Nghị định Bảo vệ dữ liệu cá nhân và một vài gợi ý triển khai

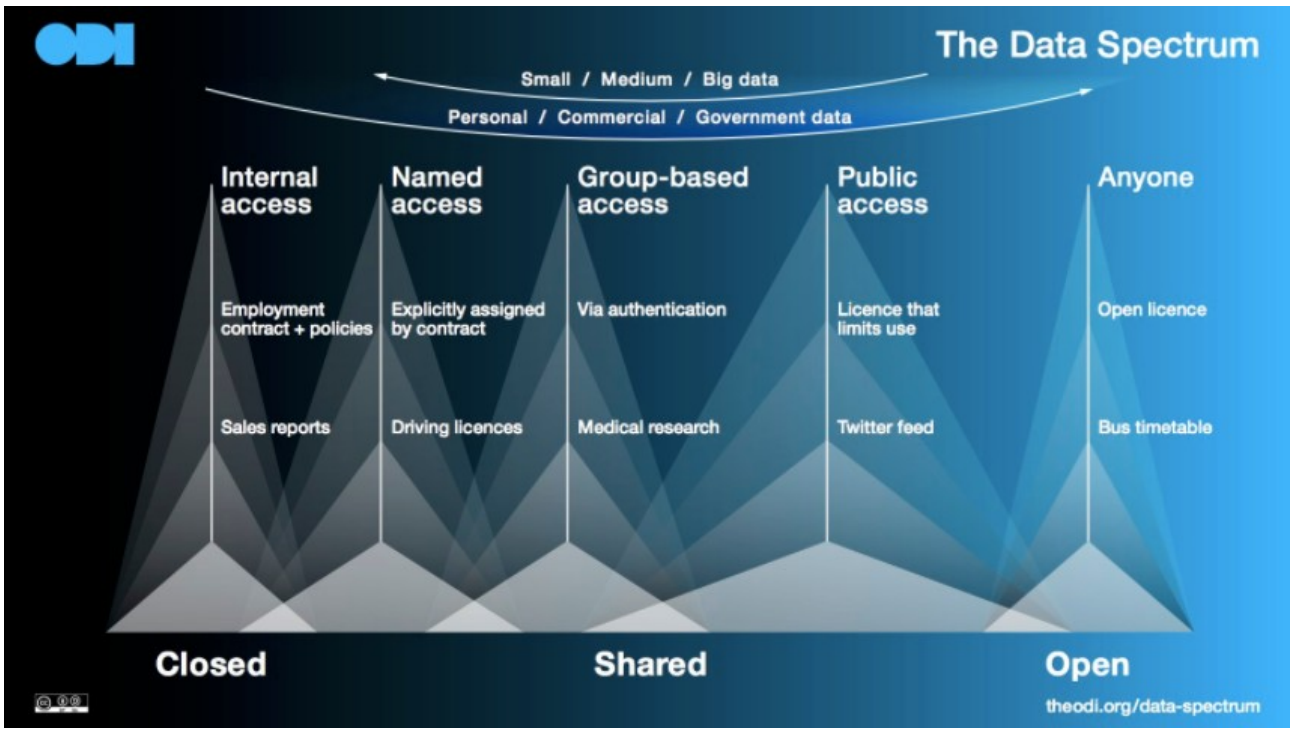
Ngày 17/04/2023, chính phủ đã ban hành Nghị định số 13/2023/NĐ-CP[1] về 'Bảo vệ dữ liệu cá nhân', có hiệu lực thi hành từ 01/07/2023. Đây là hành lang pháp lý quan trọng nhằm quy định chặt chẽ các nghĩa vụ bảo vệ dữ liệu đối với các hoạt động xử lý dữ liệu cá nhân trong không gian mạng tại Việt Nam.

Nhìn ra thế giới, việc bảo vệ dữ liệu cá nhân không là mới, nổi bật nhất trong số đó là 'Quy định bảo vệ dữ liệu chung' - GDPR[2] (General Data Protection Regulation) của Liên minh châu Âu ngày 27/04/2016, có hiệu lực đối với tất cả các quốc gia thành viên của Liên minh châu Âu và đã được áp dụng vào thực tế từ ngày 25/05/2018. Điều này gợi ý rằng Việt Nam, như người đi sau, có thể tham khảo và học hỏi được từ những kinh nghiệm của người đi trước, như Liên minh châu Âu, trong việc bảo vệ dữ liệu cá nhân.

Dù Nghị định 13/2023/NĐ-CP đã có hiệu lực từ 01/07/2023, nhưng việc triển khai vào thực tế cuộc sống các nội dung của Nghị định là không dễ cho tất cả các bên liên quan, bao gồm các bên: kiểm soát dữ liệu cá nhân; xử lý dữ liệu cá nhân; kiểm soát và xử lý dữ liệu cá nhân; bên thứ ba; và cả chủ thể dữ liệu; cùng với sự phức tạp của hệ thống các văn bản quy phạm pháp luật có liên quan tới bảo vệ dữ liệu cá nhân: theo thống kê của Bộ Công an, trước khi Nghị định số 13 được ban hành, Việt Nam có tổng cộng 68 văn bản quy phạm pháp luật liên quan trực tiếp đến bảo vệ dữ liệu cá nhân, trong đó có: Hiến pháp, 4 bộ luật, 39 luật, 1 pháp lệnh, 18 nghị định, 4 thông tư và thông tư liên tịch, 1 quyết định của Bộ trưởng. Tuy nhiên, tất cả đều chưa thống nhất về khái niệm và nội hàm dữ liệu cá nhân và bảo vệ dữ liệu cá nhân. Được biết, nhóm công tác ngân hàng nước ngoài (BWG) và đại diện Hiệp hội Ngân hàng Việt Nam (VNBA) kiến nghị một lộ trình phù hợp để có thể triển khai Nghị định 13/2023/NĐ-CP bảo vệ dữ liệu cá nhân với thời gian chuyển tiếp là 2 năm[3], đồng thời, Bộ công an và Ngân hàng Nhà nước đưa ra thông tư liên bộ để giải thích hoặc có thể vận dụng cho nghị định này.

