NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số : /2024/TT-NHNN	*Hà Nội, ngày tháng năm 2024*

DỰ THẢO

THÔNG TƯ
Quy định về triển khai giao diện lập trình ứng dụng mở trong ngành Ngân hàng

Căn cứ Luật Ngân hàng Nhà nước Việt Nam ngày 16 tháng 6 năm 2010;

Căn cứ Luật Các tổ chức tín dụng ngày 18 tháng 01 năm 2024;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 117/2018/NĐ-CP ngày 11 tháng 9 năm 2018 của Chính phủ quy định về việc giữ bí mật, cung cấp thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài;

Căn cứ Nghị định số 102/2022/NĐ-CP ngày 12 tháng 12 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ quy định về bảo vệ dữ liệu cá nhân;

Theo đề nghị của Cục trưởng Cục Công nghệ thông tin;

Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư quy định về triển khai giao diện lập trình ứng dụng mở trong ngành ngân hàng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Thông tư này quy định về việc triển khai giao diện lập trình ứng dụng mở trong ngành ngân hàng.

2. Thông tư này không áp dụng đối với việc xử lý dữ liệu chứa thông tin thuộc phạm vi bí mật nhà nước. Việc xử lý dữ liệu chứa thông tin thuộc phạm vi bí mật nhà nước được thực hiện theo quy định của pháp luật hiện hành.

3. Thông tư này áp dụng đối với ngân hàng, chi nhánh ngân hàng nước ngoài (sau đây gọi chung là Ngân hàng).

4. Tổ chức tín dụng phi ngân hàng, tổ chức tài chính vi mô và Quỹ tín dụng nhân dân, tổ chức cung ứng dịch vụ trung gian thanh toán khi triển khai dịch vụ thông qua Open API khuyến khích tuân thủ các quy định tại Thông tư này.

Điều 2. Giải thích từ ngữ

Trong Thông tư này, một số thuật ngữ được hiểu như sau:

1. API (Application Programming Interface) là giao diện lập trình ứng dụng cho phép giao tiếp giữa các ứng dụng phần mềm trong một tổ chức hoặc giữa các tổ chức với nhau.

2. Giao diện lập trình ứng dụng mở (Open API) trong ngành Ngân hàng là các API của Ngân hàng cho phép bên thứ ba có thể xử lý dữ liệu để sử dụng hoặc cung ứng sản phẩm dịch vụ cho khách hàng.

3. Bên thứ ba (TPP) là các tổ chức có thỏa thuận bằng hợp đồng sử dụng dịch vụ với Ngân hàng trong việc kết nối, xử lý dữ liệu qua Open API để sử dụng hoặc cung ứng sản phẩm dịch vụ cho khách hàng.

4. Các bên là bao gồm Ngân hàng và bên thứ ba.

5. Sự chấp thuận của khách hàng là việc thể hiện rõ ràng, tự nguyện, khẳng định việc cho phép xử lý dữ liệu cá nhân của khách hàng.

Điều 3. Nguyên tắc chung

Các bên khi thực hiện triển khai Open API phải tuân thủ các yêu cầu sau:

1. Tuân thủ các quy định về giữ bí mật, cung cấp thông tin và bảo vệ dữ liệu cá nhân.

2. Dữ liệu trong quá trình xử lý phải được quản lý, lưu trữ, khai thác, sử dụng đúng mục đích tại văn bản thỏa thuận giữa các bên.

3. Dữ liệu trong quá trình xử lý phải đảm bảo tính cập nhật và chính xác. Trường hợp có sai lệch phải thực hiện đính chính, hiệu chỉnh kịp thời theo thỏa thuận giữa các bên.

4. Dữ liệu của khách hàng trong quá trình xử lý phải được sự chấp thuận của khách hàng và chỉ phục vụ cho chính khách hàng đó.

Chương II
QUY ĐỊNH CỤ THỂ VỀ TRIỂN KHAI OPEN API

Mục 1

QUY ĐỊNH TRIỂN KHAI OPEN API

Điều 4. Nguyên tắc cung cấp dịch vụ Open API

1. Ngân hàng phải cung cấp dịch vụ Open API cho bên thứ ba để thực hiện kết nối và xử lý dữ liệu theo quy định tại Thông tư này.

2. Ngân hàng phải cung cấp các hàm Open API theo danh mục hàm Open API quy định tại khoản 2 Điều 5 Thông tư này.

3. Ngân hàng cung cấp các hàm Open API phải tuân thủ danh mục tiêu chuẩn kỹ thuật quy định tại Điều 6 Thông tư này.

Điều 5. Danh mục hàm Open API

1. Danh mục hàm Open API gồm:

a) Các hàm Open API cho phép truy vấn thông tin mà Ngân hàng phải công bố, công khai theo quy định của pháp luật;

b) Các hàm Open API cho phép truy vấn thông tin của khách hàng khi được sự chấp thuận của khách hàng;

c) Các hàm Open API cho phép khởi tạo lệnh thanh toán, chuyển tiền;

d) Các hàm Open API khác.

