cá nhân. Đồng thời, xây dựng mô tả công việc cho vị trí này và cập nhật, bổ sung các quy trình nội bộ liên quan.

## II. MỘT SỐ LƯU Ý VÀ ĐÁNH GIÁ

### 1. Các thông tin và mô hình được xây dựng từ các dữ liệu cá nhân có phải là dữ liệu cá nhân?

Theo quy định tại Nghị Định 13, dữ liệu cá nhân bao gồm thông tin gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể (ví dụ như họ tên, ngày sinh, giới tính, quốc tịch, hình ảnh, lịch sử hoạt động không gian mạng, v.v...). Hiện tại, có nhiều quan điểm khác nhau đối với câu hỏi các thông tin hoặc mô hình tổng hợp về con người (bao gồm cả hành vi con người) có được coi là dữ liệu cá nhân hay không nếu chính chúng được tạo lập từ các dữ liệu cá nhân. Có quan điểm cho rằng các thông tin hoặc mô hình này không được coi là dữ liệu cá nhân, bởi lẽ chúng không phải là thông tin về một con người cụ thể, mà được sử dụng cho các mục đích như tổng hợp thông tin hoặc đánh giá, phán đoán hành vi của bất kỳ người nào trong một nhóm người. Mặt khác, cũng có quan điểm đối lập cho rằng các thông tin và mô hình này là chính là dữ liệu cá nhân bởi chúng được tạo nên từ các thông tin khác gắn liền với từng cá nhân con người.

Nghị Định 13 là một văn bản quy phạm pháp luật mới của Việt Nam, và do đó, chúng ta chưa thể biết rõ quan điểm chính thức của cơ quan nhà nước về vấn đề này. Trong trường hợp cơ quan nhà nước coi rằng các thông tin và mô hình tổng hợp được tạo lập từ các dữ liệu cá nhân Việt Nam cũng chính là dữ liệu cá nhân, các công ty có hoạt động tại Việt Nam cũng phải thông báo và xin chấp thuận của chủ thể dữ liệu khi sử dụng các thông tin và mô hình tổng hợp đó.

### 2. Im lặng không có nghĩa là đồng ý

Chính sách bảo mật (Privacy Policy) được ban hành bởi các công ty cho khách hàng thông thường bao gồm các quy định về việc khách hàng chấp thuận công ty có quyền lưu trữ và xử lý dữ liệu cá nhân của khách hàng. Trên thị trường hiện nay, có một số công ty quy định rằng việc khách hàng

<sup>52</sup> Điều 23.1 của Nghị Định 13.

<sup>53</sup> Điều Điều 28.2, 30 và 43.1 của Nghị Định 13.

<sup>54</sup> Điều 43.2 của Nghị Định 13.

sử dụng dịch vụ, sản phẩm của họ đồng nghĩa với việc khách hàng đồng ý với Chính sách bảo mật của các công ty này. Tuy nhiên, cách thức này sẽ không còn phù hợp với Nghị Định 13.

Theo quy định tại Nghị Định 13, việc xử lý dữ liệu cá nhân phải có sự đồng ý của chủ thể dữ liệu và sự đồng ý này phải được thể hiện bởi các cách thức chủ động (ví dụ như 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). Nghị Định 13 còn quy định rõ ràng rằng việc im lặng hoặc không phản hồi sẽ không được xem là sự đồng ý.

### **3. Đồng ý phải được thể hiện ở một định dạng có thể được in và sao chép**

Nghị Định 13 quy định rằng sự đồng ý của chủ thể dữ liệu phải 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. Ngoài ra, khi có tranh chấp, bên kiểm soát và/hoặc xử lý dữ liệu phải chứng minh được sự đồng ý của chủ thể dữ liệu.

Hiện nay, chưa rõ rằng yêu cầu cụ thể của cơ quan nhà nước trong việc lưu trữ và chứng minh sự đồng ý của chủ thể dữ liệu là gì và thế nào là đủ? Ngoài ra, việc yêu cầu sự đồng ý phải được thể hiện ở định dạng có thể in và sao chép phải chẳng đã mâu thuẫn với chính quy định khác của Nghị Định 13 rằng sự đồng ý có thể được thể hiện bằng giọng nói?

### **4. Đồng ý chỉ có hiệu lực khi chủ thể đã hiểu rõ và được thông báo đầy đủ thông tin**

Theo quy định tại Nghị Định 13, kể cả khi khách hàng đã đồng ý với Chính sách bảo mật của công ty, điều đó chưa đương nhiên cho phép công ty xử lý dữ liệu cá nhân của khách hàng. Nghị Định 13 quy định rằng sự đồng ý chỉ có hiệu lực khi chủ thể dữ liệu đã được hiểu rõ về:

- (i) mục đích xử lý dữ liệu cá nhân;
- (ii) loại dữ liệu cá nhân được xử lý;
- (iii) tổ chức được xử lý dữ liệu cá nhân; và
- (iv) các quyền và nghĩa vụ của chủ thể dữ liệu.