A. Phổ dữ liệu

Để làm việc với dữ liệu nói chung, dữ liệu cá nhân nói riêng, bạn cần phải nắm được phổ dữ liệu[4]. Viện Dữ liệu Mở - ODI (Open Data Institute)[5], một tổ chức phi lợi nhuận với sứ mệnh làm việc với các công ty và chính phủ để xây dựng một hệ sinh thái dữ liệu mở, tin cậy, đã đưa ra khái niệm và hình minh họa phổ dữ liệu. Phổ dữ liệu giúp bạn hiểu được ngôn ngữ dữ liệu. Phổ dữ liệu trải từ dữ liệu đóng (Closed Data) sang dữ liệu chia sẻ (Shared Data) và sang dữ liệu mở (Open Data), như trên **Hình 1**.



Hình 1. Phổ dữ liệu

Cách thức dữ liệu được truy cập, được sử dụng và được chia sẻ hiện diện theo phổ dữ liệu này. Dữ liệu mà cần phải là riêng tư nên được giữ bí mật, nên là đóng (Closed). Dữ liệu nhạy cảm hoặc dữ liệu thương mại có thể được chia sẻ với vài người hoặc vài tổ chức (Shared). Dữ liệu mà có thể được mở nên là mở (Open).

B. Các nguyên tắc tính mở cho tổ chức kiểm soát và xử lý dữ liệu cá nhân

Lòng tin của các chủ thể dữ liệu vào các tổ chức kiểm soát và/hoặc xử lý dữ liệu cá nhân của họ là tối thượng trong vấn đề bảo vệ dữ liệu cá nhân. Tính mở về cách thức các tổ chức đang bảo vệ và quản lý các dữ liệu cá nhân xây dựng nên lòng tin. Nói cách khác, để có được lòng tin đó, thì các tổ chức kiểm soát và/hoặc xử lý dữ liệu cá nhân nên làm việc tuân theo **các nguyên tắc tính mở**, chúng bao gồm:

1. Mở với mọi người về dữ liệu cá nhân nào họ đang thu thập
2. Mở với mọi người về cách họ sử dụng dữ liệu cá nhân như thế nào
3. Mở với mọi người về cách thức dữ liệu cá nhân được chia sẻ
4. Mở với mọi người về cách thức dữ liệu cá nhân được bảo mật
5. Giải thích cho mọi người chúng ta ra các quyết định về họ như thế nào khi sử dụng dữ liệu của họ
6. Mở về các cơ chế trách nhiệm giải trình khi sử dụng sai dữ liệu cá nhân

7. Giúp mọi người hiểu và tác động đến cách dữ liệu của họ được thu thập và sử dụng như thế nào
8. Nếu thu thập hoặc sử dụng các dữ liệu cá nhân, hãy làm cho các phân tích và kết quả đầu ra của chúng càng mở càng tốt.

Mở về cách thức các dữ liệu cá nhân được sử dụng, và tính riêng tư được bảo vệ, giúp xây dựng lòng tin trong việc thu thập và sử dụng các dữ liệu cá nhân của các tổ chức. Lòng tin lớn hơn ngụ ý sự xung đột ít hơn khi phát triển các ý tưởng và các dịch vụ mới, và sử dụng nhiều hơn các ý tưởng và dịch vụ đang có. Nó giúp cho người tiêu dùng cảm thấy được trao quyền, và dẫn tới nhiều lựa chọn có đầy đủ thông tin hơn về các dịch vụ có liên quan tới thu thập các dữ liệu cá nhân. Tính mở làm cho mọi điều tốt hơn.

Các nguyên tắc về tính mở và quyền riêng tư của được thiết lập dành cho các tổ chức có mong muốn xây dựng lòng tin về cách thức họ quản lý các dữ liệu cá nhân. *Các nguyên tắc đó đặc biệt tập trung vào cách thức các tổ chức quản lý dữ liệu cá nhân, không tập trung vào dữ liệu chung mà họ thu thập và/hoặc sử dụng.* Các nguyên tắc đó có ý định sẽ áp dụng được rộng rãi cho các tổ chức trong các khu vực công, tư và bên thứ ba: các tổ chức bất kỳ kích cỡ nào đang thu thập, lưu trữ, sử dụng và/hoặc cung cấp truy cập tới các dữ liệu cá nhân.

Các nguyên tắc nêu trên không là vét cạn, dù các tổ chức nên cam kết với chúng và kết hợp chúng vào các chính sách và các quy trình của riêng mình.

Bảo vệ dữ liệu đôi khi được coi như là một gánh nặng tuân thủ. Tính mở về cách thức quyền riêng tư được bảo vệ sẽ xây dựng lòng tin, cung cấp cả những cải thiện về sự tuân thủ và dịch vụ. Các nguyên tắc đó khuyến khích các tổ chức cam kết sẽ là 'mở' theo một vài cách thức. *'Mở' ngụ ý cả việc chia sẻ thông tin (công khai trên trực tuyến và trực tiếp tới mọi người), và là mở để có phản hồi từ mọi người về cách thức mọi điều có thể được cải thiện.*

Lưu ý: đây là các nguyên tắc chỉ dẫn. Các tổ chức nên nhận thức được về các bổn phận bổ sung theo Nghị định 13/2023/NĐ-CP và các văn bản quy phạm pháp luật liên quan.

