DATA PROTECTION IN SOFTWARE DEVELOPMENT POLICY

CHÍNH SÁCH BẢO VỆ DỮ LIỆU TRONG PHÁT TRIỂN PHẦN MỀM

Privacy by Design • Minimize by Default • No Real Data in Test

Tổ chức / Organization	[Tên tổ chức]
Chủ sở hữu / Document Owner	[Data Protection Officer (DPO) / Head of Legal-Compliance]
Phê duyệt / Approved by	Engineering Governance Council
Ngày hiệu lực / Effective Date	[DD/MM/YYYY]
Phiên bản / Version	1.0
Chu kỳ rà soát / Review Cycle	Hằng năm, hoặc ngay khi có thay đổi đáng kể về pháp luật bảo vệ dữ liệu cá nhân
Tài liệu cấp trên / Parent Documents	Engineering Constitution v1.0 (Tầng 1); Software Development Governance Policy v1.0 (Tầng 2), đặc biệt Điều 5.2
Phân loại / Classification	INTERNAL

SAMPLE DOCUMENT

A. Kiểm soát tài liệu

DOCUMENT CONTROL

Phiên bản	Ngày	Người soạn	Mô tả thay đổi
1.0	[DD/MM/YYYY]	[Tên / Vai trò]	Ban hành lần đầu

B. Mục lục nội dung

CONTENTS

- 1. Mục đích
- 2. Phạm vi áp dụng
- 3. Liên kết với Engineering Constitution
- 4. Định nghĩa
- 5. Yêu cầu bắt buộc
- 6. Vai trò và trách nhiệm
- 7. Đo lường tuân thủ
- 8. Cơ chế ngoại lệ
- 9. Không tuân thủ
- 10. Chủ sở hữu tài liệu và chu kỳ rà soát
- 11. Tài liệu liên quan
- 12. Phê duyệt

1. Mục đích

PURPOSE

1. Bảo đảm dữ liệu cá nhân được bảo vệ trong suốt vòng đời phát triển phần mềm — từ thiết kế, viết mã, kiểm thử, triển khai đến vận hành — chứ không chỉ ở giai đoạn production.
2. Cụ thể hóa nguyên tắc Security and Privacy by Design (Điều 2 Engineering Constitution) và mở rộng sâu nội dung đã nêu ngắn gọn tại Software Development Governance Policy (SDGP), Điều 5.2, thành các yêu cầu kỹ thuật cụ thể, đo lường được.
3. Bảo đảm hoạt động phát triển phần mềm tuân thủ Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân (có hiệu lực từ 01/7/2023), đồng thời đối chiếu với thông lệ quốc tế tốt (GDPR, ISO/IEC 27701) khi tổ chức có sản phẩm hoặc khách hàng ở nhiều thị trường.

Chính sách này bổ sung cho SDGP, không thay thế — mọi yêu cầu của SDGP (SDLC, peer review, vai trò/trách nhiệm, cơ chế ngoại lệ, quản lý không tuân thủ...) vẫn áp dụng đầy đủ khi công việc có xử lý dữ liệu cá nhân.

2. Phạm vi áp dụng

SCOPE

- Mọi hệ thống, ứng dụng, API, cơ sở dữ liệu, kho log và pipeline dữ liệu do tổ chức phát triển hoặc vận hành có xử lý dữ liệu cá nhân của khách hàng, người dùng, nhân viên hoặc đối tác.
- Toàn bộ môi trường: production, staging, testing, development, sandbox/demo và các bản sao dữ liệu phục vụ phân tích/báo cáo.
- Nhân sự nội bộ, nhà thầu và đối tác thuê ngoài khi họ tiếp cận hoặc xử lý dữ liệu cá nhân trong quá trình phát triển phần mềm cho tổ chức (bổ sung góc độ bảo vệ dữ liệu, không thay thế Third-Party/Outsourced Development Policy).
- Không áp dụng cho dữ liệu đã được ẩn danh hóa (anonymization) đến mức không thể khôi phục nhận dạng cá nhân bằng bất kỳ biện pháp hợp lý nào — dữ liệu đã giả danh hóa (pseudonymization), có thể khôi phục bằng khóa/bảng ánh xạ, vẫn được coi là dữ liệu cá nhân và thuộc phạm vi Policy này.

