CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Keamanan dan Pengelolaan Data

Minggu 5

Dosen Pengajar: Steven Bandong S.Si., M.T

Tata Tertib Kelas

- Dosen dan mahasiswa bersama-sama secara aktif membentuk komunitas belajar yang baik
- Silahkan bertanya kalau ada yang tidak dimengerti
- Laporan / program / tugas apa pun yang anda serahkan harus jelas beda dan jelas adalah kontribusi anda atau kelompok dan bukan dari orang lain (misnya: tugas proyek).

Topik Minggu Ini dan Capaian Pembelajaran

Topik minggu ini:

1. Menjelaskan Privasi by Design dan Privasi by Engineering
2. Panduan dan persayaratan Privasi Informasi

Indikator penilaian:

1. Ketepatan dalam menjelaskan konsep privasi
2. Memahami panduan dan persayaratan Privasi Informasi

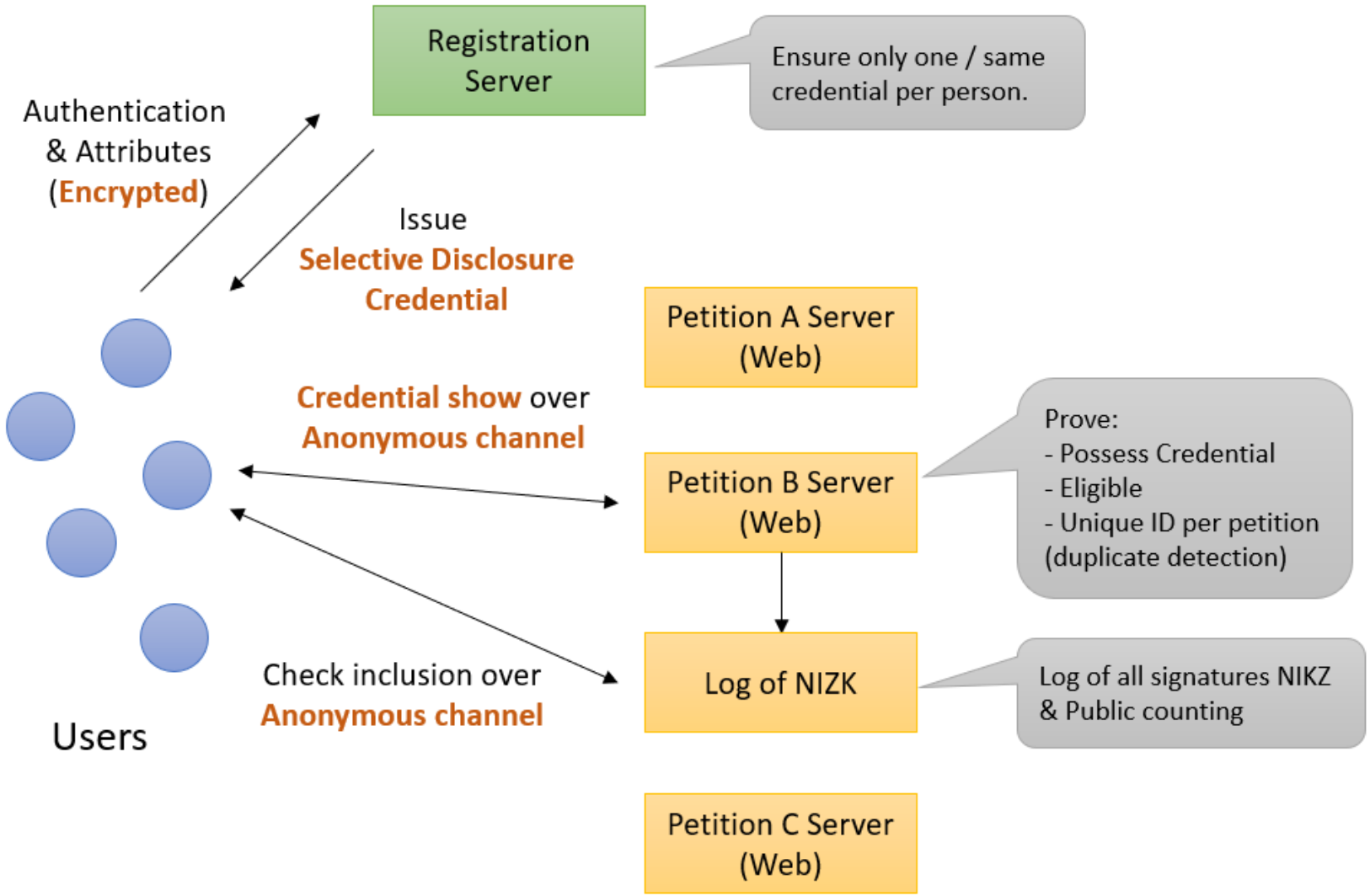
Case Study 1: e-petitions (Diaz et al. 2009)

- Petitions: a formal request to an authority.
  - E.g. EU Lisbon Treaty: 1M people across EU may request legislation.

- Two key risks:
  (1) Disclosure of who signed a petition (sensitive topics).
  (2) Discrimination or profiling on the basis of signing a petition.