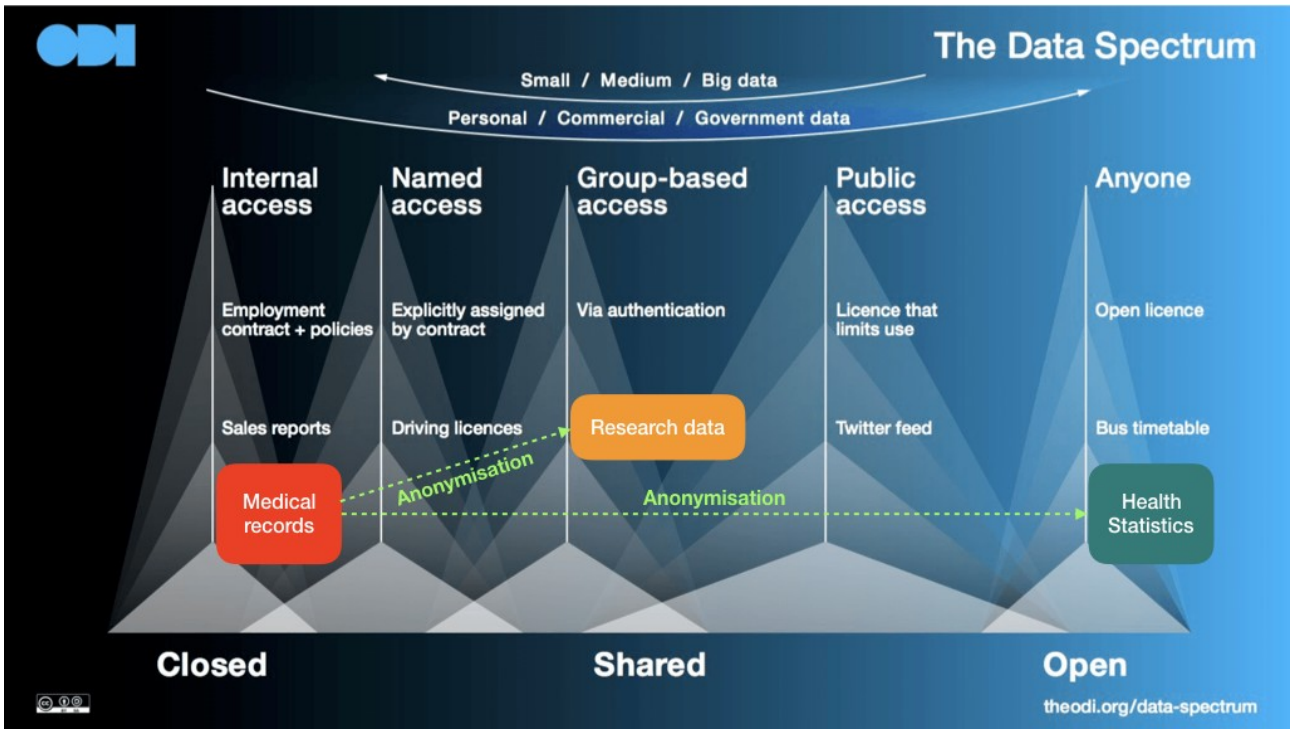
Chi tiết về các nguyên tắc tính mở cho các tổ chức xử lý dữ liệu cá nhân có thể xem trên trang web của ODI[6].

C. Ẩn danh (Anonymisation) - yếu tố xuyên suốt phổ dữ liệu

Ẩn danh (Anonymisation) là quy trình thay đổi tập hợp dữ liệu (dataset) để giảm nguy cơ nhận dạng lại nhiều nhất có thể.

Khi chi tiết hóa nguyên tắc cuối cùng trong số tám nguyên tắc tính mở ở trên, ODI đưa ra khuyến nghị rằng dữ liệu cá nhân tổng hợp được ẩn danh được các tổ chức đang tiến hành nghiên cứu sử dụng dữ liệu cá nhân và xây dựng hoặc cung cấp dịch vụ sử dụng dữ liệu cá nhân nên cung cấp lợi ích trở lại cho công chúng càng nhiều càng tốt để phản ánh giá trị mà họ cung cấp; bằng cách này, các tổ chức đóng góp trở lại cho cơ sở hạ tầng dữ liệu làm nền tảng cho các dịch vụ và kết quả đầu ra mà mọi người sử dụng hàng ngày, đồng thời giúp cơ sở hạ tầng đó tạo ra nhiều giá trị hơn cho xã hội.

Một ví dụ cụ thể được ODI đưa ra, là bằng việc sử dụng kỹ thuật ẩn danh dữ liệu hồ sơ y tế cá nhân, một trong những dữ liệu thuộc chủng loại '*Dữ liệu cá nhân nhạy cảm*' như được nêu trong Điều 2, khoản 4 của Nghị định 13/2023/NĐ-CP, để biến chúng từ dữ liệu đóng sang dữ liệu chia sẻ, và thậm chí sang dữ liệu mở mà bất kỳ ai cũng có quyền truy cập tới. Nói một cách khác, ẩn danh là yếu tố xuyên suốt phổ dữ liệu, như trên **Hình 2**.



Hình 2. Ẩn danh - yếu tố xuyên suốt phổ dữ liệu[7]

Ví dụ này cho thấy chúng ta có thể hình dung cách ẩn danh hồ sơ y tế sẽ tạo ra các dạng dữ liệu được sửa đổi có thể nằm ở những nơi khác nhau trong phổ dữ liệu – được chia sẻ và/hoặc được mở thay vì đóng như hồ sơ gốc ban đầu của nó. Điều này sẽ cho phép dữ liệu nghiên cứu được chia sẻ với các học giả thông qua các thỏa thuận chia sẻ dữ liệu và số liệu thống kê về sức khỏe sẽ được công bố công khai.