3. Liên kết với Engineering Constitution

ALIGNMENT WITH THE CONSTITUTION

Yêu cầu trong Policy	Nguyên tắc Constitution tương ứng
5.1 Phân loại dữ liệu cá nhân	Điều 2 — Security and Privacy by Design
5.2 Cấm dữ liệu sản xuất thật trong môi trường phi sản xuất	Điều 2 — Security and Privacy by Design
5.3 Data minimization trong thiết kế	Điều 2, Điều 5 — Privacy by Design / Everything as Code Where Practical
5.4 Mã hóa dữ liệu cá nhân/nhạy cảm	Điều 2 — Security and Privacy by Design

5.5 Retention và xóa dữ liệu	Điều 2, Điều 6 — Privacy by Design / Observable and Operable by Default
5.6 DPIA và chuyển dữ liệu ra nước ngoài	Điều 2, Điều 8 — Privacy by Design / Evidence over Opinion
5.7 Hỗ trợ quyền của chủ thể dữ liệu trong thiết kế	Điều 1, Điều 2 — Business Value First / Privacy by Design
5.8 Thông báo vi phạm dữ liệu cá nhân	Điều 6, Điều 8 — Observable and Operable by Default / Evidence over Opinion

4. Định nghĩa

DEFINITIONS

- **Dữ liệu cá nhân (Personal Data):** thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trong môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể, theo Nghị định 13/2023/NĐ-CP, Điều 2.
- **Dữ liệu cá nhân cơ bản:** nhóm dữ liệu về nhân thân, liên hệ, tài khoản như họ tên, ngày sinh, giới tính, địa chỉ, quốc tịch, hình ảnh, số điện thoại, số định danh cá nhân/CMND/hộ chiếu... theo Nghị định 13/2023/NĐ-CP, Điều 2, khoản 3.
- **Dữ liệu cá nhân nhạy cảm:** dữ liệu cá nhân gắn liền với quyền riêng tư mà khi bị xâm phạm sẽ ảnh hưởng trực tiếp đến quyền và lợi ích hợp pháp của cá nhân, bao gồm (không giới hạn): quan điểm chính trị/tôn giáo, tình trạng sức khỏe và hồ sơ bệnh án, nguồn gốc chủng tộc/dân tộc, đặc điểm di truyền, đặc điểm sinh học riêng, đời sống/xu hướng tình dục, dữ liệu về tội phạm — theo Nghị định 13/2023/NĐ-CP, Điều 2, khoản 4. Loại dữ liệu này đòi hỏi biện pháp bảo vệ nghiêm ngặt hơn dữ liệu cơ bản.
- **Chủ thể dữ liệu (Data Subject):** cá nhân được dữ liệu cá nhân phản ánh.
- **Bên Kiểm soát dữ liệu cá nhân / Bên Xử lý dữ liệu cá nhân / Bên Kiểm soát và xử lý dữ liệu cá nhân:** cách phân vai theo Nghị định 13/2023/NĐ-CP, Điều 2 — tổ chức quyết định mục đích và phương tiện xử lý (Kiểm soát); tổ chức thực hiện xử lý thay mặt Bên Kiểm soát theo hợp đồng (Xử lý); hoặc tổ chức vừa quyết định mục đích vừa trực tiếp xử lý (Kiểm soát và xử lý) — trường hợp phổ biến nhất với các đội phát triển phần mềm in-house.
- **Data Masking / Anonymization (Ẩn danh hóa) / Pseudonymization (Giả danh hóa):** ba kỹ thuật khác nhau về mức độ, KHÔNG được dùng thay thế lẫn nhau. Anonymization biến đổi dữ liệu đến mức không thể khôi phục nhận dạng cá nhân bằng bất kỳ biện pháp hợp lý nào — khi đó dữ liệu không còn là dữ liệu cá nhân. Pseudonymization thay thế định danh trực tiếp bằng bí danh nhưng vẫn có thể khôi phục liên kết thông qua khóa/bảng ánh xạ được lưu riêng — dữ liệu đã giả danh hóa **vẫn là dữ liệu cá nhân** và phải tiếp tục tuân thủ đầy đủ Policy này. Data masking là thuật ngữ chung cho việc che/biến đổi dữ liệu hiển thị, có thể đạt tới mức anonymization hoặc chỉ ở mức pseudonymization tùy kỹ thuật áp dụng.
- **Synthetic Data (Dữ liệu tổng hợp):** dữ liệu được sinh ra bằng thuật toán/mô hình, có đặc tính thống kê tương tự dữ liệu thật nhưng không bắt nguồn từ bất kỳ cá nhân có thật nào.
- **Data Protection Impact Assessment (DPIA — Đánh giá tác động xử lý dữ liệu cá nhân):** quy trình đánh giá trước khi triển khai một hoạt động xử lý dữ liệu cá nhân có quy mô lớn hoặc rủi ro cao, nhằm nhận diện rủi ro và biện pháp giảm thiểu; tương ứng với hồ sơ đánh giá tác động xử lý dữ liệu cá nhân tại Nghị định 13/2023/NĐ-CP, Điều 24 (xử lý trong nước) và Điều 25 (chuyển dữ liệu ra nước ngoài), và khái niệm DPIA theo GDPR (tham khảo quốc tế).