2. Danh mục hàm Open API tối thiểu quy định cụ thể tại Phụ lục 02 ban hành kèm Thông tư này.

3. Ngân hàng có thể cung cấp các hàm Open API theo nhu cầu thực tế ngoài danh mục hàm Open API tối thiểu quy định tại khoản 2 Điều này.

4. Các hàm Open API quy định tại khoản 2 Điều này do Thống đốc Ngân hàng Nhà nước quy định theo từng thời kỳ.

Điều 6. Danh mục tiêu chuẩn kỹ thuật

1. Các tiêu chuẩn kỹ thuật Open API trong ngành Ngân hàng gồm tiêu chuẩn kiến trúc, tiêu chuẩn dữ liệu và tiêu chuẩn an toàn thông tin.

2. Các tiêu chuẩn kỹ thuật Open API tối thiểu trong ngành Ngân hàng quy định cụ thể tại Phụ lục 01 ban hành kèm Thông tư này.

Điều 7. Công khai dịch vụ Open API

Ngân hàng phải công khai dịch vụ Open API trên cổng thông tin điện tử của Ngân hàng bao gồm tối thiểu các nội dung sau:

1. Hệ thống thử nghiệm để cung cấp cho bên thứ ba phục vụ kết nối, xử lý dữ liệu thử nghiệm qua Open API.

2. Các tài liệu phục vụ kết nối, xử lý dữ liệu đối với hệ thống thử nghiệm Open API gồm: Quy trình thực hiện kết nối, luồng xử lý dữ liệu và các thông tin chi tiết đối với từng hàm Open API.

3. Tối thiểu các hàm Open API quy định tại khoản 2, Điều 5 Thông tư này.

Điều 8. Lộ trình triển khai Open API

Ngân hàng phải triển khai Open API theo các mốc thời gian sau:

1. Cung cấp các hàm Open API theo quy định tại điểm a khoản 1 Điều 5 trong vòng 12 tháng kể từ thời điểm Thông tư này có hiệu lực.

2. Cung cấp các hàm Open API theo quy định tại điểm b khoản 1 Điều 5 trong vòng 18 tháng kể từ thời điểm Thông tư này có hiệu lực.

3. Cung cấp các hàm Open API theo quy định tại điểm c khoản 1 Điều 5 trong vòng 24 tháng kể từ ngày Thông tư này có hiệu lực.

Mục 2

QUYỀN VÀ TRÁCH NHIỆM CỦA NGÂN HÀNG

Điều 9. Quyền của Ngân hàng

1. Từ chối hoặc tạm dừng cung cấp dịch vụ Open API khi bên thứ ba không đáp ứng đầy đủ các điều kiện tại điểm đ khoản 1 Điều 10.

2. Yêu cầu bên thứ ba cung cấp các thông tin cần thiết liên quan đến quá trình kết nối, xử lý dữ liệu thông qua dịch vụ Open API phù hợp quy định của pháp luật.

3. Các quyền khác theo hợp đồng với bên thứ ba.

Điều 10. Trách nhiệm của Ngân hàng

1. Trách nhiệm của Ngân hàng đối với cung cấp dịch vụ Open API:

a) Hoàn thiện cơ sở hạ tầng hệ thống thông tin để sẵn sàng kết nối, xử lý dữ liệu;

b) Xây dựng và hoàn thiện các tài liệu hướng dẫn kết nối, xử lý dữ liệu;

c) Bảo đảm chất lượng dữ liệu trong quá trình xử lý được cung cấp; Thông báo kịp thời cho bên thứ ba khi có sự sai lệch dữ liệu, phối hợp với bên thứ ba đính chính, hiệu chỉnh kịp thời khi có sai lệch;

d) Hệ thống thông tin phục vụ dịch vụ Open API phải bảo đảm an toàn, an ninh mạng đáp ứng tối thiểu cấp độ 3 theo quy định tại Nghị định của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ và tuân thủ Thông tư của Ngân hàng Nhà nước Việt Nam quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng;

đ) Chỉ hợp tác với bên thứ ba nếu thỏa mãn tối thiểu các điều kiện sau:

- Có hệ thống thông tin phục vụ cho mục đích kết nối, xử lý dữ liệu của bên thứ ba bảo đảm an toàn, an ninh mạng đáp ứng tối thiểu tương đương với cấp độ của hệ thống cung cấp Open API của Ngân hàng nhưng không thấp hơn cấp độ 3 theo quy định tại Nghị định của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Là đơn vị hoạt động được cấp mã số thuế còn hoạt động hợp pháp tại Việt Nam;

- Bảo đảm nhân sự có kinh nghiệm đối với từng vị trí: An ninh an toàn thông tin, vận hành, phát triển hệ thống công nghệ thông tin và pháp chế về công nghệ thông tin;

e) Chỉ cho phép bên thứ ba sử dụng dịch vụ Open API theo quy định tại Điều 4, Điều 5 và Điều 6 Thông tư này;

g) Cung cấp công cụ hoặc chức năng cho phép khách hàng của ngân hàng có thể:

- Tra cứu các dữ liệu mà khách hàng chấp thuận cho bên thứ ba xử lý;