Một ví dụ khác, giả thiết một tổ chức tiến hành khảo sát tất cả các nhân viên của mình để thu thập dữ liệu về số buổi làm việc trên trực tuyến theo tuần nhằm tối ưu hóa chi phí văn phòng. Bây giờ, họ đang xem xét liệu có thể phát hành một phiên bản ẩn danh

kết quả khảo sát để có thể chia sẻ lợi ích cho các công ty khác hay không[8]. Tập hợp dữ liệu thô ban đầu (1) đã đi qua các bước kỹ thuật ẩn danh: (2) Thay 'Họ và tên' bằng mã số ID; (3) Thay 'ngày sinh' bằng độ tuổi; và (4) Hoán đổi 10% giá trị của các hàng - kết quả sau các bước ẩn danh đã làm khó hơn rất nhiều để nhận dạng lại các cá nhân.

Họ và tên	Ngày sinh	Số buổi làm việc trực tuyến trong tuần
Nguyễn Văn A	16/03/1969	5
Trần Thị H	02/12/1985	1
...	...	...
Phạm Thị T	26/05/2000	2

ID	Ngày sinh	Số buổi làm việc trực tuyến trong tuần
1	16/03/1969	5
2	02/12/1985	1
...	...	...
753	26/05/2000	2

1 2 3 4

ID	Độ tuổi đến tháng 2/2019	Số buổi làm việc trực tuyến trong tuần
1	40–50	5
2	30–40	1
...	...	...
753	10–20	2

ID	Độ tuổi đến tháng 2/2019	Số buổi làm việc trực tuyến trong tuần (hoán đổi 10% các hàng)
1	40–50	1
2	30–40	5
...	...	...
753	10–20	2

Hình 3. Ví dụ về ẩn danh một tập hợp dữ liệu qua từng bước

Trên thực tế, số lượng các kỹ thuật ẩn danh là không có giới hạn.

Có thể nói rằng, luôn luôn tồn tại khả năng dù lớn hay nhỏ, một kẻ tấn công có động lực lớn, kỹ năng cao, nhiều nguồn lực để tái nhận diện những dữ liệu ẩn danh. Bởi vậy, phần lớn các dữ liệu ẩn danh đều được quản trị và kiểm soát hết sức nghiêm ngặt. Tuy nhiên, vẫn có những ví dụ về dữ liệu ẩn danh vừa mở nhưng vừa duy trì được tính tiện ích đáng kể. Một trong số đó là dữ liệu thống kê.

Liên quan tới khía cạnh kỹ thuật và xây dựng hạ tầng dữ liệu nói chung, bao gồm dữ liệu cá nhân, Viện Dữ liệu Mở đã đưa vào Chiến lược của Viện các năm 2023-2028 nguyên tắc sau[9]:

> *"**Nguyên tắc 2**: Hạ tầng dữ liệu mạnh bao gồm dữ liệu khắp phổ dữ liệu, từ mở tới chia sẻ tới đóng. **Nhưng nền tảng tốt nhất có thể là dữ liệu mở**, được hỗ trợ và duy trì như là hạ tầng dữ liệu. Chỉ với nền tảng này, mọi người, các doanh*

nghiệp và chính phủ mới có thể nhận ra tiềm năng của hạ tầng dữ liệu trong toàn xã hội và nền kinh tế.”

Các tổ chức và doanh nghiệp có thể tham khảo và/hoặc tận dụng một số phần mềm nguồn mở đã được chứng minh tuân thủ với GDPR trong hạ tầng dữ liệu của mình để có thể hỗ trợ cho việc tuân thủ Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân như trên **Hình 4** và **Hình 5**.

PMNM	Magento	EspoCRM	SuiteCRM	Vtiger CRM	NextCloud
Giấy phép mở	OSL v3, AFLv3	GPLv3	AGPLv3	SUGARCRM PL v1.1.2	AGPLv3
PMNM	**OwnCloud**	**RocketChat**	**ERPNext**	**Axelor ERP**	**Dolibarr ERP/ CRM**
Giấy phép mở	AGPLv3	MIT	GPL	AGPLv3	GPLv3+
PMNM	**Matomo**	**OWA**	**GrandNode**	**0 A.D.**	**Wordpress**
Giấy phép mở	AGPLv3	MIT	GPLv3	GPLv2	GPLv2+
PMNM	**Zenario CMS**	**Jahia CMS**			
Giấy phép mở	BSD	GPLv3			

Hình 4. Có 17 dự án nguồn mở sẵn sàng với GDPR cho doanh nghiệp

PMNM	PostHog	Plausible	Countly	GoAccess	Matomo
Giấy phép mở	MIT	AGPLv3	AGPLv3	MIT	AGPLv3