- **Privacy by Design and by Default:** nguyên tắc thiết kế hệ thống lồng ghép bảo vệ dữ liệu cá nhân ngay từ đầu và mặc định chỉ xử lý dữ liệu cần thiết, theo tinh thần GDPR Điều 25 (tham khảo quốc tế, không phải cơ sở pháp lý bắt buộc tại Việt Nam).

5. Yêu cầu bắt buộc

MANDATORY REQUIREMENTS

5.1 Phân loại dữ liệu cá nhân trong phát triển phần mềm

1. Mọi hệ thống xử lý dữ liệu cá nhân **PHẢI (MUST)** phân loại dữ liệu đang xử lý theo hai nhóm tại Điều 4 — dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm — ngay từ giai đoạn thiết kế (data model, API contract).
2. Việc phân loại **PHẢI (MUST)** được thể hiện bằng tài liệu (data inventory/data map) gắn với từng hệ thống, nêu rõ: loại dữ liệu, mục đích thu thập, nơi lưu trữ, và các hệ thống hạ nguồn (downstream) có nhận dữ liệu đó.
3. Dữ liệu cá nhân nhạy cảm **PHẢI (MUST)** áp dụng biện pháp bảo vệ nghiêm ngặt hơn dữ liệu cơ bản ở mọi khâu: mã hóa (Điều 5.4), giới hạn truy cập theo nguyên tắc đặc quyền tối thiểu, và ưu tiên hàng đầu khi thực hiện data masking (Điều 5.2).

