MỤC LỤC

I. THÔNG TIN CHUNG

1. Mục đích

Quy chế bảo vệ dữ liệu cá nhân này ("**Quy chế**") được xây dựng và triển khai nhằm mục đích bảo vệ dữ liệu cá nhân và an toàn thông tin của các khách hàng, người lao động và đối tác của Công ty. Quy chế này đưa ra các yêu cầu chung đối với Công ty về việc thu thập và xử lý dữ liệu cá nhân.

2. Phạm vi và đối tượng áp dụng

Quy chế này áp dụng tại [*Công ty cổ phần FPT và các Công ty thành viên (CTTV) thuộc FPT theo chuẩn quản trị]* (sau đây gọi chung là "**Công ty**").

3. Thuật ngữ

- "**DLCN**" (dữ liệu cá nhân) được hiểu 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. DLCN bao gồm DLCN cơ bản và DLCN nhạy cảm. DLCN mà Công ty có thể thu thập từ nguồn DLCN của Khách Hàng, DLCN của Người Lao Động, DLCN Vãng lai.
- "**DLCN của Khách hàng**" được hiểu là thông tin cá nhân của khách hàng mà Công ty thu thập, xử lý trong quá trình giao dịch, cung cấp hàng hóa, dịch vụ cho khách hàng.
- "**DLCN của Người Lao động**" được hiểu là các thông tin cá nhân và người thân của người lao động của Công ty mà Công ty thu thập, xử lý trong quá trình người lao động làm việc tại Công ty.
- "**DLCN Vãng lai**" được hiểu là các thông tin của cá nhân mà Công ty có được nhưng **không** thông qua (i) hoạt động giao dịch, cung cấp hàng hóa, dịch vụ cho khách hàng của Công ty, (ii) quá trình hợp tác, giao dịch, ký kết và thực hiện hợp đồng với đối tác của Công ty, và (iii) việc ký kết và thực hiện hợp đồng lao động. DLCN Vãng lai thường bao gồm *hình ảnh, hoạt động, vị trí thu thập được (VD: qua camera, cảm biến) của người qua lại các cửa hàng kinh doanh, khu văn phòng… của Tập đoàn* và các thông tin tương tự khác.
- "**Chủ thể Dữ liệu**" được hiểu là cá nhân được DLCN phản ánh.
- "**Xử lý DLCN**" là một hoặc nhiều hoạt động tác động tới DLCN, như: 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 DLCN hoặc các hành động khác có liên quan.
- "**Bên Kiểm soát DLCN**" hay "**Bên Kiểm soát dữ liệu cá nhân**" được hiểu là cá nhân, tổ chức quyết định mục đích và phương thức xử lý DLCN. Để làm rõ, Bên Kiểm soát DLCN bao gồm cả đơn vị không sở hữu nguồn DLCN nhưng được sử dụng các DLCN đó hoặc là bên kiểm soát thông tin, dữ liệu chứa đựng các DLCN đó.
- "**Bên Xử Lý DLCN**" được hiểu là cá nhân hoặc tổ chức thực hiện việc xử lý DLCN thay mặt cho Bên Kiểm soát DLCN, thông qua một hợp đồng hoặc thỏa thuận với Bên Kiểm soát DLCN.
- "**Bên Kiểm soát và Xử lý DLCN**" là tổ chức, cá nhân đồng thời quyết định mục đích, phương tiện và trực tiếp xử lý DLCN.
- "**Bên thứ ba**" là tổ chức, cá nhân ngoài Chủ thể Dữ liệu, Bên Kiểm soát DLCN, Bên Xử lý DLCN, Bên Kiểm soát và Xử lý DLCN được phép xử lý DLCN.
- "**Sự cố Thông tin**" được hiểu là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng; hoặc sự cố xâm phạm an toàn dẫn tới việc phá hủy, mất, thay đổi trái pháp luật hoặc bất ngờ, tiết lộ trái phép, hoặc truy cập trái phép thông tin được thu thập và/hoặc xử lý.

4. Nguyên tắc chung

4.1 Nguyên tắc bảo vệ DLCN

- DLCN được xử lý hợp pháp, minh bạch và được bảo vệ bởi các biện pháp phù hợp theo quy định của Quy chế này, và theo quy định của pháp luật.