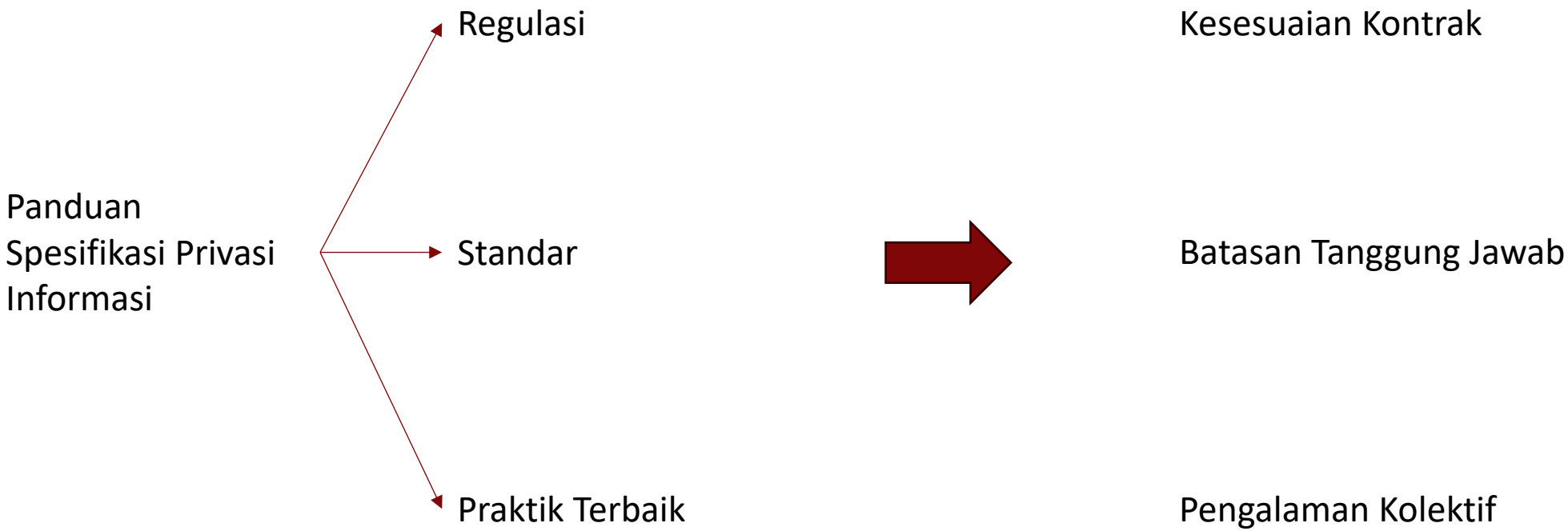
- Requirements:
  - “The signatures correspond to existing individuals.”
  - “Only individuals eligible to sign a petition are able to do so.”
  - “Each individual can sign a petition only once.”
  - “The number of signatures is correctly counted.”
  - Note: “identifiability not inherent” -> Principle of data minimization …

Case Study 1: e-petitions (Diaz et al. 2009)



Information Privacy Requirements and Guidelines

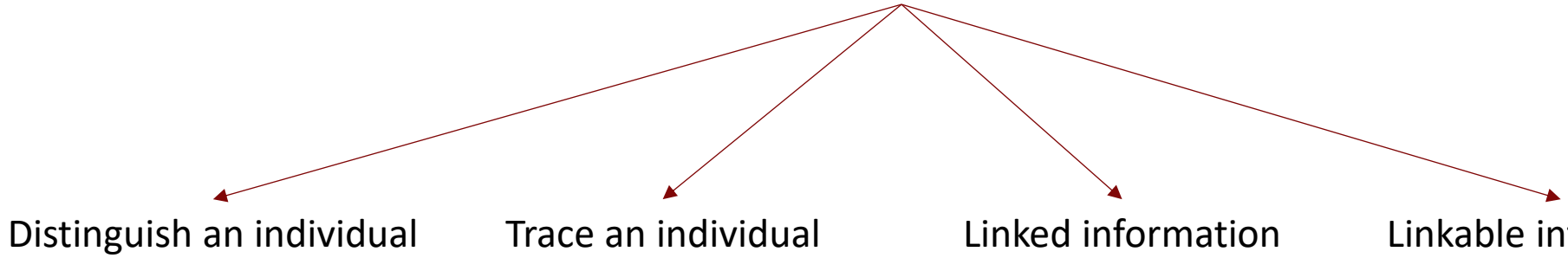
Spesifikasi Privasi Informasi



Data Pribadi

Setiap informasi tentang individu yang disimpan oleh lembaga, termasuk informasi yang dapat digunakan untuk membedakan atau menelusuri identitas individu, seperti nama, nomor jaminan sosial, tanggal dan tempat lahir, nama gadis ibu, atau catatan biometrik; serta informasi lain yang terkait atau dapat dihubungkan dengan individu, seperti informasi medis, pendidikan, keuangan, dan pekerjaan.

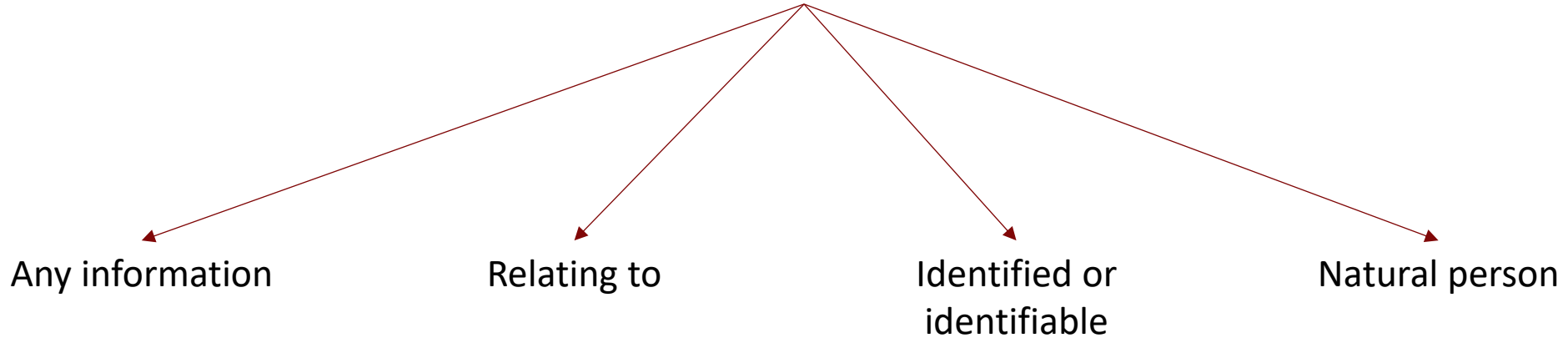
NIST SP 800-122



Data Pribadi

Setiap informasi terkait individu yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, termasuk nama, nomor identifikasi, lokasi, pengenal daring, atau faktor lain yang terkait dengan fisik, fisiologis, genetik, mental, ekonomi, budaya, atau identitas sosial seseorang.

Regulasi Uni Eropa (GDPR)



Sumber Informasi Identitas Pribadi (PII)

1. **Identifikasi yang Dikeluarkan Pemerintah:**
   Contoh: SIM, paspor, akta kelahiran, dan pengidentifikasi manfaat pensiun serta medis (misalnya, di Amerika Serikat: nomor Jaminan Sosial dan nomor Medicare).
2. **Informasi Kontak:**
   Contoh: Alamat email, alamat fisik, dan nomor telepon.
3. **Informasi Daring:**
   Contoh: Akun Facebook dan media sosial lainnya, kata sandi, dan PIN (nomor identifikasi pribadi).
4. **Data Geolokasi:**
   Contoh: Dari ponsel cerdas, perangkat GPS, dan kamera.
5. **Alamat Perangkat:**
   Contoh: Alamat IP dari perangkat yang terhubung ke Internet atau alamat kontrol akses media (MAC) perangkat yang terhubung ke jaringan lokal.
6. **Data Verifikasi:**
   Contoh: Nama gadis ibu, nama hewan peliharaan atau anak, dan nama sekolah menengah.
7. **Informasi Catatan Medis:**
   Contoh: Resep obat, catatan medis, hasil pemeriksaan, dan gambar medis.
8. **Informasi Biometrik dan Genetik:**
   Contoh: Sidik jari, pemindaian retina, dan DNA.
9. **Nomor Akun:**
   Contoh: Nomor rekening bank, asuransi, investasi, dan kartu debit/kredit.