Ngoài ra, trước khi xử lý dữ liệu cá nhân, bên kiểm soát và xử lý dữ liệu cũng phải thông báo thêm cho chủ thể dữ liệu về:

- (v) thông tin về các tổ chức, cá nhân có liên quan tới mục đích xử lý;
- (vi) hậu quả, thiệt hại không mong muốn có khả năng xảy ra; và
- (vii) thời gian bắt đầu, thời gian kết thúc xử lý dữ liệu.

Do đó, nếu Chính sách bảo mật và các thông báo của công ty không có đầy đủ 07 nội dung trên, sự đồng ý của chủ thể dữ liệu là không có giá trị hiệu lực.

### **5. Thông báo khái quát hay cụ thể mục đích xử lý dữ liệu cá nhân?**

Thông thường Chính sách bảo mật thông tin của các công ty chỉ quy định và liệt kê một cách khái quát về các mục đích xử lý dữ liệu cá nhân. Mặt khác, cần lưu ý rằng Nghị Định 13 quy định sự đồng ý của chủ thể dữ liệu chỉ có hiệu lực khi họ biết rõ về các nội dung quan trọng như đã đề cập tại mục trên, bao gồm nội dung về mục đích xử lý dữ liệu cá nhân. Do Nghị Định 13 là một văn

bản pháp luật mới, nên chưa thể biết rằng cơ quan nhà nước có đồng ý với việc liệt kê khái quát mục đích (ví dụ như nghiên cứu và phát triển) mà không cần phải nêu cụ thể mục đích (ví dụ như nghiên cứu và phát triển mô hình đánh giá và phán đoán hành vi, thói quen con người để chia sẻ với các đối tác) hay không.

## **6. Quyền được biết và quyền được lãng quên**

Ngoài quyền đồng ý, chủ thể dữ liệu cá nhân còn có quyền được biết (bao gồm quyền được biết về hoạt động xử lý dữ liệu cá nhân, quyền được truy cập để xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân, và quyền được yêu cầu cung cấp dữ liệu cá nhân của mình) và quyền được lãng quên (bao gồm quyền được xóa hoặc yêu cầu xóa dữ liệu cá nhân, quyền được yêu cầu hạn chế xử lý dữ liệu cá nhân, và quyền được ngăn chặn hoặc hạn chế tiết lộ dữ liệu cá nhân cho mục đích quảng cáo, tiếp thị).

## **7. Lưu trữ đám mây và chuyển dữ liệu ra nước ngoài**

Nghị Định 13 quy định rằng bên chuyển dữ liệu ra nước ngoài phải thực hiện đánh giá tác động chuyển dữ liệu ra nước ngoài và tuân thủ các thủ tục luật định. Cần lưu ý rằng quy định này sẽ ảnh hưởng đến một phần lớn các công ty đang có hoạt động xử lý dữ liệu cá nhân tại Việt Nam, kể cả là công ty trong nước. Bởi lẽ, một số lượng lớn các công ty trong nước hiện nay đang sử dụng dịch vụ điện toán đám mây (cloud computing) của các nhà cung cấp dịch vụ nước ngoài (ví dụ như Amazon, Google, hoặc Microsoft) để lưu trữ thông tin và dữ liệu, bao gồm dữ liệu cá nhân của khách hàng.

## **8. Nhân sự phụ trách bảo vệ dữ liệu cá nhân**

Nghị Định 13 yêu cầu tất cả cơ quan, tổ chức, doanh nghiệp liên quan đến hoạt động xử lý dữ liệu cá nhân đều phải chỉ định nhân sự/bộ phận phụ trách bảo vệ dữ liệu. Tuy nhiên, hiện chưa có hướng dẫn cụ thể liên quan đến phạm vi công việc, yêu cầu, tiêu chuẩn dành cho nhân sự phụ trách bảo vệ dữ liệu cá nhân; do đó, chúng ta sẽ cần chờ thêm hướng dẫn của cơ quan nhà nước về vấn đề này. Mặt khác, trong thời gian này, các công ty có thể tham khảo hướng dẫn của Liên minh Châu Âu liên quan đến các nhân sự phụ trách bảo vệ dữ liệu cá nhân (data protection officer) tại <https://gdpr.eu/data-protection-officer/>.

\* \* \* \* \*