5.2 Cấm dữ liệu sản xuất thật trong môi trường phi sản xuất

1. **KHÔNG ĐƯỢC PHÉP (MUST NOT)** sử dụng dữ liệu cá nhân thật lấy trực tiếp từ môi trường production (chưa qua xử lý che dữ liệu) trong bất kỳ môi trường development, testing, staging, demo hay sandbox nào.
2. Khi cần dữ liệu "giống thật" để kiểm thử, đội ngũ phát triển **PHẢI (MUST)** áp dụng theo thứ tự ưu tiên: (a) **Synthetic data** — sinh dữ liệu không bắt nguồn từ cá nhân có thật, ưu tiên hàng đầu; (b) **Anonymization** — biến đổi không thể khôi phục về dữ liệu gốc, khi cần giữ đặc tính thống kê của dữ liệu thật; (c) **Pseudonymization** có kiểm soát chặt chẽ, chỉ dùng khi thực sự cần khôi phục liên kết trong phạm vi được phê duyệt — lưu ý dữ liệu này vẫn là dữ liệu cá nhân theo Điều 4 và phải tiếp tục được bảo vệ tương ứng (mã hóa, kiểm soát truy cập) ngay trong môi trường test.
3. Quy trình sao chép dữ liệu từ production sang môi trường thấp hơn **PHẢI (MUST)** đi qua bước masking/anonymization tự động, tích hợp trong pipeline — không phụ thuộc vào việc từng kỹ sư tự giác thực hiện thủ công.
4. Ngoại lệ dùng dữ liệu thật giới hạn (ví dụ điều tra sự cố production phức tạp cần tái hiện chính xác) chỉ được thực hiện theo đúng cơ chế ngoại lệ tại Điều 8: có thời hạn ngắn, môi trường cô lập với kiểm soát truy cập và ghi log tương đương production, và phải xóa/thu hồi ngay sau khi hoàn thành mục đích.

5.3 Data minimization trong thiết kế

1. Khi thiết kế API, lược đồ cơ sở dữ liệu và định dạng log, đội ngũ phát triển **PHẢI (MUST)** chỉ thu thập và lưu trữ trường dữ liệu cá nhân thực sự cần thiết cho mục đích nghiệp vụ đã xác định — không thu thập "phòng khi cần dùng sau này".
2. Log ứng dụng, log hệ thống và log của pipeline CI/CD **KHÔNG ĐƯỢC PHÉP (MUST NOT)** ghi lại dữ liệu cá nhân nhạy cảm, mật khẩu/secret, hoặc toàn bộ nội dung request/response có chứa dữ liệu cá nhân, trừ khi có nhu cầu nghiệp vụ/điều tra sự cố được phê duyệt và có biện pháp che/mã hóa tương ứng. Pipeline CI/CD **NÊN (SHOULD)** tích hợp công cụ quét tự động để phát hiện dữ liệu cá nhân/secret bị lộ vào log hoặc biến môi trường trước khi build hoàn tất.
3. Trường dữ liệu cá nhân không còn phục vụ mục đích ban đầu **NÊN (SHOULD)** được rà soát và loại bỏ khỏi lược đồ dữ liệu trong lần refactor gần nhất, thay vì giữ lại vô thời hạn.

4. Yêu cầu này cụ thể hóa nguyên tắc data minimization và purpose limitation (GDPR Điều 5 — tham khảo quốc tế) áp dụng vào giai đoạn thiết kế kỹ thuật.

5.4 Mã hóa dữ liệu cá nhân và dữ liệu nhạy cảm

1. Dữ liệu cá nhân nhạy cảm **PHẢI (MUST)** được mã hóa khi lưu trữ (encryption at rest) trong cơ sở dữ liệu, backup và kho lưu trữ file.
2. Dữ liệu cá nhân (cơ bản và nhạy cảm) **PHẢI (MUST)** được mã hóa khi truyền tải (encryption in transit) giữa client-server, giữa các dịch vụ nội bộ, và khi gửi cho bên thứ ba.
3. Khóa mã hóa **PHẢI (MUST)** được quản lý tách biệt khỏi dữ liệu đã mã hóa, có kiểm soát truy cập riêng và quy trình xoay vòng (rotation) định kỳ.
4. Việc lựa chọn thuật toán/giải pháp mã hóa cụ thể do Standard bảo mật liên quan (Tầng 3) quy định; Policy này chỉ đặt yêu cầu bắt buộc phải mã hóa, không quy định chi tiết kỹ thuật.