Sensitivitas Informasi Identitas Pribadi (PII)

PII sensitive ➔ PII yang jika hilang, dikompromikan, atau diungkapkan tanpa izin dapat menyebabkan kerugian, ketidaknyamanan, rasa malu, atau ketidakadilan kepada individu.

Contoh PII Sensitif:

1. Nomor Jaminan Sosial.
2. Tempat/tanggal lahir.
3. Nama gadis ibu.
4. Informasi biometrik.
5. Data medis (kecuali referensi singkat).
6. Informasi keuangan pribadi.
7. Nomor kartu kredit/debit.
8. Nomor paspor.
9. Informasi pekerjaan sensitif (misalnya, hasil investigasi latar belakang).
10. Riwayat kriminal.
11. Informasi yang dapat menstigmatisasi atau berdampak buruk pada individu.

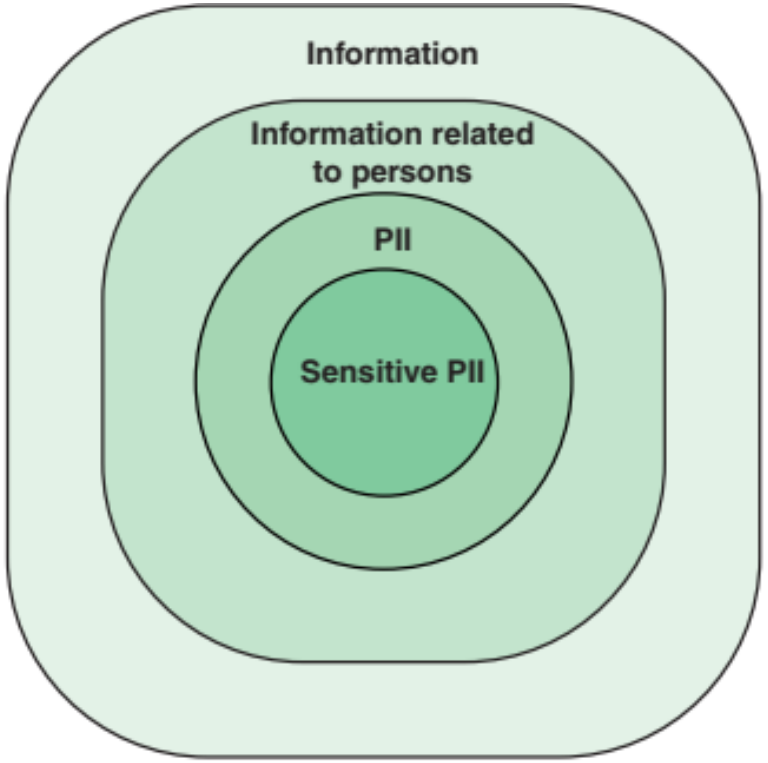
Contoh PII Tidak Sensitif:

1. Nama individu.
2. Alamat email kantor.
3. Alamat kerja.
4. Nomor telepon kerja.

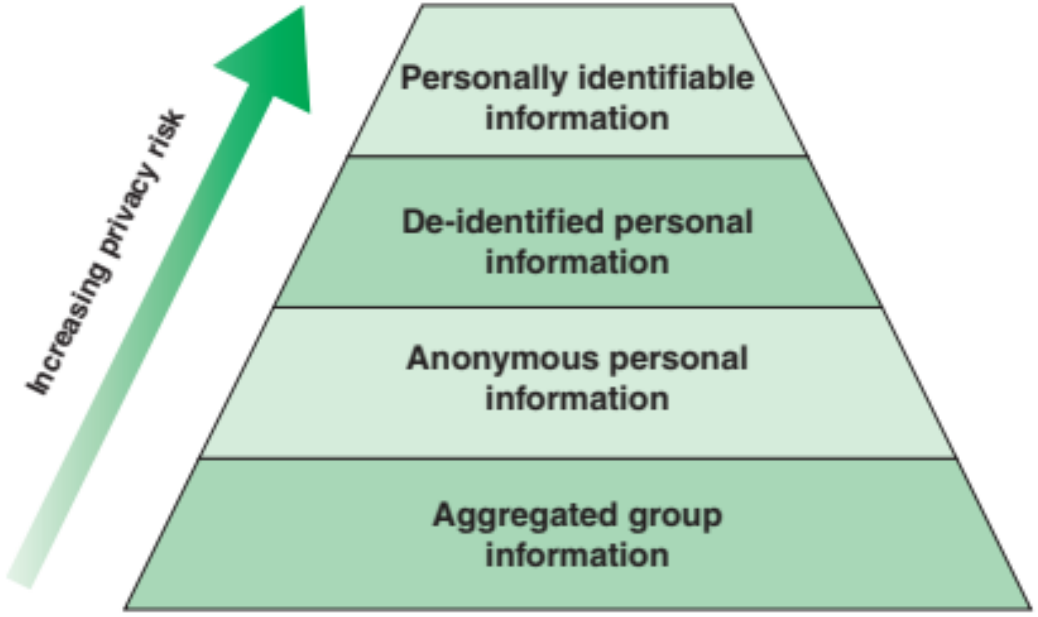
Konteks dan Sensitivitas:

Daftar nama pegawai biasa tidak dianggap sensitif, tetapi daftar pegawai penegak hukum

Sensitivitas Informasi Identitas Pribadi (PII)



