ISOCENTER INDONESIA

PRIVACY ENGINEERING 101:

Merancang Sistem yang Data-Centric & Compliance-Ready

20250429-00

Bagian I

Pendahuluan

Apa itu Privacy Engineering?

"A set of engineering processes, responsibilities, and technical methods to ensure that privacy requirements are systematically identified, analyzed, and built into systems and technologies." *(Sumber: Spiekermann, Sarah. "Engineering Privacy." IEEE Transactions on Software Engineering, 2012.)*

Terjemahan kontekstual:

Privacy Engineering adalah pendekatan teknis untuk merancang dan membangun sistem yang secara inheren melindungi data pribadi dan memenuhi persyaratan perlindungan privasi sejak tahap desain.

IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 35, NO. 1, JANUARY/FEBRUARY 2009 67

Engineering Privacy

Sarah Spiekermann and Lorrie Faith Cranor, *Senior Member, IEEE*

Abstract—In this paper, we integrate insights from diverse islands of research on electronic privacy to offer a holistic view of privacy engineering and a systematic structure for the discipline's topics. First, we discuss privacy requirements grounded in both historic and contemporary perspectives on privacy. We use a three-layer model of user privacy concerns to relate them to system operations (data transfer, storage, and processing) and examine their effects on user behavior. In the second part of this paper, we develop guidelines for building privacy-friendly systems. We distinguish two approaches: "privacy-by-policy" and "privacy-by-architecture." The privacy-by-policy approach focuses on the implementation of the notice and choice principles of fair information practices, while the privacy-by-architecture approach minimizes the collection of identifiable personal data and emphasizes anonymization and client-side data storage and processing. We discuss both approaches with a view to their technical overlaps and boundaries as well as to economic feasibility. This paper aims to introduce engineers and computer scientists to the privacy research domain and provide concrete guidance on how to design privacy-friendly systems.

Index Terms—Privacy, security, privacy-enhancing technologies, anonymity, identification.

1 Introduction

While privacy has long been heralded as a dead issue by some [1], [2], it is viewed as a key business requirement by others [3], [4]. New regulatory requirements and consumer concerns are driving companies to consider more privacy-friendly policies, but such policies often conflict with the desire to leverage customer data. The widespread adoption of loyalty card schemes and the rise of social network platforms suggest that some consumers are willing to sacrifice privacy for benefits they value. At the same time, perceived privacy breaches often result in consumer outcries. For example, the social networking website Facebook has repeatedly sparked protest from its users by introducing new services with privacy-invasive features turned on by default [5]. Negative news on privacy issues impact stock market valuation [6] and companies are confronted with expensive fines or settlements for privacy breaches [7], [8]. As a result, companies are increasingly unsure how critical customer privacy really is to their operations and sustainable market success.

Surveys suggest that individuals are deeply concerned about privacy. An increasing majority of US citizens say that existing laws and organizational practices do not provide a reasonable level of consumer privacy protection and that companies share personal information inappropriately [7], [9]. Even in Germany, which has the highest legal data protection standards worldwide [10], 47 percent of people do not believe their personal data is adequately protected [11].

While there is evidence that consumers may not always act on their privacy concerns [12], [13], there is convincing data to suggest that these concerns have some impact on consumer behavior and the acceptability and adoption of new technologies. A 2005 survey conducted by Privacy & American Business found that concerns about the use of personal information led 64 percent of respondents to decide not to purchase something from a company [14]. In many countries, new privacy regulations as well as media attention are increasing public awareness of privacy. For example, a 2004 analysis by the European press on radio frequency identification technology (RFID) revealed that about one-third of media messages about the new technology were related to consumer privacy fears [15]. Laboratory studies have shown that, when privacy information is readily available in search results, some consumers will pay a small premium to shop at websites with good privacy policies [16]. Against this background, privacy is a highly relevant issue in systems engineering today.

Despite increasing consciousness about the need to consider privacy in technology design, engineers have barely recognized its importance. Lahlou et al. [17] found that, when engineers were asked about privacy issues as related to prototype development, the issues were viewed either as "an abstract problem, not an immediate problem, not a problem at all (firewalls and cryptography would take care of it), not their problem (one for politicians, lawmakers, or society), or simply not part of the project deliverables." Conversely, privacy-conscious engineers often strive for extremely high degrees of privacy protection that may lead to mechanisms that undermine system usability [18], [19].