5.5 Retention và xóa dữ liệu

1. Mỗi loại dữ liệu cá nhân được thu thập **PHẢI (MUST)** có thời hạn lưu trữ (retention period) được xác định rõ, dựa trên mục đích thu thập và nghĩa vụ pháp luật liên quan (nếu có), ghi trong tài liệu phân loại tại Điều 5.1.
2. Hệ thống **PHẢI (MUST)** có cơ chế (tự động hoặc quy trình vận hành có kiểm soát) để xóa hoặc ẩn danh hóa dữ liệu cá nhân khi hết thời hạn lưu trữ, hoặc khi chủ thể dữ liệu yêu cầu xóa hợp lệ theo Điều 5.7.
3. Việc xóa **PHẢI (MUST)** áp dụng nhất quán trên mọi nơi dữ liệu được sao chép đến (bản chính, backup, cache, kho dữ liệu phân tích, log) trong phạm vi kỹ thuật khả thi; các trường hợp không thể xóa ngay (ví dụ backup đóng băng theo chu kỳ) phải có kế hoạch xóa theo chu kỳ backup tiếp theo.

5.6 Đánh giá tác động xử lý dữ liệu cá nhân (DPIA) và chuyển dữ liệu ra nước ngoài

1. Tính năng hoặc hệ thống mới xử lý dữ liệu cá nhân ở quy mô lớn, dữ liệu cá nhân nhạy cảm, hoặc có rủi ro cao đến quyền và lợi ích của chủ thể dữ liệu **PHẢI (MUST)** thực hiện đánh giá tác động xử lý dữ liệu cá nhân (DPIA) trong giai đoạn thiết kế — trước khi viết mã — tương ứng với yêu cầu lập hồ sơ đánh giá tác động tại Nghị định 13/2023/NĐ-CP, Điều 24.
2. Khi kiến trúc hệ thống có sử dụng hạ tầng đám mây, dịch vụ SaaS hoặc bên thứ ba đặt máy chủ/xử lý dữ liệu ngoài lãnh thổ Việt Nam, đội thiết kế **PHẢI (MUST)** xác định cùng DPO/Legal xem hoạt động đó có cấu thành "chuyển dữ liệu cá nhân ra nước ngoài" theo Nghị định 13/2023/NĐ-CP, Điều 25 hay không, để lập hồ sơ đánh giá tác động chuyển dữ liệu ra nước ngoài tương ứng nếu thuộc phạm vi này. Việc lập và gửi hồ sơ là trách nhiệm pháp lý/tuân thủ của DPO/Legal, không thuộc phạm vi kỹ thuật của Policy này.
3. DPIA **PHẢI (MUST)** được thực hiện song song và liên kết với hoạt động threat modeling của Secure Software Development Policy, vì hai hoạt động chia sẻ nhiều đầu vào (luồng dữ liệu, tác nhân đe dọa, biện pháp giảm thiểu).
4. Kết quả DPIA (bao gồm rủi ro nhận diện và biện pháp giảm thiểu) **PHẢI (MUST)** được lưu lại như bằng chứng (evidence) và là điều kiện đầu vào cho cổng phê duyệt thiết kế trước khi chuyển sang giai đoạn phát triển.

5.7 Hỗ trợ quyền của chủ thể dữ liệu trong thiết kế hệ thống

1. Hệ thống xử lý dữ liệu cá nhân **PHẢI (MUST)** được thiết kế để có thể đáp ứng về mặt kỹ thuật các quyền cơ bản của chủ thể dữ liệu: quyền truy cập dữ liệu của mình, quyền yêu cầu chỉnh sửa, quyền yêu cầu

xóa, và quyền rút lại sự đồng ý đã cho theo Nghị định 13/2023/NĐ-CP, Điều 11.