Information and PII

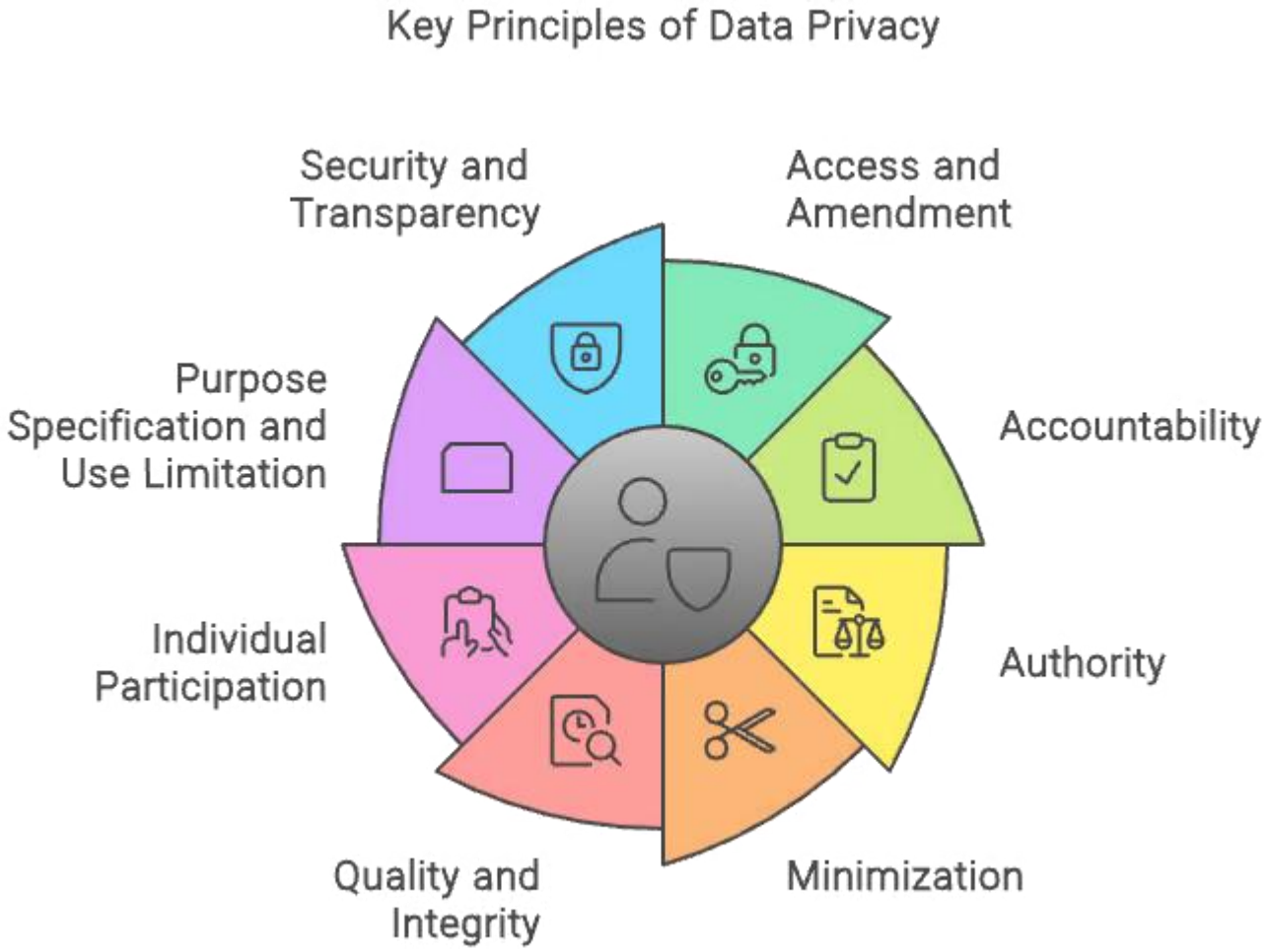


Degrees of Privacy Risk

Fair Information Practice Principles

Individu memiliki hak untuk berpartisipasi dalam pengelolaan informasi pribadi yang dapat diidentifikasi, termasuk menentukan isi dan penggunaannya.
Laporan tahun 1973 dari Departemen Kesehatan, Pendidikan, dan Kesejahteraan AS (HEW) yang berjudul Records, Computers, and the Rights of Citizens.

Pada tahun 1980, Organisasi untuk Kerja Sama dan Pembangunan Ekonomi (OECD) memperluas prinsip ini menjadi delapan prinsip yang dikenal sebagai OECD Fair Information Practice Principles



OECD Fair Information Practice Principles

Privacy Regulations

UNI EROPA

General Data Protection Regulation (GDPR),

Presentasi berjudul "10 Fakta Kunci yang Perlu Diketahui Bisnis tentang GDPR" dari European Identity & Cloud Conference tahun 2016 merangkum aspek-aspek penting GDPR

- **Berlaku Secara Global** – Semua perusahaan di dunia yang memproses data pribadi penduduk UE harus mematuhi GDPR.
- **Definisi Data Pribadi yang Lebih Luas** – GDPR memperluas cakupan data pribadi dibandingkan regulasi sebelumnya.
- **Aturan Ketat untuk Persetujuan** – Persetujuan pemrosesan data harus eksplisit, spesifik, dan diberikan secara sadar.
- **Penunjukan DPO** – Otoritas publik dan organisasi tertentu harus menunjuk **Data Protection Officer (DPO)**.

Privacy Regulations

UNI EROPA

General Data Protection Regulation (GDPR),

Presentasi berjudul "10 Fakta Kunci yang Perlu Diketahui Bisnis tentang GDPR" dari European Identity & Cloud Conference tahun 2016 merangkum aspek-aspek penting GDPR

- **Penilaian Dampak Privasi** – Organisasi wajib melakukan **privacy impact assessment** untuk mengidentifikasi risiko pelanggaran data.
- **Pelaporan Pelanggaran Data** – Insiden kebocoran data harus dilaporkan ke otoritas dalam waktu **72 jam**.
- **Hak untuk Dilupakan** – Individu dapat meminta penghapusan data pribadinya dari sistem organisasi.
- **Privasi Berdasarkan Desain** – Perlindungan data harus diterapkan sejak awal pengembangan sistem, bukan sebagai tambahan.

Privacy Regulations

U.S. Privacy Laws and Regulations

Tidak ada satu regulasi tunggal untuk privasi di AS, melainkan kumpulan undang-undang federal yang mencakup berbagai aspek, baik untuk lembaga pemerintah maupun sektor swasta.

- **Privacy Act (1974)** – Mengatur pengumpulan dan penggunaan data pribadi oleh lembaga federal.
- **FACTA (2003)** – Mencegah pencurian identitas dalam transaksi keuangan.
- **HIPAA (1996)** – Melindungi privasi data kesehatan.
- **FERPA (1974)** – Melindungi privasi catatan pendidikan siswa.
- **GLBA (1999)** – Menjaga keamanan data keuangan konsumen.
- **Federal Policy for Human Subjects (1991)** – Menetapkan prinsip etika dalam penelitian manusia.
- **COPPA** – Mengatur perlindungan data anak-anak di bawah 13 tahun secara online.
- **Electronic Communications Privacy Act** – Melarang akses ilegal terhadap komunikasi elektronik.
- **California Consumer Privacy Act (CCPA)** – Undang-undang privasi penting di California yang mengatur perlindungan data konsumen.