In the privacy research literature, we observe two areas of work with seemingly very different goals. The first area includes research aimed at developing cryptographic privacy protections and systems with provable privacy guarantees (JAP [20], Tor [21], and work on differential privacy [22]). Researchers in this area work under a threat model that assumes sophisticated adversaries who will not be deterred by policies or regulations, or regard states and

- S. Spiekermann is with the Institute of Information Systems, Humboldt University Berlin, Spandauer Strasse 1, 10178 Berlin, Germany. E-mail: sspiekl@wiwi.hu-berlin.de.
- L.F. Cranor is with Carnegie Mellon University, 4720 Forbes Ave., Pittsburgh, PA 15213. E-mail: lorrie@cmu.edu.

Manuscript received 17 Jan. 2008; revised 3 Sept. 2008; accepted 16 Sept. 2008; published online 25 Oct. 2008.
Recommended for acceptance by P. McDaniel.
For information on obtaining reprints of this article, please send e-mail to: tse@computer.org, and reference IEEECS Log Number TSE-2008-01-0018.
Digital Object Identifier no. 10.1109/TSE.2008.88.

Published by the IEEE Computer Society

Mengapa Privacy Engineering Penting?

Sarah Spiekermann-Hoff, Ph.D.

- Isu privasi pada saat itu (dan sampai sekarang) sering **hanya dianggap tugas hukum atau kebijakan perusahaan, bukan benar-benar dirancang untuk menjaga privasi**.
- Akibatnya, sistem informasi banyak yang gagal melindungi privasi pengguna secara efektif, karena privasi tidak dibangun sejak tahap desain teknis.
- Oleh karena itu, ia mengajukan konsep bahwa **privasi harus menjadi bagian dari rekayasa sistem itu sendiri** – itulah inti dari Privacy Engineering.

Tiga Privacy Layer menurut Spiekermann

Agar efektif, organisasi harus menerapkan di tiga level pengendalian sebagai berikut:

Level	Fokus	Contoh
Social Level	Nilai-nilai etis, ekspektasi sosial terhadap privasi.	Hak pengguna untuk mengontrol data pribadinya.
Organizational Level	Kebijakan organisasi, standar internal, governance, compliance.	Kebijakan internal soal data retention sesuai ketentuan yang berlaku.
Technical Level	Arsitektur sistem, coding, protokol teknis.	Implementasi enkripsi, pseudonymization.

Fokus

Tahapan Privacy Engineering

Tahapan/Elemen	Penjelasan
1. Privacy Requirements Analysis	Mengidentifikasi dan menganalisis kebutuhan privasi dari hukum, etika, ekspektasi sosial, bisnis, ataupun standar yang diadopsi oleh organisasi.
2. Privacy Design Strategies	Menyusun pendekatan teknis dan arsitektur untuk memenuhi kebutuhan privasi tersebut.
3. Privacy-Enhancing Technologies (PETs)	Menerapkan teknologi nyata untuk melindungi data, misal: enkripsi, anonymization, access control.
4. System Validation	Menguji dan memverifikasi bahwa sistem benar-benar melindungi privasi seperti yang direncanakan.

Tahapan Privacy Engineering dalam SDLC

Fase SDLC	Elemen Privacy Engineering	Contoh Aktivitas Utama
Requirements Gathering	Privacy Requirements Analysis	Identifikasi kebutuhan privasi dari hukum, sosial, dan bisnis.
System Design	Privacy Design Strategies	Menyusun pendekatan desain teknis untuk memenuhi kebutuhan privasi.
Development (Coding)	Privacy-Enhancing Technologies (PETs)	Implementasi PETs: enkripsi, pseudonymization, access control.
Testing	System Validation	Privacy Testing dan Compliance Validation untuk memastikan sistem memenuhi persyaratan privasi.
Deployment	System Validation (Final Review)	Final confirmation bahwa privasi terjaga saat sistem go-live.
Maintenance	Privacy Monitoring & Updates	Audit, monitoring privasi, Privacy Impact Assessment untuk perubahan sistem.