- Nghiêm cấm mọi hình thức mua, bán DLCN.
- DLCN được cập nhật, bổ sung phù hợp và chỉ được xử lý cho các mục đích hợp pháp của Công ty, và đã được tuyên bố và được sự chấp thuận của chủ thể dữ liệu.
- Tôn trọng các quyền của chủ thể dữ liệu liên quan đến thông tin cá nhân của họ.
- Công ty có trách nhiệm bảo đảm an toàn thông tin mạng đối với DLCN do mình xử lý.

4.2 Lưu ý áp dụng

- Các thông tin được Công ty thu thập, xử lý có thể thuộc sở hữu của các Chủ thể Dữ liệu ở nhiều quốc gia khác nhau (Việt Nam, Hoa Kỳ, Châu Âu, Hàn Quốc, v.v.). Ngoài ra, thông tin thu thập, xử lý ở một quốc gia có thể được chuyển sang một hoặc nhiều quốc gia khác. Do đó, Công ty cần lưu ý tuân thủ không chỉ luật Việt Nam mà cả pháp luật của các nước liên quan, trong đó có đạo luật General Data Protection Regulation ("**GDPR**") khi xử lý thông tin của Chủ thể Dữ liệu người nước ngoài liên quan.
- Quy chế này được xây dựng chủ yếu dựa trên các quy định của pháp luật về dữ liệu cá nhân và an toàn thông tin của Việt Nam, trong đó có tính đến một số quy định quan trọng của GDPR.
- Quy chế chỉ đưa ra các quy định mang tính định hướng dựa trên các quy định pháp luật cơ bản và trực diện nhất. Quy chế không bao gồm tất cả các quy định pháp luật trong và ngoài nước có liên quan. Do đó, trường hợp phát sinh tình huống không nằm trong Quy chế này, yêu cầu đơn vị chủ động liên hệ với người phụ trách hoặc tham vấn ý kiến của pháp chế Công ty, và/hoặc luật sư trong trường hợp cần thiết.

II. NỘI DUNG CHÍNH

1. Xử lý DLCN

1.1. Trước khi xử lý dữ liệu

Trước khi thu thập, xử lý DLCN của Chủ thể Dữ liệu, Công ty phải xin chấp thuận (sự đồng ý) của người đó:

- Khi xin chấp thuận, Chủ thể Dữ liệu phải được thông báo về: mục đích, cách thức, thời gian bắt đầu và kết thúc việc xử lý; loại DLCN và thông tin về bên thứ ba liên quan đến mục đích xử lý.
- Sự im lặng hoặc không phản hồi của Chủ thể Dữ liệu không được coi là sự đồng ý.
- Chỉ được xử lý, sử dụng thông tin cho mục đích khác với mục đích ban đầu sau khi được Chủ thể Dữ liệu chấp thuận bổ sung (phải tiến hành các bước xin chấp thuận bổ sung).
- Sự đồng ý của Chủ thể Dữ liệu phải 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.

Việc xin chấp thuận được hướng dẫn đối với từng chủ thể như sau:

1.1.1 Đối với DLCN của Khách Hàng

- Việc xin chấp thuận/chấp thuận bổ sung thực hiện theo CHÍNH SÁCH BẢO MẬT DỮ LIỆU CÁ NHÂN được Công ty đăng tải công khai hoặc quy định trong các văn bản thỏa thuận ký kết với Chủ thể DLCN. Bản mẫu chính sách bảo mật DLCN được đính kèm theo Quy chế này. Công ty xây dựng phương thức thực hiện phù hợp cho từng sản phẩm, dịch vụ của mình.
- Đối với việc xử lý DLCN của Khách hàng để kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo cần phổ biến cho Khách hàng biết rõ nội dung, phương thức, hình thức, tần suất giới thiệu sản phẩm.

1.1.2 Đối với DLCN của Người Lao Động

- Việc xin chấp thuận thực hiện theo CHÍNH SÁCH BẢO MẬT DỮ LIỆU CÁ NHÂN CỦA CÁN BỘ NHÂN VIÊN áp dụng trong nội bộ. Bản mẫu chính sách bảo mật DLCN của CBNV được đính kèm theo Quy chế này.

1.1.3 Đối với DLCN vãng lai

- Tại các địa điểm mà Công ty có khả năng thu thập và xử lý DLCN vãng lai, cần truyền tải rộng rãi bằng phương thức hợp lý, trong đó (i) nêu rõ khu vực có sử dụng camera/sensor đối với khu vực thuộc quyền sử dụng của Công ty, (ii) có link (hoặc mã QR) dẫn chiếu đến chính sách bảo mật của Công ty. Tuy nhiên, kể cả trong trường hợp đã đặt các thông báo này, việc sử dụng DLCN vãng lai cho mục đích thương mại cũng cần được cân nhắc, và chỉ sử dụng cho mục đích bảo đảm an toàn an ninh và các mục đích hợp lệ theo quy định của pháp luật.