Privacy Regulations

Regulasi Privasi Data di Indonesia

Undang-Undang Perlindungan Data Pribadi (UU PDP) – 2022

- Setara dengan GDPR, mengatur hak pemilik data dan kewajiban pengelola data.
- Mengatur persetujuan eksplisit (*explicit consent*) untuk pengolahan data.
- Mewajibkan **penunjukan Pejabat Perlindungan Data (DPO)** untuk perusahaan yang memproses data dalam skala besar.
- **Sanksi**: Denda hingga **2% dari pendapatan tahunan** atau hukuman pidana untuk pelanggaran berat.

Privacy Regulations

Regulasi Privasi Data di Indonesia

Peraturan Menteri Kominfo No. 20 Tahun 2016

- Mengatur perlindungan data dalam sistem elektronik.
- Mewajibkan penyedia layanan untuk menyimpan data di dalam negeri.

Privacy Regulations

Regulasi Privasi Data di Indonesia

UU Informasi dan Transaksi Elektronik (UU ITE) – 2008 (Revisi 2016, 2020)

- Mengatur penggunaan dan penyalahgunaan data elektronik.
- Memuat sanksi pidana untuk pencurian atau penyalahgunaan data.

Privacy Regulations

Regulasi Privasi Data di Indonesia

Peraturan OJK No. 13 Tahun 2018

Mengatur keamanan data pribadi dalam layanan keuangan digital dan fintech.

Peraturan Bank Indonesia No. 22/2020

Mengatur data pribadi dalam sistem pembayaran dan transaksi digital.

Standar Privasi

- **Privasi dalam sistem informasi** melibatkan berbagai teknologi seperti **kriptografi, keamanan jaringan, keamanan basis data, dan deteksi malware**.
- Fokus privasi mencakup **penyimpanan data, komunikasi, keamanan aset, dan aspek hukum**.
- **Keamanan privasi harus sistematis**, bukan pendekatan ad hoc, untuk mencegah kegagalan.
- **ISO dan NIST** adalah standar utama yang memberikan panduan internasional untuk manajemen privasi.

Standar Privasi

International Organization for Standardization (ISO)

ISO adalah organisasi internasional yang mengembangkan standar, termasuk keamanan informasi.

ISO bekerja sama dengan IEC untuk mengembangkan standar dalam komunikasi data, jaringan, dan keamanan.

ISO 27000 adalah standar utama dalam manajemen keamanan informasi (ISMS), mencakup kebijakan dan prosedur perlindungan data.

Standar penting dalam ISO 27000:

- **ISO 27001** – Standar sertifikasi keamanan ISMS.
- **ISO 27002** – Kerangka kerja kontrol keamanan informasi.
- **ISO 27005** – Panduan manajemen risiko keamanan informasi.

ISO 27001 & 27002 menjadi standar global untuk **sertifikasi keamanan informasi**, meningkatkan kredibilitas dan kepatuhan hukum organisasi.

Standar Privasi

International Organization for Standardization (ISO)

ISO mengembangkan standar privasi tambahan untuk **seri ISO 27000**, terutama untuk perlindungan **data pribadi (PII)**:

1. **ISO 27701** – Ekstensi ISO 27001 & 27002 untuk **manajemen informasi privasi (PIMS)** dan sertifikasi perlindungan data.
2. **ISO 27018** – Panduan perlindungan **PII dalam layanan cloud publik**.

Selain itu, **seri ISO 29100** memberikan pedoman spesifik:

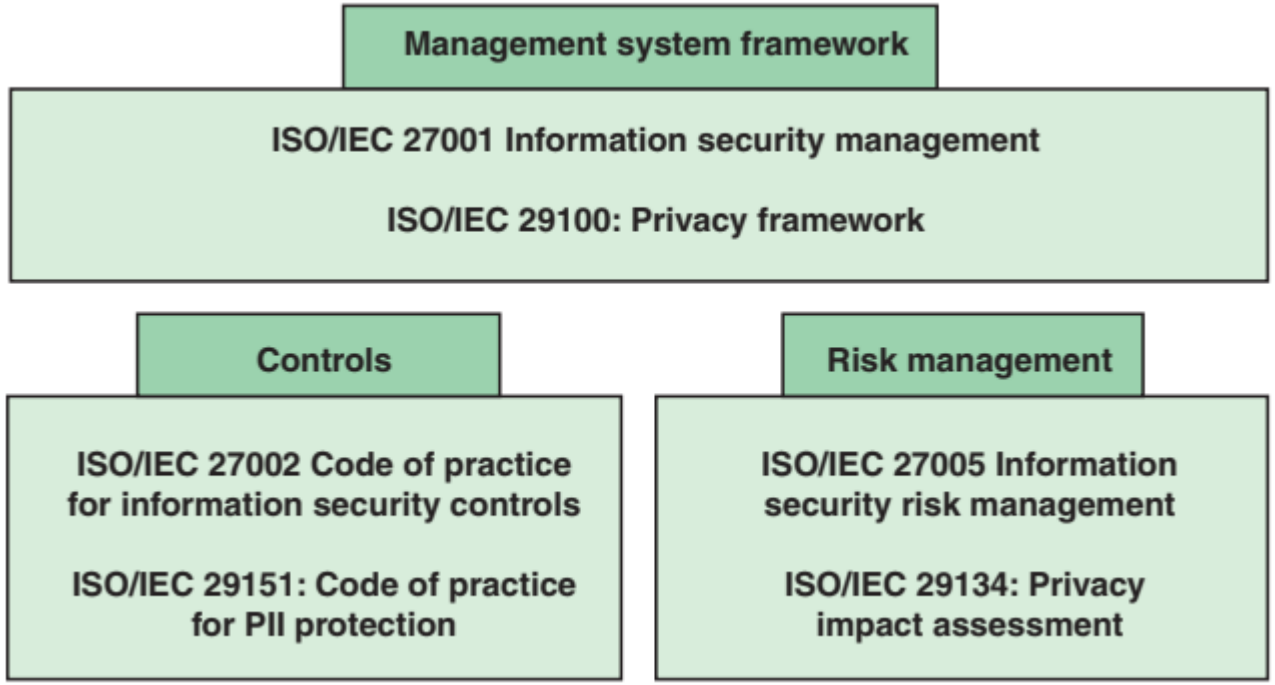
3. **ISO 29100** – Kerangka kerja perlindungan PII.
4. **ISO 29134** – Panduan **Privacy Impact Assessment (PIA)**.
5. **ISO 29151** – Praktik perlindungan data pribadi.
6. **DIS 29184** – Panduan pemberitahuan privasi online & persetujuan pengguna.
7. Standar tambahan:

   ISO 20889 – Teknik **de-identifikasi data** dalam dataset terstruktur.