Bagian II

Privacy Requirements Analysis

Pengertian Privacy Requirements Analysis

- Privacy Requirements Analysis merupakan: Tahapan sistematis dalam proses Privacy Engineering yang bertujuan untuk mengidentifikasi, memahami, dan merumuskan kebutuhan perlindungan privasi yang harus dipenuhi dalam pengembangan sistem informasi.
- Pada tahapan ini, kebutuhan privasi tidak hanya diidentifikasi berdasarkan regulasi hukum, tetapi juga mempertimbangkan ekspektasi sosial, kebijakan organisasi, serta potensi ancaman terhadap data pribadi.

Pentingnya Privacy Requirements Analysis

Privacy Requirements Analysis memiliki peranan krusial karena:

- Menjamin bahwa perlindungan privasi **menjadi bagian integral sejak tahap awal perancangan system.**
- Memastikan **kesesuaian sistem terhadap ketentuan hukum yang berlaku** seperti UU Perlindungan Data Pribadi (UU PDP) dan regulasi lainnya.
- **Mengurangi risiko reputasi dan biaya tinggi** akibat perbaikan sistem akibat "salah desain" di kemudian hari.
- Membangun kepercayaan pengguna terhadap pengelolaan data pribadi.

Dengan demikian, Privacy Requirements Analysis berfungsi sebagai landasan dalam memastikan sistem memenuhi *prinsip privacy by design*.

Tahapan Privacy Requirements Analysis

Aktivitas	Penjelasan
Identifikasi Persyaratan Hukum	Menelaah dan memahami ketentuan hukum terkait perlindungan data pribadi yang berlaku, baik nasional maupun internasional.
Identifikasi Ekspektasi Pemangku Kepentingan	Menggali harapan pengguna, masyarakat, dan pihak lain yang relevan terhadap perlindungan data dan hak privasi mereka.
Identifikasi Kebijakan Organisasi	Mengkaji kebijakan internal perusahaan atau institusi yang berkaitan dengan pengelolaan dan perlindungan data pribadi.
Identifikasi Ancaman Kontekstual	Menganalisis potensi ancaman terhadap privasi berdasarkan karakteristik sistem dan lingkungannya.
Transformasi ke Persyaratan Teknis	Menerjemahkan kebutuhan hukum, sosial, dan organisasi ke dalam bentuk spesifikasi teknis yang dapat diimplementasikan.

Keluaran Utama Privacy Requirements Analysis

Dokumen/Daftar Persyaratan Privasi yang memuat daftar kebutuhan privasi yang harus dipenuhi system yang disertai dengan prioritas dan metode implementasi teknis yang direncanakan.

Contoh Daftar Persyaratan Privasi (1)

No	Persyaratan Privasi	Sumber	Prioritas	Alasan Prioritas
1	Data pribadi pengguna hanya boleh dikumpulkan berdasarkan persetujuan eksplisit dan terpisah dari persyaratan layanan.	UU PDP Pasal 20, Kebijakan Internal Perlindungan Data XYZ Bab II.3	Tinggi	Persetujuan eksplisit merupakan dasar sah pengolahan data, pelanggaran berisiko sanksi berat.
2	Pengguna harus dapat mengajukan permintaan penghapusan data pribadi kapan saja.	UU PDP Pasal 5 huruf f, Kebijakan Penghapusan Data XYZ Bab IV.2	Tinggi	Hak pengguna utama menurut UU PDP, wajib diakomodasi untuk menghindari pelanggaran hak individu.
3	Semua data pribadi harus dienkripsi selama penyimpanan dan transmisi.	UU PDP Pasal 35, Kebijakan Keamanan Informasi XYZ Bab III.5	Tinggi	Keamanan data adalah kewajiban hukum dan best practice TI; kegagalan berisiko besar.