2. **KHÔNG ĐƯỢC PHÉP (MUST NOT)** thiết kế hệ thống theo cách khiến việc thực hiện các quyền trên trở nên bất khả thi về mặt kỹ thuật — ví dụ dữ liệu cá nhân bị phân tán, sao chép không kiểm soát vào nhiều hệ thống không có cơ chế tra cứu/xóa tương ứng, khiến không thể xác định đầy đủ nơi lưu trữ khi có yêu cầu.
3. Khi thiết kế tính năng thu thập sự đồng ý (consent), đội ngũ phát triển **PHẢI (MUST)** bảo đảm giao diện thể hiện rõ ràng loại dữ liệu, mục đích xử lý và cho phép rút lại sự đồng ý dễ dàng tương đương với lúc cho phép, phù hợp tinh thần Điều 11 nêu trên.

5.8 Thông báo vi phạm dữ liệu cá nhân (Data Breach Notification)

1. Khi phát hiện sự cố có khả năng dẫn đến truy cập, tiết lộ, sửa đổi hoặc phá hủy trái phép dữ liệu cá nhân, đội ngũ liên quan **PHẢI (MUST)** báo cáo ngay cho Document Owner (DPO/Legal) và kích hoạt quy trình ứng phó sự cố bảo mật nội bộ của tổ chức; nếu sự cố có yếu tố không tuân thủ Policy, xử lý song song theo SDGP, Điều 9.
2. Document Owner (DPO/Legal) chịu trách nhiệm đánh giá và, nếu thuộc trường hợp phải thông báo, gửi thông báo vi phạm quy định bảo vệ dữ liệu cá nhân tới cơ quan nhà nước có thẩm quyền trong thời hạn tối đa 72 giờ kể từ khi phát hiện vi phạm, theo Nghị định 13/2023/NĐ-CP, Điều 23. Việc soạn và gửi thông báo là trách nhiệm pháp lý/tuân thủ, không thuộc phạm vi kỹ thuật của Policy này.
3. Đội phát triển/vận hành **PHẢI (MUST)** cung cấp kịp thời cho DPO/Legal các thông tin kỹ thuật cần thiết để lập thông báo: loại và phạm vi dữ liệu bị ảnh hưởng, thời điểm xảy ra và phát hiện, nguyên nhân sơ bộ, biện pháp đã và sẽ áp dụng để khắc phục và giảm thiểu hậu quả.

> **Không lặp lại nội dung của SDGP:** Các yêu cầu về SDLC, peer review kỹ thuật, phân tách trách nhiệm, cơ chế ngoại lệ chung và quản lý không tuân thủ đã quy định đầy đủ tại SDGP. Policy này chỉ bổ sung phần chuyên sâu về bảo vệ dữ liệu cá nhân; khi có xung đột hoặc trùng lặp diễn giải với phần chung, bản quy định tại SDGP được ưu tiên áp dụng.

6. Vai trò và trách nhiệm

ROLES & RESPONSIBILITIES

- **Data Protection Officer (DPO) / Head of Legal-Compliance:** sở hữu Policy này; đầu mối đánh giá và gửi thông báo vi phạm dữ liệu cá nhân cho cơ quan quản lý; tư vấn pháp lý về Nghị định 13/2023/NĐ-CP (bao gồm chuyển dữ liệu ra nước ngoài) cho các đội phát triển.
- **Engineering Governance Council:** phê duyệt Policy và các sửa đổi; giải quyết xung đột giữa yêu cầu bảo vệ dữ liệu và tiến độ sản phẩm khi cần.
- **Head of Engineering / Kiến trúc sư:** bảo đảm data minimization và Privacy by Design được đưa vào chuẩn thiết kế hệ thống; phê duyệt kết quả DPIA trước khi phát triển.
- **Đội phát triển (Engineering Teams):** thực hiện phân loại dữ liệu, data masking, mã hóa, retention/xóa dữ liệu theo Điều 5; báo cáo ngay khi phát hiện nghi ngờ vi phạm dữ liệu cá nhân.
- **DevOps/Nền tảng:** vận hành pipeline masking dữ liệu khi sao chép giữa môi trường; quản lý khóa mã hóa và cơ chế xóa dữ liệu tự động; vận hành công cụ quét dữ liệu cá nhân/secret trong CI/CD.