1.1.4 Các quy định khác

a. Không cần xin chấp thuận của Chủ thể Dữ liệu trong các trường hợp sau:
   - Trường hợp khẩn cấp để bảo vệ tính mạng, sức khỏe của Chủ thể Dữ liệu hoặc người khác;
   - Việc công khai DLCN theo quy định của luật;
   - Để thực hiện nghĩa vụ theo hợp đồng của Chủ thể Dữ liệu với Công ty;
   - DLCN có được từ hoạt động ghi âm, ghi hình nơi công cộng với mục đích 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;
   - Trường hợp khó xác định, nên thu thập sự chấp thuận của Chủ thể Dữ liệu.

b. Trong trường hợp Công ty có thỏa thuận cho phép bên thứ ba được quyền chia sẻ, truy cập hoặc sử dụng DLCN của Công ty thì đơn vị liên quan ký kết thỏa thuận với đối tác phải đảm bảo việc cho phép đối tác được sử dụng DLCN là phù hợp với mục đích đã được Chủ thể Dữ liệu cho phép và đối tác phải tuyệt đối tuân thủ quy định về bảo vệ DLCN cũng như các yêu cầu khác về bảo mật thông tin của Công ty.

1.2. Trong quá trình xử lý dữ liệu

Trong quá trình xử lý dữ liệu, Chủ thể Dữ liệu có quyền yêu cầu cung cấp, truy cập, sửa đổi, rút lại sự đồng ý, xóa, hạn chế xử lý, phản đối xử lý dữ liệu. Khi nhận được các yêu cầu thực hiện quyền của Chủ thể Dữ liệu, bộ phận phụ trách tại từng Công ty cần lưu ý:

- Thực hiện yêu cầu, hoặc cung cấp cho Chủ thể Dữ liệu quyền tiếp cận để tự cập nhật, sửa đổi thông tin, trừ trường hợp có quy định khác;
- Sau khi nhận được các yêu cầu về: cung cấp dữ liệu; hạn chế xử lý dữ liệu; yêu cầu phản đối xử lý dữ liệu; hoặc xóa dữ liệu, bộ phận phụ trách cần thực hiện trong 72 giờ;
- Khi rút lại sự đồng ý, cần thực hiện thông báo cho Chủ thể Dữ liệu về hậu quả, thiệt hại có thể xảy ra;
- Đối với yêu cầu chỉnh sửa dữ liệu, nếu không thể thực hiện thì cần thông báo tới Chủ thể Dữ liệu sau 72 giờ kể từ khi nhận được yêu cầu;
- Công ty, nếu phát sinh hoạt động thu thập và xử lý DLCN, cần chỉ định bộ phận/nhân sự phụ trách bảo vệ DLCN.

1.3. Báo cáo đánh giá tác động

- Kể từ thời điểm bắt đầu xử lý DLCN, cần lập và lưu giữ hồ sơ đánh giá tác động xử lý DLCN hoặc việc chuyển DLCN ra nước ngoài sẵn sàng để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an theo quy định của pháp luật tại từng thời kỳ.
- Hồ sơ đánh giá tác động được thực hiện theo hướng dẫn tại Nghị định 13/2023/NĐ-CP hoặc các quy định khác theo từng thời kỳ.

2. Thuê ngoài xử lý dữ liệu

- Trong trường hợp Công ty thuê ngoài xử lý dữ liệu, cần có hợp đồng hoặc thỏa thuận với Bên Xử Lý DLCN.
- Trường hợp Công ty xử lý DLCN của người nước ngoài là công dân thuộc và đang sinh sống tại khối Liên minh Châu Âu, nếu Công ty thuê ngoài dịch vụ xử lý thông

tin, hợp đồng với Bên Xử lý DLCN phải có một số điều khoản bắt buộc theo Điều 28.3 của GDPR1.