Contoh Daftar Persyaratan Privasi (2)

No	Persyaratan Privasi	Sumber	Prioritas	Alasan Prioritas
4	Pengumpulan data dibatasi hanya pada data minimal yang diperlukan untuk keperluan transaksi.	UU PDP Pasal 16, Kebijakan Data Minimization XYZ Bab II.2	Sedang	Minimalisasi data mengurangi risiko kebocoran, tetapi dampak hukum langsung relatif lebih kecil.
5	Jika terjadi insiden kebocoran data pribadi, pemberitahuan kepada pengguna harus dilakukan paling lambat 72 jam setelah diketahui.	UU PDP Pasal 46, Kebijakan Manajemen Insiden Keamanan Data XYZ Bab V.4	Tinggi	Kewajiban hukum dengan tenggat waktu ketat; keterlambatan dapat dikenakan sanksi.
6	Penggunaan cookie untuk keperluan selain operasional inti harus mendapat persetujuan pengguna.	UU PDP Pasal 23, Kebijakan Cookie Management XYZ Bab III.1	Sedang	Wajib berdasarkan regulasi, namun risiko hukum lebih moderat dibanding pelanggaran data sensitif.

Contoh Daftar Persyaratan Privasi (3)

No	Persyaratan Privasi	Sumber	Prioritas	Alasan Prioritas
7	Akses ke data pribadi dalam sistem internal dibatasi berdasarkan prinsip *least privilege* dan diaudit secara berkala.	UU PDP Pasal 38, Kebijakan Akses Data XYZ Bab III.7	Tinggi	Pembatasan akses krusial untuk mencegah risiko kebocoran internal.
8	Pengguna harus diberikan informasi yang mudah dipahami mengenai bagaimana data mereka digunakan, disimpan, dan dilindungi.	UU PDP Pasal 9, Kebijakan Komunikasi Privasi XYZ Bab II.5	Sedang	Meningkatkan transparansi dan kepercayaan pengguna; penting, namun urgensi hukum lebih moderat.

Bagian III

Privacy Design Strategies

Pengertian Privacy Design Strategies

- Privacy Design Strategy adalah pendekatan sistematis dalam **merancang arsitektur dan fungsi sistem teknologi informasi dengan tujuan utama untuk memastikan bahwa kebutuhan privasi yang telah diidentifikasi dipenuhi sejak tahap desain awal**.
- Dengan kata lain, ini **adalah kerangka pikir dan pendekatan teknis** untuk:
  - ✓ Menerjemahkan kebutuhan privasi (yang dihasilkan dari Privacy Requirements Analysis), dan
  - ✓ Menjadi keputusan desain sistem yang nyata dan dapat diimplementasikan.

Prinsip Umum dalam Privacy Design Strategy

Prinsip	Penjelasan
Data Minimization	Mengumpulkan, memproses, dan menyimpan sesedikit mungkin data pribadi.
Purpose Limitation	Data pribadi hanya digunakan untuk tujuan spesifik yang disetujui pengguna.
Security by Design	Mengintegrasikan langkah-langkah keamanan data sejak tahap desain sistem.
Transparency	Membuat penggunaan data pribadi menjadi dapat dipahami dan dilacak oleh pengguna.
User Control	Memberikan kendali kepada pengguna atas bagaimana data mereka dikumpulkan, digunakan, dan dihapus.
Accountability	Memastikan bahwa organisasi dapat membuktikan bahwa sistem telah dirancang dengan perlindungan privasi yang memadai.

Pendekatan dalam Privacy Design Strategies

a) Strategi Data-Oriented: Fokus pada **pengelolaan data pribadi itu sendiri**:

- **Minimize**: Jangan mengumpulkan data yang tidak perlu.
- **Hide**: Enkripsi, pseudonymization, atau anonymization untuk melindungi data.
- **Separate**: Simpan data secara terpisah untuk meminimalkan korelasi yang tidak diinginkan.
- **Aggregate**: Gunakan data agregat atau ringkasan jika memungkinkan, daripada data individual.

b) Strategi Process-Oriented: Fokus pada **proses pengolahan dan kontrol data**:

- **Inform**: Pastikan pengguna mengetahui bagaimana data mereka digunakan.
- **Control**: Berikan mekanisme bagi pengguna untuk mengelola preferensi privasi mereka.
- **Enforce**: Pastikan semua kebijakan privasi ditegakkan secara teknis.
- **Demonstrate**: Siapkan dokumentasi dan audit trail yang menunjukkan kepatuhan.