7. Đo lường tuân thủ

COMPLIANCE MEASUREMENT

- Tỷ lệ hệ thống xử lý dữ liệu cá nhân đã có tài liệu phân loại dữ liệu (data inventory) đầy đủ theo Điều 5.1.
- Số lần phát hiện dữ liệu production thật tồn tại trong môi trường non-production khi kiểm tra/audit.
- Tỷ lệ tính năng/hệ thống rủi ro cao có DPIA hoàn thành trước khi phát triển, theo Điều 5.6.
- Số yêu cầu thực hiện quyền của chủ thể dữ liệu (truy cập/chỉnh sửa/xóa/rút đồng ý) được đáp ứng đúng hạn.
- Thời gian trung bình từ khi phát hiện đến khi báo cáo nội bộ một nghi ngờ vi phạm dữ liệu cá nhân, đối chiếu với hạn 72 giờ tại Điều 5.8.

8. Cơ chế ngoại lệ

EXCEPTIONS

Áp dụng theo đúng cơ chế và giới hạn tại Engineering Constitution, Điều 8 và SDGP, Điều 8. Riêng ngoại lệ liên quan đến dùng dữ liệu thật ngoài môi trường production (Điều 5.2) hoặc bỏ qua mã hóa dữ liệu nhạy cảm (Điều 5.4) **PHẢI (MUST)** có ý kiến chấp thuận của Document Owner (DPO/Legal), không chỉ đơn thuần phê duyệt kỹ thuật.

9. Không tuân thủ

NON-COMPLIANCE

Áp dụng theo đúng nguyên tắc tại SDGP, Điều 9: báo cáo và khắc phục cho vi phạm thông thường; chỉ xem xét kỷ luật lao động — qua HR/Pháp chế, theo Nội quy lao động — đối với hành vi cố ý (ví dụ: cố tình sao chép dữ liệu production thật vào môi trường test để "tiện việc", hoặc che giấu sự cố lộ dữ liệu cá nhân thay vì báo cáo theo Điều 5.8).

10. Chủ sở hữu tài liệu và chu kỳ rà soát

DOCUMENT OWNERSHIP & REVIEW CYCLE

Document Owner: [Data Protection Officer (DPO) / Head of Legal-Compliance], phối hợp Head of Engineering. Chu kỳ rà soát: hằng năm, hoặc ngay khi có thay đổi đáng kể về pháp luật bảo vệ dữ liệu cá nhân (ví dụ văn bản sửa đổi/thay thế Nghị định 13/2023/NĐ-CP) hoặc khi phát sinh sự cố dữ liệu cá nhân nghiêm trọng.

11. Tài liệu liên quan

RELATED DOCUMENTS

- Engineering Constitution v1.0, Software Development Governance Policy v1.0 (Tầng 1-2)
- Secure Software Development Policy, Data Classification Standard, Data Retention Standard, Encryption Standard (Tầng 3)
- Data Protection Impact Assessment (DPIA) Procedure/Template, Data Subject Request Handling Procedure, Data Breach Notification Procedure, Cross-Border Data Transfer Procedure (Tầng 4/5)

Dữ liệu cá nhân không phải nguyên liệu miễn phí để kiểm thử cho nhanh;
môi trường thấp hơn production không đồng nghĩa với rủi ro thấp hơn cho chủ thể dữ liệu;
mỗi trường dữ liệu thu thập thêm là một trách nhiệm thêm phải bảo vệ và một ngày phải xóa đi;
và quyền của chủ thể dữ liệu phải khả thi trên hệ thống thật, không chỉ tồn tại trên giấy.

12. Phê duyệt

APPROVAL

Vai trò	Họ tên	Chữ ký	Ngày
Chair, Engineering Governance Council			
Chief Technology Officer			
Data Protection Officer / Head of Legal-Compliance (Document Owner)			
Head of Engineering			