3. Nhật ký xử lý dữ liệu

- Công ty phải ghi lại và lưu trữ nhật ký hệ thống quá trình hoạt động xử lý DLCN. Phụ thuộc vào cấp độ hệ thống thông tin của từng công ty, Công ty có thể xây dựng tiêu chuẩn nhật ký hệ thống tương ứng theo hướng dẫn tại TCVN 11930:2017 công nghệ thông tin – các kỹ thuật an toàn – yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ hoặc các quy định khác theo từng thời kỳ.
- Ví dụ, đối với hệ thống thông tin cấp độ 2[2], nhật ký hệ thống gồm: Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống; Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia hoạt động giám sát.

4. Biện pháp bảo vệ dữ liệu

- Công ty cần tiến hành các biện pháp quản lý, kỹ thuật cần thiết để bảo đảm thông tin không bị mất, đánh cắp, tiết lộ, thay đổi hoặc phá huỷ. Việc xây dựng phương án bảo đảm an toàn thông tin đáp ứng yêu cầu cơ bản theo từng cấp độ có thể thực hiện theo nguyên tắc quy định tại Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ hoặc các quy định khác theo từng thời kỳ.

4.1. Biện pháp quản lý

Công ty có thể lựa chọn thiết lập các yêu cầu cơ bản đối với từng cấp độ hệ thống thông tin của mình, bao gồm:

- Chính sách an toàn thông tin (Vui lòng xem thêm tại Quy định quản trị dữ liệu Tập đoàn FPT mã hiệu 05-QD/TT/HDCV/FPT);
- Tổ chức bảo đảm an toàn thông tin;
- Bảo đảm nguồn nhân lực;
- Quản lý thiết kế, xây dựng hệ thống;
- Quản lý vận hành hệ thống;
- Phương án quản lý rủi ro an toàn thông tin;
- Phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.

4.2. Biện pháp kỹ thuật

Công ty có thể lựa chọn thiết lập các yêu cầu cơ bản đối với từng cấp độ hệ thống thông tin của mình, bao gồm:

- Bảo đảm an toàn mạng;
- Bảo đảm an toàn máy chủ;
- Bảo đảm an toàn cho máy tính của người dùng;
- Bảo đảm an toàn ứng dụng;
- Bảo đảm an toàn dữ liệu.

5. Xử lý sự cố/Thông báo vi phạm

5.1. Trách Nhiệm Thông Báo

Khi phát hiện Sự cố Thông tin, bộ phận phụ trách phải thông báo cho bộ phận IT để phối hợp xử lý. Trường hợp mức độ ảnh hưởng lớn, bộ phận phụ trách phối hợp với bộ phận IT để thông báo cho Ban Điều hành của Công ty đó.

5.2. Thông báo vi phạm

[1] https://gdpr-info.eu/art-28-gdpr/
Tham khảo: https://learn.microsoft.com/vi-vn/legal/gdpr

[2] Việc xác định cấp độ hệ thống thông tin thực hiện theo Luật An toàn thông tin mạng; Nghị định 85/2016/NĐ-CP hoặc các quy định khác theo từng thời kỳ.

Chậm nhất 72 giờ sau khi xảy ra hành vi vi phạm, Công ty phải thông báo cho Bộ Công an – Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao khi phát hiện các trường hợp sau:

- Phát hiện hành vi vi phạm pháp luật đối với DLCN;
- DLCN bị xử lý sai mục đích, không đúng thỏa thuận ban đầu giữa chủ thể dữ liệu và Bên Kiểm soát DLCN, Bên Kiểm soát và xử lý DLCN hoặc vi phạm quy định của pháp luật;
- Không bảo đảm quyền của chủ thể dữ liệu hoặc không được thực hiện đúng;
- Trường hợp khác theo quy định của pháp luật.

Báo cáo được thực hiện theo quy định tại Nghị định 13/2023/NĐ-CP hoặc các quy định khác theo từng thời kỳ.

6. Đào tạo

Người được giao làm công tác bảo vệ DLCN được đào tạo nhận thức an toàn thông tin, bảo vệ dữ liệu định kỳ hàng năm.

III. TỔ CHỨC THỰC HIỆN

1. Ban Công nghệ Thông tin, Ban Nhân sự, Ban Công nghệ, Ban Giám sát tuân thủ của Tập đoàn và các đơn vị liên quan chịu trách nhiệm triển khai, hướng dẫn các CTTV xây dựng hệ thống bảo vệ DLCN tại đơn vị, tuân thủ theo Quy chế này và các quy chế liên quan đã được ban hành của Tập đoàn FPT.
2. Chủ tịch/Tổng giám đốc CTTV chịu trách nhiệm triển khai các quy định của Quy chế này.

CÔNG TY CỔ PHẦN FPT