Contoh Penerapan Privacy Design Strategies (1)

No	Privacy Design Requirement	Design Principle yang Relevan	Strategi Implementasi
1	Data pribadi harus terlindungi selama penyimpanan dan transmisi.	**Hide**	Menerapkan mekanisme perlindungan data seperti enkripsi dan pseudonymization untuk menyembunyikan informasi dari pihak tidak berwenang.
2	Pengguna memiliki hak untuk menghapus seluruh data pribadinya.	**Control**	Menyediakan kontrol penuh kepada pengguna untuk mengelola dan menghapus data yang tersimpan di sistem kapan pun diperlukan.
3	Data pribadi yang dikumpulkan harus dibatasi hanya pada informasi yang diperlukan.	**Minimize**	Mendesain formulir dan alur bisnis agar hanya mengumpulkan data esensial untuk keperluan layanan, menghindari pengumpulan data berlebih.

Contoh Penerapan Privacy Design Strategies (2)

No	Privacy Design Requirement	Design Principle yang Relevan	Strategi Implementasi
4	Pengguna harus diberi informasi yang jelas tentang penggunaan data mereka.	**Inform**	Menyediakan kebijakan privasi dan notifikasi yang ringkas, jelas, dan mudah dipahami mengenai bagaimana data dikumpulkan, diproses, dan dibagikan.
5	Akses terhadap data pribadi internal harus dibatasi secara ketat berdasarkan kebutuhan pekerjaan.	**Enforce**	Menerapkan kebijakan akses berbasis peran (role-based access control) dan audit internal untuk menegakkan pembatasan akses.
6	Data harus diproses sedemikian rupa sehingga sulit untuk mengidentifikasi individu bila tidak diperlukan.	**Separate / Aggregate**	Mengelola data dengan teknik pemisahan basis data (separate storage) atau penggunaan data agregat untuk analisis tanpa mengidentifikasi individu.

Bagian IV

Privacy-Enhancing Technologies (PETs)

Pengertian PETs

Privacy-Enhancing Technologies (PETs) adalah **sekumpulan alat, metode, dan teknologi yang dirancang untuk melindungi data pribadi** dan meminimalkan risiko privasi ketika data diproses, disimpan, atau ditransmisikan.

Tujuan utama PETs:

- Melindungi hak privasi individu.
- Memastikan kepatuhan terhadap regulasi perlindungan data.
- Mengurangi jumlah data pribadi yang terekspos atau dikumpulkan.

PETs adalah teknologi nyata yang digunakan untuk mengimplementasikan strategi perlindungan privasi dalam sistem.

Peran PETs

PETs digunakan untuk:

- **Menerjemahkan prinsip dan strategi privasi** (seperti Hide, Minimize, Control) menjadi tindakan teknis nyata.
- **Memberikan proteksi teknis** terhadap data di sepanjang siklus hidupnya (collection, processing, storage, transmission, deletion).
- Membantu organisasi **membuktikan keptuhan secara teknis** terhadap hukum seperti UU PDP dan persyaratan kepatuhan lainnya.

PETs itu jawaban teknis dari "bagaimana secara konkrit kita mewujudkan privacy by design".

Beberapa Metode Umum PETs

Metode	Penjelasan	Contoh Teknologi
Data Anonymization	Menghapus atau mengubah data identitas supaya individu tidak bisa dikenali.	K-anonymity, differential privacy, data masking.
Encryption	Melindungi data dengan kode rahasia, hanya bisa dibaca oleh pihak yang berwenang.	AES-256 (storage encryption), TLS 1.3 (transport encryption).
Access Control	Mengatur siapa yang boleh mengakses data dan apa yang boleh mereka lakukan.	Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC).
Pseudonymization	Mengganti identitas asli dengan pengenal lain yang tidak langsung menunjuk individu.	Tokenization (mengganti kartu kredit dengan token), pseudonym databases.
Secure Multi-Party Computation (SMPC)	Memungkinkan analisis data bersama tanpa mengungkapkan data masing-masing pihak.	Kriptografi SMPC dalam sistem keuangan atau data medis bersama.
Zero Knowledge Proofs (ZKP)	Membuktikan suatu klaim benar tanpa mengungkapkan data sebenarnya.	Verifikasi identitas tanpa mengungkapkan password.
Privacy-Preserving Data Mining	Menambang pola dari data tanpa mengekspos data mentahnya.	Federated Learning (seperti yang digunakan Google dalam pengembangan model AI).
Auditing & Logging	Mencatat semua aktivitas terhadap data untuk transparansi dan pelacakan pelanggaran.	Immutable audit logs, blockchain-based audit trails.