- Hủy bỏ quyền xử lý dữ liệu của bên thứ ba;

h) Thời gian xử lý dữ liệu khách hàng khi được khách hàng chấp thuận không quá 180 ngày;

i) Cung cấp thông tin tình hình triển khai Open API cho Ngân hàng Nhà nước khi được yêu cầu (thông qua Cục Công nghệ thông tin);

k) Phối hợp với bên thứ ba theo thỏa thuận và cơ quan có thẩm quyền giải quyết vướng mắc, tranh chấp trong quá cung cấp dịch vụ Open API;

l) Ngân hàng phải có giải pháp công nghệ cung cấp cho bên thứ ba phục vụ việc nhận biết và xác minh thông tin nhận biết khách hàng trong quá trình triển khai dịch vụ Open API; chịu trách nhiệm về rủi ro phát sinh (nếu có);

m) Ngân hàng có mẫu Hợp đồng cung cấp dịch vụ Open API với tối thiểu các nội dung sau:

- Cam kết bảo mật thông tin;

- Cam kết sử dụng dữ liệu do ngân hàng cung cấp đúng phạm vi, mục đích;

- Bên thứ ba phải thông báo cho ngân hàng khi phát hiện nhân sự vi phạm quy định về an toàn thông tin đối với dịch vụ Open API;

- Thông tin về sản phẩm dịch vụ;

- Thông tin về phí dịch vụ (nếu có);

- Điều khoản chấm dứt hợp đồng;

- Điều khoản về Hệ thống thông tin kết nối, xử lý dữ liệu thông qua Open API phải đạt cấp độ 3 trở lên;

n) Trường hợp sử dụng dịch vụ công nghệ thông tin của bên thứ ba, Ngân hàng phải tuân thủ Thông tư của Ngân hàng Nhà nước Việt Nam quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng;

o) Thực hiện kiểm tra bên thứ ba đáp ứng điều kiện tại điểm e khoản 1 Điều này định kỳ hàng năm.

2. Trách nhiệm của Ngân hàng đối với quản lý bên thứ ba:

Ngân hàng phải yêu cầu bên thứ ba thực hiện những nội dung sau:

a) Cung cấp công cụ hoặc chức năng cho phép khách hàng có thể:

- Tra cứu các dữ liệu mà khách hàng chấp thuận cho bên thứ ba xử lý;

- Hủy bỏ quyền xử lý dữ liệu của bên thứ ba.

b) Quy định và thông báo cho khách hàng các điều khoản, điều kiện về việc sử dụng dịch vụ qua kênh thích hợp như: Trang thông tin điện tử của bên thứ ba, tờ rơi, mẫu hợp đồng/mẫu đăng ký sử dụng dịch vụ;

c) Hướng dẫn khách hàng cách thức sử dụng dịch vụ;

d) Ban hành Quy trình quản lý rủi ro; Quy trình chăm sóc khách hàng; Quy trình xử lý khiếu nại; Quy trình đảm bảo hoạt động liên tục và Quy trình sử dụng dịch vụ đối tác khi cung cấp dịch vụ cho khách hàng;

đ) Bảo đảm an toàn, bảo mật thông tin khi thực hiện xử lý dữ liệu thông qua Open API do Ngân hàng cung cấp;

e) Khai thác và sử dụng dữ liệu đúng phạm vi theo thỏa thuận giữa các bên và theo quy định của pháp luật;

g) Thông báo kịp thời cho Ngân hàng khi xảy ra sự cố về công nghệ thông tin, an toàn thông tin có liên quan. Hình thức và thời gian thông báo theo thỏa thuận giữa các bên;

h) Thông báo kịp thời cho Ngân hàng khi có sự sai lệch dữ liệu, phối hợp với Ngân hàng đính chính, hiệu chỉnh kịp thời khi có sai lệch;

i) Tuân thủ các quy định về triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến theo quy định của pháp luật khi thực hiện khởi tạo lệnh thanh toán, chuyển tiền qua Open API;

j) Giới hạn số lần truy vấn tự động thông tin khách hàng của bên thứ ba theo ngày.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 11. Trách nhiệm của Cục Công nghệ thông tin

1. Chủ trì, phối hợp với các đơn vị liên quan thuộc Ngân hàng Nhà nước xử lý các vướng mắc phát sinh trong quá trình thực hiện Thông tư này.

2. Làm đầu mối tiếp nhận thông tin tình hình triển khai về việc triển khai Open API của các ngân hàng.

3. Thực hiện kiểm tra Ngân hàng trong việc thực hiện Thông tư này.

Điều 12. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày ... tháng ... năm 2024.

Điều 13. Tổ chức thực hiện

Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các đơn vị liên quan thuộc Ngân hàng Nhà nước, Chủ tịch Hội đồng quản trị, Hội đồng thành viên, Tổng giám đốc (Giám đốc) các ngân hàng, chi nhánh ngân hàng nước ngoài chịu trách nhiệm tổ chức thực hiện Thông tư này./.

Nơi nhận:
- Như Điều 13;
- Ban Lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Cổng TTĐT của NHNN;
- Lưu VP, PC, CNTT (03 bản).

THỐNG ĐỐC