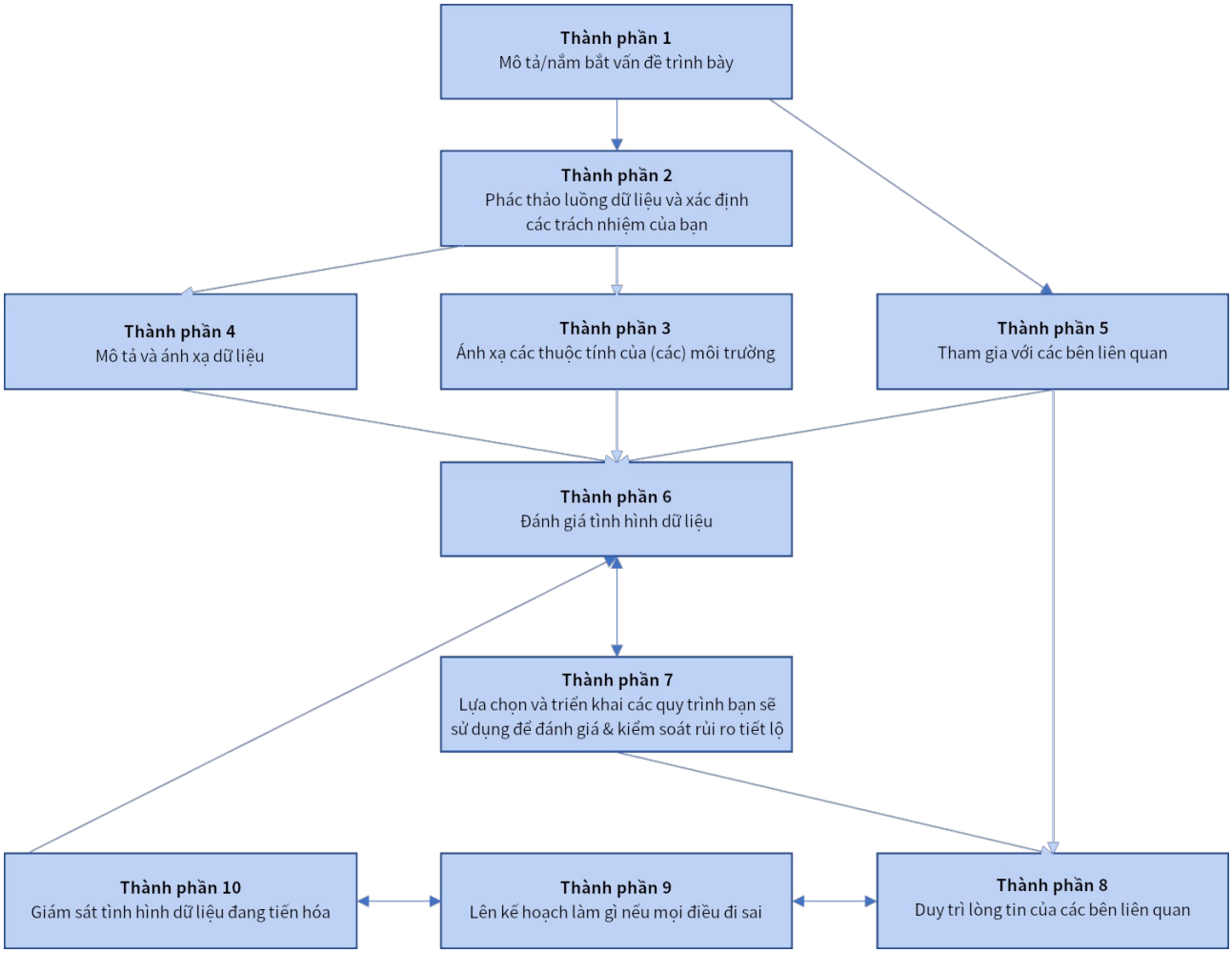
Hình 5. Có 5 công cụ phân tích tuân thủ với GDPR là PMNM

Chi tiết hơn về các phần mềm nguồn mở tuân thủ GDPR có trong bài viết ‘*Phần mềm nguồn mở: Trên đường bảo vệ dữ liệu cá nhân*’[10].

D. Khung ra quyết định ẩn danh - dành cho người thực hành bảo vệ dữ liệu cá nhân

Ẩn danh là một quy trình phức tạp, không chỉ phụ thuộc vào khía cạnh kỹ thuật công nghệ xung quanh dữ liệu cá nhân, mà còn cả môi trường và pháp luật có liên quan tới nó. Để giúp cho các tổ chức làm việc với dữ liệu cá nhân có thể chia sẻ được dữ liệu có nguồn gốc từ dữ liệu cá nhân nhưng vẫn đảm bảo tuân thủ Quy định Bảo vệ Dữ liệu Chung (GDPR), Vương quốc Anh đã ban hành Khung Ra quyết định Ẩn danh - ADF (Anonymisation Decision-making Framework) và hàng loạt các tài liệu hướng dẫn chi tiết khác đi kèm. Dưới đây trình bày vắn tắt Khung này.

Khung Ra quyết định Ẩn danh[11] *- ADF (Anonymisation Decision-making Framework) đưa ra cách thức suy nghĩ về ẩn danh và sử dụng lại dữ liệu cá nhân thoát ra khỏi các ràng buộc của các khuôn khổ quá kỹ thuật hoặc quá pháp lý của vấn đề. Quy định Bảo vệ Dữ liệu Chung - GDPR (General Data Protection Regulation) của Liên minh châu Âu từng luôn có ý định tạo thuận lợi cho việc chia sẻ và sử dụng lại dữ liệu đúng và phù hợp cũng như bảo vệ các chủ thể dữ liệu, và hoàn toàn có cách để dữ liệu vẫn hữu ích trong khi vẫn duy trì việc tuân thủ với GDPR, miễn là có một khung ra quyết định ẩn danh và một tập hợp các công cụ phù hợp.*



Hình 6. Khung ra quyết định ẩn danh (ADF) của chính phủ Vương quốc Anh

ADF (**Hình 6**) kết hợp hai khung hành động: một **khung kỹ thuật**, khung kia là **khung theo bối cảnh**. Yếu tố kỹ thuật của khung sẽ cho phép bạn suy nghĩ về cả việc định lượng rủi ro tiết lộ thông tin và cách quản lý nó. Yếu tố bối cảnh sẽ cho phép bạn suy nghĩ và giải quyết các yếu tố ảnh hưởng đến rủi ro đó.