Contoh Penerapan PETs (1)

1	Privacy Design Requirement	Design Principle	Strategi Implementasi	Contoh PETs	Alasan Pemilihan Contoh PETs
1	Data pribadi harus terlindungi selama penyimpanan dan transmisi.	Hide	Menerapkan perlindungan data melalui enkripsi dan pseudonymization.	- **AES-256 Encryption**	- **AES-256** dipilih karena standar industri untuk enkripsi data dengan keamanan sangat tinggi.
				- **TLS 1.3**	- **TLS 1.3** digunakan karena versi terbaru ini mempercepat koneksi dan menghilangkan kerentanan yang ada di TLS 1.2.
2	Pengguna memiliki hak untuk menghapus seluruh data pribadinya.	Control	Menyediakan kontrol penuh kepada pengguna untuk penghapusan data.	- **Data Deletion API**	- **Data Deletion API** memungkinkan penghapusan otomatis dan terdokumentasi di backend.
				- **Consent Management Platform**	- **Consent Management Platform** mendukung pencatatan persetujuan sekaligus penghapusan berbasis permintaan pengguna.

Contoh Penerapan PETs (2)

No	Privacy Design Requirement	Design Principle	Strategi Implementasi	Contoh PETs	Alasan Pemilihan Contoh PETs
3	Data pribadi yang dikumpulkan harus dibatasi hanya pada informasi yang diperlukan.	Minimize	Mendesain formulir dan proses bisnis agar hanya mengumpulkan data esensial.	- **Data Minimization Engine**	- **Data Minimization Engine** digunakan untuk memfilter input data sesuai kebutuhan minimal bisnis.
				- **Selective Disclosure Protocols**	- **Selective Disclosure** memungkinkan pengguna hanya mengungkapkan sebagian informasi saat diperlukan.
4	Pengguna harus diberi informasi yang jelas tentang penggunaan data mereka.	Inform	Menyediakan kebijakan privasi dan pemberitahuan yang jelas.	- **Privacy Notice Generator**	- **Privacy Notice Generator** memudahkan pembuatan kebijakan yang sesuai hukum dan user-friendly.
				- **Consent Tracking Tools**	- **Consent Tracking Tools** memungkinkan organisasi membuktikan persetujuan yang sah kapan saja.

Contoh Penerapan PETs (3)

No	Privacy Design Requirement	Design Principle	Strategi Implementasi	Contoh PETs	Alasan Pemilihan Contoh PETs
5	Akses terhadap data pribadi internal harus dibatasi berdasarkan kebutuhan pekerjaan.	Enforce	Menerapkan kebijakan akses berbasis peran dan audit internal.	- **Role-Based Access Control (RBAC)**	- **RBAC** membatasi akses hanya kepada pihak berwenang berdasarkan jabatan/tugas.
				- **Immutable Audit Logs**	- **Immutable Audit Logs** memastikan semua aktivitas akses tercatat permanen dan tidak dapat diubah.
6	Data harus diproses sehingga sulit untuk mengidentifikasi individu bila tidak diperlukan.	Separate / Aggregate	Mengelola data melalui pemisahan dan agregasi.	- **Data Anonymization Tools**	- **Data Anonymization Tools** digunakan untuk menghapus elemen identifikasi langsung.
				- **Differential Privacy Algorithms**	- **Differential Privacy** memungkinkan analisis data agregat dengan jaminan bahwa individu tidak dapat dikenali secara statistik.

Bagian V

System Validation

Pengertian System Validation

System Validation adalah **tahap di mana sistem yang telah dibangun diuji dan diverifikasi** untuk memastikan bahwa semua kebutuhan perlindungan privasi yang dirancang dan diimplementasikan benar-benar berjalan dengan efektif.