Standar ini membantu organisasi memastikan keamanan informasi dan kepatuhan privasi, khususnya dalam perlindungan data pribadi dan layanan cloud.

Standar Privasi

International Organization for Standardization (ISO)



Relationships of ISO Security and Privacy Standards

Standar Privasi

International Organization for Standardization (ISO)

ISO 29100 adalah kerangka privasi yang mengatur perlindungan **Informasi Identifikasi Pribadi (PII)** dalam organisasi.

Kerangka ini memiliki dua tujuan utama:

1.Memberikan panduan kepada organisasi dalam mengidentifikasi, menilai, dan mengelola risiko serta solusi privasi.

2.Menetapkan elemen dan prinsip utama yang menjadi dasar bagi standar privasi lainnya dalam seri 29100.

Standar Privasi

International Organization for Standardization (ISO)

11 Prinsip Privasi ISO 29100:

1. **Persetujuan dan Pilihan** – Individu dapat memberikan atau menarik persetujuan atas pengumpulan dan penggunaan PII.
2. **Legalitas dan Spesifikasi Tujuan** – Pemrosesan PII harus memiliki dasar hukum yang sah dan tujuan yang jelas.
3. **Pembatasan Pengumpulan** – Pengumpulan PII hanya sebatas yang diperlukan dan sesuai hukum.
4. **Minimisasi Data** – PII yang diproses dan diungkap harus seminimal mungkin.
5. **Pembatasan Penggunaan dan Penyimpanan** – PII hanya digunakan dan disimpan untuk tujuan yang sah.
6. **Akurasi dan Kualitas** – PII harus akurat, diperbarui, dan diperoleh dari sumber terpercaya.
7. **Transparansi dan Pemberitahuan** – Pengendali PII harus memberikan informasi yang jelas tentang kebijakan dan praktik privasi.
8. **Partisipasi dan Akses PII** – Individu dapat mengakses, memperbaiki, atau menghapus PII mereka.
9. **Akuntabilitas** – Organisasi harus memiliki kebijakan dan langkah konkret untuk melindungi PII.
10. **Keamanan Informasi** – PII harus dilindungi dari akses tidak sah, kehilangan, atau modifikasi.
11. **Kepatuhan Privasi** – Audit berkala diperlukan untuk memastikan kepatuhan terhadap regulasi privasi.

Standar Privasi

International Organization for Standardization (ISO)

Kerangka Privasi ISO 29100

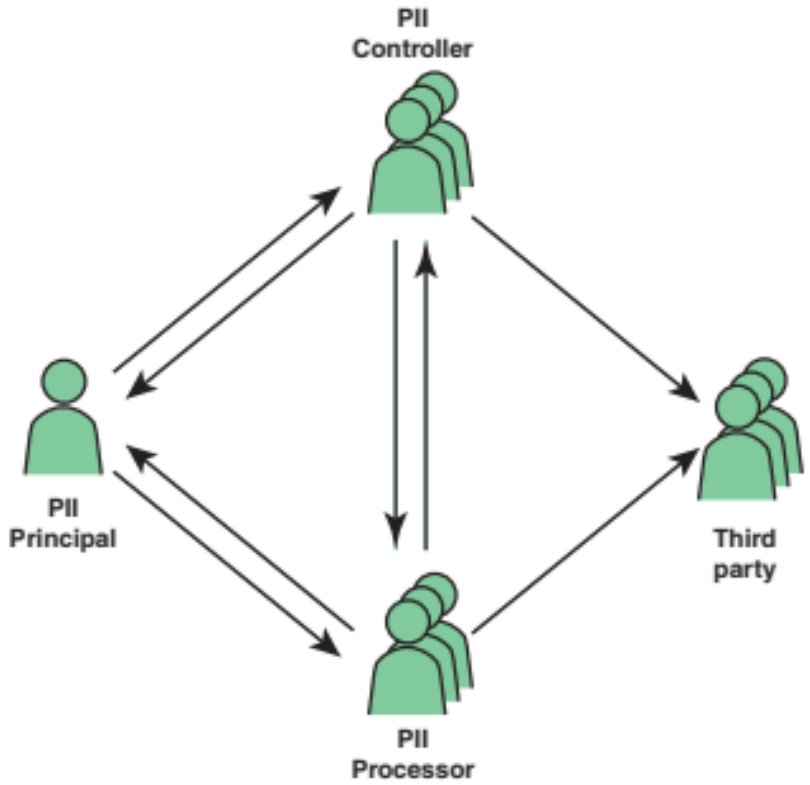
ISO 29100 mengidentifikasi elemen utama dalam kerangka privasi, termasuk **aktor, interaksi, PII (Informasi Identifikasi Pribadi), persyaratan perlindungan privasi, kebijakan, dan kontrol privasi**.

Aktor dalam Pemrosesan PII:

1. **PII Principal** – Individu yang terkait dengan PII (*data subject*).
2. **Privacy Stakeholder** – Pihak yang memiliki kepentingan dalam pemrosesan PII, termasuk karyawan, pemerintah, pemilik saham, dan komunitas.
3. **PII Controller** – Pihak yang menentukan tujuan dan cara pemrosesan PII.
4. **PII Processor** – Pihak yang memproses PII sesuai instruksi **PII Controller**. Bisa jadi entitas yang sama dengan **PII Controller**.
5. **Third Party** – Pihak lain yang menerima PII selain **PII Principal, Controller, dan Processor**.

Standar Privasi

International Organization for Standardization (ISO)



Roles and Interactions in the ISO Privacy Framework

Standar Privasi

International Organization for Standardization (ISO)

Code of Practice for PII Protection

ISO 29151 melengkapi ISO 27002 dengan pedoman perlindungan PII, mencakup pemilihan, penerapan, dan pengelolaan kontrol keamanan informasi

Organisasi tidak wajib menerapkan semua kontrol, tetapi memilih yang relevan berdasarkan penilaian dampak privasi.