Khung này được củng cố bởi một cách suy nghĩ tương đối mới về vấn đề nhận dạng lại, cho rằng bạn phải xem xét cả dữ liệu và bối cảnh của chúng để xác định các biện pháp rủi ro thực tế. Đây được gọi là ***cách tiếp cận tình huống dữ liệu***. Chính thức, một tình

huống dữ liệu là *tập hợp tổng hợp các mối quan hệ giữa một số dữ liệu và tập hợp các môi trường của chúng*.

Khung Ra quyết định Ẩn danh (ADF) được xây dựng dựa vào các nguyên tắc sau:

1. **Nguyên tắc toàn diện: Bạn không thể quyết định liệu dữ liệu có an toàn để chia sẻ/phát hành hay không chỉ bằng cách xem xét dữ liệu, nhưng bạn vẫn cần xem xét dữ liệu.** Nguyên tắc này gói gọn cách tiếp cận tình huống dữ liệu được nêu ở trên, trong đó rủi ro được coi là phát sinh từ sự tương tác giữa dữ liệu, con người và cấu trúc (mềm và cứng) định hình sự tương tác đó (chẳng hạn như chính sách quốc gia về chia sẻ và truy cập dữ liệu, khung pháp lý, hệ thống CNTT, thực tiễn quản trị, thái độ văn hóa đối với việc chia sẻ dữ liệu và quyền riêng tư, v.v.). Bạn cũng cần biết dữ liệu của mình – nghĩa là có thể xác định các thuộc tính quan trọng của dữ liệu và đánh giá chúng có thể ảnh hưởng đến rủi ro như thế nào. Điều này sẽ đưa vào các quyết định về lượng dữ liệu sẽ chia sẻ hoặc phát hành, với ai và như thế nào.
2. **Nguyên tắc tiện ích: Ẩn danh là một quá trình tạo ra dữ liệu an toàn nhưng nó chỉ có ý nghĩa nếu những gì bạn đang tạo ra là dữ liệu <u>hữu ích</u> an toàn.** *Bạn có thể thắc mắc tại sao chúng tôi nói về sự cần thiết phải cân bằng tiện ích dữ liệu với an toàn dữ liệu trong quy trình ẩn danh.* Rốt cuộc, thật dễ để nghĩ về việc ẩn danh chỉ trong điều kiện tạo ra dữ liệu an toàn, nhưng nếu làm vậy, nghịch lý thay, bạn có thể gặp rủi ro mà không có lợi ích thực sự (hoặc tệ hơn).
3. **Nguyên tắc rủi ro thực tế: Rủi ro bằng không không phải là khả năng thực tế nếu bạn muốn tạo ra dữ liệu hữu ích.** Đây là điều cơ bản. *Chức năng ẩn danh là về quản lý rủi ro, không hơn không kém; chấp nhận rằng có rủi ro còn lại trong tất cả các dữ liệu hữu ích chắc chắn sẽ đặt bạn vào lĩnh vực cân bằng giữa rủi ro và tiện ích.* Nhưng sự đánh đổi giữa lợi ích cá nhân và xã hội với rủi ro cá nhân và xã hội là nội dung của cuộc sống hiện đại. Điều này cũng tập trung vào vấn đề tham gia của các bên liên quan. Không có thỏa thuận nào về cách trò chuyện với các chủ thể dữ liệu và công chúng rộng rãi hơn về vấn đề này và có những lo ngại (không phải là không có cơ sở) về việc gây lo lắng không cần thiết bằng cách thu hút sự chú ý đến các rủi ro bảo mật. Đồng thời, cần phải công nhận rằng mọi người có khả năng cân bằng giữa rủi ro và lợi ích trong phần lớn cuộc sống hàng ngày của họ bất cứ khi nào họ sang đường, lái xe ô tô, v.v.
4. **Nguyên tắc tương xứng: Các biện pháp bạn đưa ra để quản lý rủi ro phải tỷ lệ thuận với rủi ro đó và tác động có thể xảy ra của nó.** *Theo nguyên tắc rủi ro*

thực tế, sự tồn tại của rủi ro không nhất thiết là lý do để từ chối quyền truy cập dữ liệu. Tuy nhiên, hiểu biết chín chắn về rủi ro đó sẽ cho phép bạn đưa ra quyết định tương xứng về dữ liệu, ai nên có quyền truy cập và trong những điều kiện nào. *Tuy nhiên, phổ biến dưới dạng dữ liệu ẩn danh mà vẫn là dữ liệu cá nhân là vi phạm Luật bảo vệ dữ liệu.*

Dựa vào 4 nguyên tắc trên, ADF xây dựng 10 thành phần, xoay quanh 3 hoạt động chính[12] gồm: (1) kiểm tra tình hình dữ liệu (các thành phần 1-6); (2) phân tích và kiểm soát rủi ro tiết lộ (thành phần 7); và (3) quản lý tác động (các thành phần 8-10).

Hình 7. Dữ liệu dịch chuyển qua nhiều môi trường

Ví dụ ở thành phần 2: Phác thảo dòng chảy dữ liệu và xác định các trách nhiệm của bạn. Ở đây bạn cần xác định các vấn đề sau:

- **Vai trò**: Bạn đang hành động theo chỉ đạo của tổ chức của mình hay tổ chức khác? Bạn là người kiểm soát dữ liệu, người xử lý hay người sử dụng dữ liệu?
- **Nguồn gốc dữ liệu**: Dữ liệu đã tới từ đâu, và chúng đang đi về đâu?
- **Phân loại và triển vọng dữ liệu**: Tình trạng dữ liệu là gì (dữ liệu cá nhân hay thông tin ẩn danh) đối với các bên liên quan trong dòng chảy dữ liệu đó?