Tujuannya:

- **Memastikan bahwa semua Privacy Requirements telah terpenuhi**.
- Menguji bahwa Privacy Design Strategies dan Privacy-Enhancing Technologies (PETs) **bekerja sebagaimana mestinya**.
- **Menemukan dan memperbaiki kekurangan** sebelum sistem dioperasikan penuh (go-live).

Aktivitas Utama System Validation

Aktivitas	Penjelasan
Privacy Testing	Menguji fitur-fitur yang terkait privasi: misal, hak hapus data, data minimization, pengendalian akses, enkripsi.
Security Testing Fokus Privasi	Uji kerentanan khusus yang bisa membocorkan data pribadi: misal, improper access control, insecure storage.
Validation Against Requirements	Memastikan bahwa semua Privacy Requirements yang telah disusun di awal dipenuhi secara lengkap.
Privacy Impact Assessment (PIA)	Menilai kembali apakah sistem menghadirkan risiko baru terhadap privasi dan apakah mitigasi sudah cukup.
Audit Readiness Review	Menyiapkan bukti-bukti teknis dan dokumentasi untuk audit internal atau eksternal tentang privasi.

Contoh Skrip Pengujian

Area yang Diuji	Skrip Pengujian
Hak Subjek Data	Apakah pengguna dapat mengakses, mengubah, dan menghapus data mereka?
Data Minimization	Apakah hanya data yang diperlukan yang dikumpulkan dan disimpan?
Enkripsi	Apakah data dienkripsi saat disimpan dan saat ditransmisikan?
Access Control	Apakah hanya pihak berwenang yang bisa mengakses data pribadi?
Audit Logging	Apakah semua akses dan perubahan data pribadi tercatat dengan benar?
Data Sharing	Apakah ada kontrol ketat atas berbagi data dengan pihak ketiga?

Bagian VI

Kesimpulan

Kesimpulan

- Privacy Engineering adalah penerapan perlindungan data pribadi melalui proses teknis terstruktur.
- Dimulai dengan Privacy Requirements Analysis untuk mengidentifikasi kebutuhan privasi.
- Dilanjutkan dengan Privacy Design Strategies untuk merancang solusi berbasis prinsip privasi.
- Privacy-Enhancing Technologies (PETs) diterapkan untuk melindungi data secara teknis.
- System Validation dilakukan untuk memastikan sistem memenuhi kebutuhan privasi.
- Privacy Engineering harus diintegrasikan dalam seluruh fase SDLC.
- Tujuannya adalah mencapai Privacy by Design dan Privacy by Default secara nyata.

About Us

ISO CENTER INDONESIA adalah penyedia layanan terkait ISO dan Sistem Manajemen yang komprehensif. Kami adalah The Ultimate ISO and Management System Resources yang siap meningkatkan kinerja organisasi Anda melalui penyediaan informasi, pelatihan, implementasi, dan asesmen standar internasional berbasis ISO dan sistem manajemen yang efektif, efisien, out of the box, dan menggunakan metode terkini yang di-enable oleh teknologi dan AI.Jangan lupa untuk selalu kunjungi situs kami dan mengakses tautan Articles yang memuat kajian-kajian terkini kami dan Download yang berisi video-video pembalajaran, e-book hasil riset kami, dan alat-alat bantu yang berupa kertas-kertas kerja dan template yang selau kami kinikan.

Semua itu kami persembahkan untuk Anda!

ISOCENTER INDONESIA

Thank You!

ISO Center Indonesia (Jakarta)

Permata Kuningan Building
17th Floor, HR Rasuna Said.
Kuningan Mulia, Menteng Atas,
Setia Budi, South Jakarta City,
Jakarta 12920

East Office (Surabaya)

AMG Tower Lantai 17,
Jl. Raya Dukuh Menanggal
No 1A, East Java, Gayungan
Surabaya, Indonesia 60234

Contact Us :

Website : https://isoindonesiacenter.com/
email : admin@isoindonesiacenter.com
telepon : +62 813-184-5942 (Sinthia - WhatsApp/Call)
+62 895-2956-5008 (Louqman – WhatsApp/Call)
+62 89-6551-88175 (Ardi - WhatsApp/Call)

ISOCENTER INDONESIA