Control Category	Privacy Controls
Information security policies	Management direction for information security
Organization of information security	Internal organization Mobile devices and teleworking
Human resource security	Prior to employment During employment Termination and change of employment
Asset management	Responsibility for assets Information classification Media handling
Access control	Business requirements of access control User access management User responsibilities System and application access control
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas Equipment
Operations security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management Information systems audit considerations
Communications security	Network security management Information transfer
System acquisition, development, and maintenance	Security requirements of information systems Security in development and support processes Test data
Supplier relationships	Information security in supplier relationships
Information security incident management	Management of information security incidents and improvements
Information security aspects of business continuity management	Information security continuity Redundancies
Compliance	Compliance with legal and contractual requirements Information security reviews

Standar Privasi

National Institute of Standards and Technology (NIST)

Dokumen yang dihasilkan Computer Security Resource Center (CSRC) terbagi dalam tiga kategori utama: kontrol privasi, rekayasa privasi, dan kerangka kerja privasi.

SP 800-53 dan SP 800-53A, yang menyediakan kontrol privasi untuk organisasi.

Untuk mengatasi ancaman privasi dan mematuhi regulasi, NIST membagi kontrolnya ke dalam dua kelompok utama:

1. **Kontrol Khusus Privasi** (hanya menangani privasi):
    1. **Partisipasi Individu**: Memungkinkan individu mengakses dan memperbaiki PII mereka.
    2. **Otorisasi Privasi**: Menentukan dasar hukum untuk pengumpulan dan penggunaan PII.
2. **Kontrol Gabungan Privasi/Keamanan** (menangani baik privasi maupun keamanan), mencakup:
    1. **Kontrol Akses, Audit, Manajemen Risiko, Respons Insiden, dan Perlindungan Sistem**.
    2. Total **15 keluarga kontrol** yang mengatasi aspek privasi dan keamanan.

Standar Privasi

National Institute of Standards and Technology (NIST)

ID	Family	Number of Privacy Controls
Privacy-Specific Controls		
IP	Individual Participation	6
PA	Privacy Authorization	4
Joint Privacy/Security Controls		
AC	Access Control	3
AT	Awareness and Training	4
AU	Audit and Accountability	4
CA	Assessment, Authorization, and Monitoring	4
CM	Configuration Management	4
CP	Contingency Planning	4
IA	Identification and Authentication	3
IR	Incident Response	9
MP	Media Protection	1
PL	Planning	5
PM	Program Management	23
RA	Risk Assessment	4
SA	System and Services Acquisition	11
SC	System and Communications Protection	4
SI	System and Information Integrity	8

NIST Privacy and Joint Control Families

Standar Privasi

National Institute of Standards and Technology (NIST)

ID	Name
Individual Participation (IP)	
IP-1	Individual Participation Policy and Procedures
IP-2	Consent
IP-2(1)	Attribute Management
IP-2(2)	Just-in-Time Notice of Consent
IP-3	Redress
IP-3(1)	Notice of Correction or Amendment
IP-3(2)	Appeal
IP-4	Privacy Notice
IP-4(1)	Just-in-Time Notice of Privacy Authorization
IP-5	Privacy Act Statements
IP-6	Individual Access
Privacy Authorization (PA)	
PA-1	Privacy Authorization Policy and Procedures
PA-2	Authority to Collect
PA-3	Purpose Specification
PA-3(1)	Usage restrictions of PII
PA-3(2)	Automation
PA-4	Information Sharing with External Parties

NIST Privacy-Specific Controls

Standar Privasi

National Institute of Standards and Technology (NIST)

SP 800-53 menyediakan lebih dari **100 kontrol privasi dan keamanan** yang dapat dipilih dan diterapkan oleh organisasi sesuai kebijakan privasinya.

- **Kontrol dasar** menetapkan tindakan keamanan yang harus dilakukan oleh organisasi atau sistem informasi.
- **Panduan tambahan** memberikan informasi opsional yang dapat diterapkan sesuai kebutuhan organisasi.
- **Peningkatan kontrol** dapat menambahkan fungsionalitas atau memperkuat kontrol keamanan untuk sistem yang memerlukan perlindungan lebih tinggi, terutama berdasarkan **penilaian risiko organisasi**.

CALVIN INSTITUTE OF TECHNOLOGY

IP-2 CONSENT	
Control: Implement [Assignment: organization-defined tools or mechanisms] for users to authorize the processing of their PII prior to its collection that:	
IP-2(a)	Use plain language and provide examples to illustrate the potential privacy risks of the authorization.
IP-(2b)	Provide a means for users to decline the authorization.
Supplemental Guidance: This control transfers risk that arises from the processing of PII from the organization to an individual. It is only selected as required by law or regulation or when individuals can be reasonably expected to understand and accept any privacy risks arising from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. To help users understand the risks being accepted when providing consent, organizations write materials in plain language and avoid technical jargon. The examples required in IP-2(a) focus on key points necessary for user decision-making. When developing or purchasing consent tools, organizations consider the application of good information design procedures in all user-facing consent materials; use of active voice and conversational style; logical sequencing of main points; consistent use of the same word (rather than synonyms) to avoid confusion; the use of bullets, numbers, and formatting where appropriate to aid readability; and legibility of text, such as font style, size, color, and contrast with surrounding background. Related controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.	
Control Enhancements: (1) *CONSENT | ATTRIBUTE MANAGEMENT* Allow data subjects to tailor use permissions to selected attributes. Supplemental Guidance: Allowing individuals to select how specific data attributes may be further used or disclosed beyond the original use may help reduce privacy risk arising from the most sensitive of the data attributes while maintaining utility of the data (2) *CONSENT | JUST-IN-TIME NOTICE OF CONSENT* Present authorizations to process personally identifiable information in conjunction with the data action or [Assignment: organization-defined frequency]. Supplemental Guidance: If the circumstances under which an individual gave consent have changed or a significant amount of time has passed since an individual gave consent for the processing of his or her personally identifiable information, the data subject's assumption about how the information is being processed might no longer be accurate or reliable. Just-in-time notice can help maintain individual satisfaction with how the personally identifiable information is being processed	
References: NIST Special Publication 800-50. NIST Interagency Report 8062.	

FIGURE 3.5 Privacy Control IP-2 in SP 800-53

Standar Privasi

National Institute of Standards and Technology (NIST)

Rekayasa Privasi (Privacy Engineering) NIST

NISTIR 8062 mendefinisikan **tiga tujuan utama** dalam rekayasa privasi untuk membantu perancang sistem dan insinyur dalam mengelola risiko privasi:

1. **Predictability (Prediktabilitas)** – Memastikan bahwa individu dan pemangku kepentingan dapat **memahami dan mempercayai** bagaimana PII mereka digunakan.
2. **Manageability (Kemampuan Pengelolaan)** – Memberikan individu kendali atas informasi mereka, seperti **pengubahan, penghapusan, dan pengungkapan selektif**, tanpa mengganggu fungsionalitas sistem.
3. **Disassociability (Kemampuan Pemisahan)** – Memungkinkan pemrosesan PII **tanpa mengasosiasikannya langsung** dengan individu, kecuali jika diperlukan, untuk mengurangi risiko privasi.