Hình 7 là ví dụ dữ liệu dịch chuyển qua nhiều môi trường. Trong môi trường 1, Tổ chức A thu thập dữ liệu cá nhân và chia sẻ chúng với tổ chức B theo một hợp đồng dịch vụ dữ liệu, bao gồm điều khoản hợp đồng là Tổ chức B là người đồng kiểm soát bộ dữ liệu cá nhân đó. Trong môi trường 2, Tổ chức B tiến hành kỹ thuật ẩn danh để tạo ra một

tập con dữ liệu ẩn danh với mục đích sẽ chia sẻ nó với các nhà nghiên cứu được cấp quyền truy cập, rồi chia sẻ các dữ liệu ẩn danh đó cho Tổ chức C gồm các nhà nghiên cứu được cấp quyền truy cập các dữ liệu ẩn danh đó trong môi trường 3. Các nhà nghiên cứu sử dụng các dữ liệu cá nhân đã qua kỹ thuật ẩn danh trong môi trường 3 để nghiên cứu và phân tích rồi viết báo cáo và phát hành báo cáo cùng kết quả phân tích vào môi trường truy cập mở số 4, nơi bất kỳ ai cũng có thể truy cập tới báo cáo đó.

Ví dụ này cho thấy, Tổ chức A và Tổ chức B cùng là người kiểm soát dữ liệu cá nhân; Tổ chức B vừa là người kiểm soát, vừa là người xử lý dữ liệu cá nhân; các nhà nghiên cứu ở Tổ chức C là những người sử dụng và phân tích (xử lý) dữ liệu cá nhân đã qua ẩn danh; và cuối cùng, bất kỳ ai cũng có thể là người sử dụng các dữ liệu cá nhân là kết quả của cả kỹ thuật ẩn danh và quy trình phân tích của nhà nghiên cứu trong báo cáo kết quả nghiên cứu. **Ví dụ này cũng cho thấy, dữ liệu có thể chuyển từ đóng sang chia sẻ rồi sang mở khi trải qua các bước kỹ thuật ẩn danh đúng cách để trở thành dữ liệu hữu ích an toàn.**

Trong thực tế, dòng chảy của dữ liệu sẽ có trong vô số các kịch bản khác nhau, vì thế việc xác định vai trò của một tổ chức, nguồn gốc của dữ liệu và việc phân loại tình trạng dữ liệu không phải lúc nào cũng dễ dàng.

Chi tiết hơn về 10 thành phần của ADF có thể tham khảo bài viết '*Khung Ra quyết định Ẩn danh của Vương quốc Anh?*'[13] hoặc bản thân bản gốc tiếng Anh của tài liệu '*Khung ra quyết định ẩn danh ấn bản 2*'[12]. Ngoài ra, đi kèm với ADF còn có vài tài liệu và các mẫu hướng dẫn khác, có trên website Mạng Ẩn danh của Vương quốc Anh[14].

E. Kết luận và gợi ý

Để đáp ứng được nhu cầu của chủ thể dữ liệu và cũng là để đảm bảo các quyền của họ như được nêu trong Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, chẳng hạn như quyền '*được biết về hoạt động liên quan tới xử lý dữ liệu cá nhân của mình*' (Điều 3 khoản 2. Nguyên tắc bảo vệ dữ liệu cá nhân) như quyền được biết, quyền đồng ý, quyền truy cập, quyền rút lại sự đồng ý, quyền xóa dữ liệu, quyền hạn chế xử lý dữ liệu, quyền cung cấp dữ liệu, quyền phản đối xử lý dữ liệu, và các quyền khác (được ghi trong Điều 9. Quyền của chủ thể dữ liệu), có lẽ không có cách nào khác ngoài việc tất cả các bên liên quan tới dữ liệu cá nhân, bao gồm cả bên kiểm soát, bên xử lý, bên kiểm soát và xử lý, bên thứ ba cần áp dụng và tuân thủ tối thiểu 8 nguyên tắc tính mở được nêu ở phần trên, vì chỉ bằng cách đó họ mới có thể tạo được niềm tin của chủ thể dữ liệu vào những người nắm giữ và xử lý dữ liệu cá nhân của họ. Ngắn gọn '*Không mở, không tin!*'

Tất cả các bên liên quan tới việc bảo vệ dữ liệu cá nhân đều cần nắm được phổ dữ liệu và cần hiểu rằng dữ liệu cá nhân là có thể bảo vệ được và cùng lúc, có thể đi qua toàn bộ phổ dữ liệu, từ đóng sang chia sẻ sang mở nhờ có kỹ thuật ẩn danh đúng cách để trở thành dữ liệu hữu ích an toàn. Bổ sung thêm rằng, "Dữ liệu có thể hoặc hữu ích hoặc được ẩn danh tuyệt vời, nhưng không bao giờ có cả hai". Nói cách khác, một khi RỦI RO = 0 THÌ LỢI ÍCH CŨNG = 0.

Bảo vệ dữ liệu cá nhân không chỉ là về vấn đề kỹ thuật dữ liệu, mà còn là về vấn đề môi trường và pháp lý. Để điều này có thể xảy ra, có lẽ các cơ quan có thẩm quyền và các bên liên quan tới việc bảo vệ dữ liệu cá nhân cũng nên xem xét việc xây dựng một Khung ra quyết định ẩn danh dựa vào và/hoặc được tùy chỉnh từ 4 nguyên tắc cơ bản như của ADF của Vương quốc Anh, kết hợp hài hòa giữa khung kỹ thuật và khung theo bối cảnh, phù hợp với bối cảnh và pháp luật Việt Nam (như, Nghị định 13/2023/NĐ-CP) và cho Việt Nam. Gợi ý từ năm 2024 trở đi, các sự kiện Security Bootcamp (SBC) thường niên nên có phiên dành riêng cho vấn đề '*Bảo vệ dữ liệu cá nhân*' do tầm ảnh hưởng to lớn và sâu rộng của nó tới mọi mặt của đời sống xã hội và có liên quan chặt chẽ tới các nội dung của sự kiện SBC thường niên đã được tổ chức cho tới nay.