Standar Privasi

National Institute of Standards and Technology (NIST)

OECD FIPP	Predictability	Manageability	Disassociability
Collection limitation		✓	✓
Data quality		✓	
Purpose specification	✓		
Use limitation	✓		
Security safeguards			
Openness	✓		
Individual participation		✓	
Accountability	✓	✓	✓

Standar Privasi

National Institute of Standards and Technology (NIST)

NIST Cybersecurity and Privacy Frameworks

Komponen Utama Kerangka Keamanan Siber NIST

1. **Core** – Kumpulan aktivitas keamanan siber dan hasil yang diharapkan.
2. **Implementation Tiers** – Menunjukkan tingkat kematangan pengelolaan risiko keamanan siber.
3. **Profiles** – Disesuaikan dengan kebutuhan bisnis untuk mencapai tujuan keamanan.

Lima Fungsi Utama dalam Kerangka Keamanan Siber NIST

1. **Identify** – Mengidentifikasi risiko keamanan siber.
2. **Protect** – Melindungi sistem dan data dari ancaman.
3. **Detect** – Mendeteksi insiden keamanan siber.
4. **Respond** – Menanggapi insiden keamanan yang terdeteksi.
5. **Recover** – Memulihkan layanan yang terkena dampak insiden siber.

Function	Description	Category
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Access Control
		Awareness and Training
		Data Security
		Information Protection Processes and Procedures
		Maintenance
		Protective Technology
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Recovery Planning

Standar Privasi

National Institute of Standards and Technology (NIST)

NIST Cybersecurity and Privacy Frameworks

Kerangka Privasi NIST

- Membantu organisasi memahami **dampak sistem dan layanan mereka terhadap individu**.
- Mengintegrasikan praktik privasi ke dalam proses bisnis untuk **mengurangi risiko privasi**.
- Mencakup fungsi: **Identify, Protect, Control, Inform, dan Respond** untuk menangani risiko privasi.

Function	Description	Category
Identify	Develop the organizational understanding to manage privacy risk for individuals arising from data processing or their interactions with system, products, or services.	Inventor and Mapping
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management
Function	**Description**	**Category**
Protect	Develop and implement appropriate data processing safeguards.	Identity Management, Authentication, and Access Control
		Awareness and Training
		Data Security
		Data Protection Processes and Procedures
		Maintenance
		Protective Technology
		Protected Processing
Control	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	Data Management Processes and Procedures
		Data Management
Inform	Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed.	Transparency Processes and Procedures
		Data Processing Awareness
Respond	Develop and implement appropriate activities to take action regarding a privacy breach or event.	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
		Redress

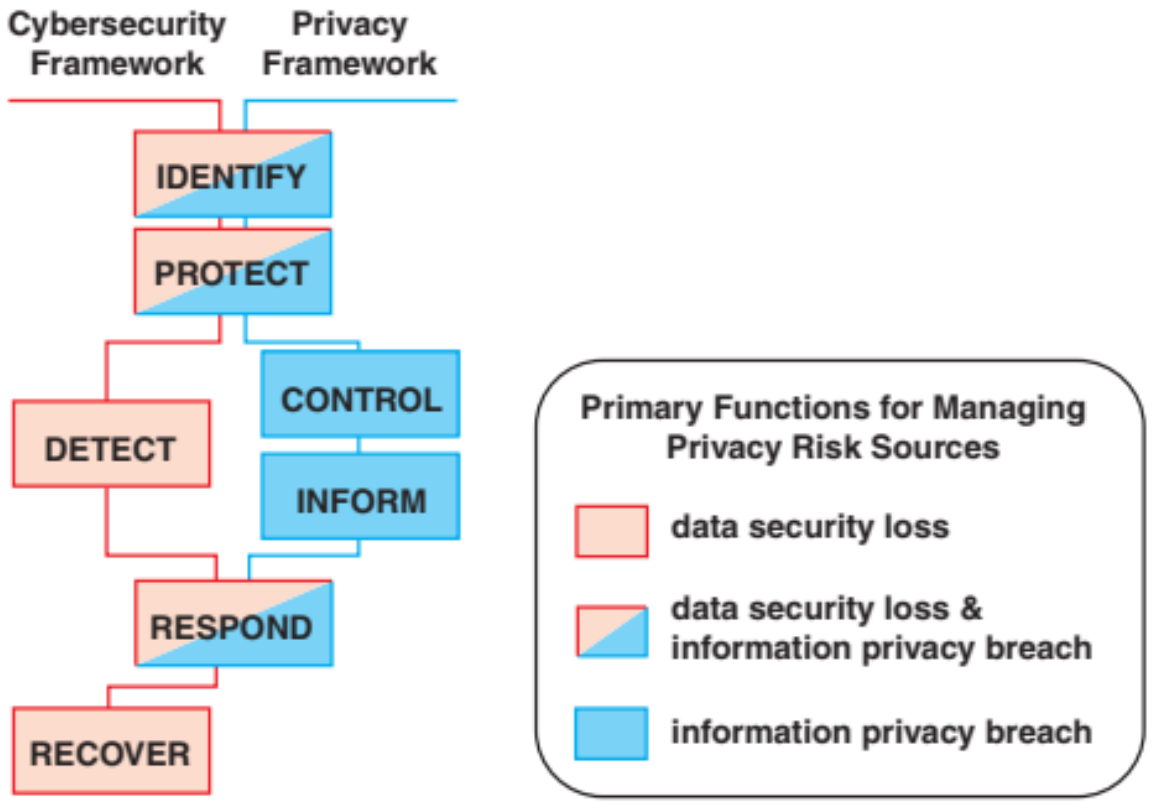
Standar Privasi

National Institute of Standards and Technology (NIST)

NIST Cybersecurity and Privacy Frameworks

Hubungan Keamanan Siber dan Privasi

- **Keamanan siber melindungi data dari ancaman eksternal**, sedangkan **privasi berfokus pada perlindungan data individu**.
- Fungsi keduanya saling berhubungan, seperti **Protect, Respond, dan Identify** yang berlaku untuk keamanan dan privasi.



Cybersecurity Framework and Privacy Framework Functions Relationship

CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Terima Kasih
Tuhan Memberkati