Cuối cùng, việc xây dựng hạ tầng dữ liệu mạnh là tối cần thiết, và theo nguyên tắc như ở trên đã nêu: "*Hạ tầng dữ liệu mạnh bao gồm dữ liệu khắp phổ dữ liệu, từ mở tới chia sẻ tới đóng.* ***Nhưng nền tảng tốt nhất có thể là dữ liệu mở****, được hỗ trợ và duy trì như là hạ tầng dữ liệu. Chỉ với nền tảng này, mọi người, các doanh nghiệp và chính phủ mới có thể nhận ra tiềm năng của hạ tầng dữ liệu trong toàn xã hội và nền kinh tế.*"" Ngoài ra, đã có rồi nhiều phần mềm nguồn mở sẵn sàng cho mục đích bảo vệ dữ liệu cá nhân mà các bên liên quan ở Việt Nam có thể tận dụng, chứ không nhất thiết phải 'làm lại cái bánh xe'.

Các chú giải

[1] Trang web của Chính phủ: *Nghị định số 13/2023/NĐ-CP của Chính phủ: Bảo vệ dữ liệu cá nhân*: https://vanban.chinhphu.vn/?pageid=27160&docid=207759

[2] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION: General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[3] VNEconomy: *Nghị định 13 về bảo vệ dữ liệu cá nhân: Các ngân hàng kiến nghị có thời gian chuyển tiếp khi thực hiện*: https://vneconomy.vn/nghi-dinh-13-ve-bao-ve-du-lieu-ca-nhan-cac-ngan-hang-kien-nghi-co-thoi-gian-chuyen-tiep-khi-thuc-hien.htm

[4] ODI: *The Data Spectrum*: https://theodi.org/about-the-odi/the-data-spectrum/

[5] ODI: *About the ODI*: https://www.theodi.org/about-the-odi/

[6] ODI (2016): *Openness principles for organisations handling personal data*: https://theodi.org/guides/openness-principles-for-organisations-handling-personal-data. Bản dịch sang tiếng Việt: https://vnfoss.blogspot.com/2018/02/cac-nguyen-tac-cua-tinh-mo-oi-voi-cac.html

[7] ODI (2019): *Anonymisation and Open Data: An introduction to managing the risk of re-identification*: https://docs.google.com/document/d/1CoXniaTnQL_4ZyQuji9_MA_YCEElQjx4z1SEdB08c2M/edit, p.7. Bản dịch sang tiếng Việt: https://www.dropbox.com/s/qmc5gbcmdci1et2/%23OPEN%20RDP8%20Anonymisation%20and%20open%20data%20An%20introduction%20to%20managing%20the%20risk%20of%20re-identification_Vi-11042022.pdf?dl=0, tr. 9.

[8] Lê Trung Nghĩa (2022): *Dữ liệu cá nhân trở thành dữ liệu mở?*: https://giaoducmo.avnuc.vn/bai-viet-toan-van/khi-du-lieu-ca-nhan-co-the-tro-thanh-du-lieu-mo-653.html

[9] Open Data Institute (ODI) (2023): *5 Year Strategy 2023 - 2028 Summary*: https://www.theodi.org/wp-content/uploads/2023/02/ODI-Five-Year-Strategy-2023-2028-Summary.pdf, Principle 2, p. 9. Bản dịch sang tiếng Việt: https://www.dropbox.com/scl/fi/5iaibka09k6d9hb6krq53/ODI-Five-Year-Strategy-2023-2028-Summary_Vi-09082023.pdf?rlkey=fhnr9g5qfrvvd9kbn0tgwokdf&dl=0, tr.9.

[10] Lê Trung Nghĩa (2022): *Phần mềm nguồn mở: Trên đường bảo vệ dữ liệu cá nhân*: https://giaoducmo.avnuc.vn/bai-viet-toan-van/phan-mem-nguon-mo-tren-duong-bao-ve-du-lieu-ca-nhan-635.html

[11] Elaine Mackey, Mark Elliot, Kieron O'Hara (2016): *The Anonymisation Decision-making Framework*. Published by ODI, 2016: https://fpf.org/wp-content/uploads/2016/11/Mackey-Elliot-and-OHara-Anonymisation-Decision-making-Framework-v1-Oct-2016.pdf; pp1-2.

[12] Mark Elliot, Elaine Mackey & Kieron O'Hara (2020): *The Anonymisation Decision-Making Framework 2nd Edition: European Practitioners' Guide*: https://msrbcel.files.wordpress.com/2020/11/adf-2nd-edition-1.pdf, pp. 14-19.

[13] Lê Trung Nghĩa (2022): *Khung Ra quyết định Ẩn danh của Vương quốc Anh?*: https://giaoducmo.avnuc.vn/bai-viet-toan-van/khung-ra-quyet-dinh-an-danh-cua-vuong-quoc-anh-676.html

[14] UK Anonimisation Network: *The ADF*: https://ukanon.net/framework/

Lê Trung Nghĩa, ORCID iD: https://orcid.org/0009-0007-7683-7703

Viện Nghiên cứu, Đào tạo và Phát triển Tài nguyên Giáo dục Mở

Hiệp hội các trường đại học cao đẳng Việt Nam

(Bài viết dành cho hội thảo với chủ đề 'WAI!' tại sự kiện Security Bootcamp 2023, diễn ra trong các ngày 08-10/09/2023 tại Đà Nẵng).