RSNI3

Rancangan Standar Nasional Indonesia 3

RSNI3 ISO/IEC TS 27570:2021
(Ditetapkan oleh BSN tahun 2024)

Proteksi privasi — Pedoman privasi untuk kota cerdas

Privacy protection — Privacy guidelines for smart cities

(ISO/IEC TS 27570:2021, IDT)

ICS 35.030

BADAN STANDARDISASI NASIONAL

BSN
Email: dokinfo@bsn.go.id
www.bsn.go.id

Diterbitkan di Jakarta

Daftar Isi

Daftar Gambar

Daftar Tabel

Prakata

SNI ISO/IEC TS 27570:2021, *Proteksi privasi - Pedoman privasi untuk kota cerdas*, merupakan standar yang disusun dengan jalur adopsi tingkat keselarasan identik dari ISO/IEC TS 27570:2021, *Privacy protection – Privacy guidelines for smart cities*, dengan metode adopsi terjemahan dua bahasa dan ditetapkan oleh BSN pada tahun 2024.

Standar ini disusun oleh Komite Teknis 35-04, Keamanan Informasi, Keamanan Siber dan Perlindungan Privasi. Standar ini telah dibahas melalui rapat teknis dan disepakati dalam rapat konsensus pada tanggal 21 Juni 2024 di Depok, yang dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari pemerintah, pelaku usaha, konsumen, dan pakar. Standar ini telah melalui tahap jajak pendapat pada tanggal 18 Juli 2024 sampai dengan 1 Agustus 2024 dengan hasil akhir disetujui menjadi SNI.

Kosakata yang digunakan dalam Standar ini mengikuti bentuk baku yang dicantumkan dalam Kamus Besar Bahasa Indonesia (KBBI), tetapi ada beberapa kosakata yang belum ada di dalam KBBI.

Kata/istilah "*privacy-by-design*", "*unlinkability*", dan "*dataset*" tidak diterjemahkan dalam Standar ini karena Komite Teknis 35-04 belum menemukan padanan kata/istilah yang sesuai dengan konteks yang sesuai dalam Bahasa Indonesia.

Apabila pengguna menemukan keraguan dalam standar ini maka disarankan untuk melihat standar aslinya yaitu ISO/IEC TS 27570:2021, dan/atau dokumen terkait lain yang menyertainya.

Perlu diperhatikan bahwa kemungkinan beberapa unsur dari standar ini dapat berupa hak kekayaan intelektual (HAKI). Namun selama proses perumusan SNI, Badan Standardisasi Nasional telah memperhatikan penyelesaian terhadap kemungkinan adanya HAKI terkait substansi SNI. Apabila setelah penetapan SNI masih terdapat permasalahan terkait HAKI, Badan Standardisasi Nasional tidak bertanggung jawab mengenai bukti, validitas, dan ruang lingkup dari HAKI tersebut.

Pendahuluan

Bertumbuhnya integrasi TIK (misalnya komputasi awan, IoT, data raya, jaringan seluler, kecerdasan artifisial, dan pemelajaran mesin) di kota cerdas akan memungkinkan peningkatan kapabilitas berbagi data untuk mencapai layanan yang lebih baik. Namun bertumbuhnya kompleksitas infrastruktur TIK juga akan menciptakan kerentanan pada level keamanan dan privasi. Insiden keamanan dapat menyebabkan layanan esensial tidak beroperasi dengan benar, misalnya kekurangan pasokan listrik secara masif. Demikian juga, akses takterotorisasi terhadap data pribadi dapat menyebabkan pelanggaran privasi yang berat, misalnya akses terhadap rekaman data kesehatan pribadi.

Memastikan privasi ditangani dengan benar di kota cerdas merupakan sebuah tantangan. Pertama, berbagai pemangku kepentingan publik dan privat dapat dilibatkan seperti:

— agensi yang bertanggung jawab memanajemeni layanan kota yang esensial, misalnya layanan administrasi;

— organisasi bisnis yang bertanggung jawab mengoperasikan layanan, misalnya distribusi listrik;

— organisasi dalam rantai pasokan yang terasosiasi dengan penerapan infrastuktur terkait, misalnya sistem transportasi; dan

— asosiasi yang mewakili sudut pandang warga kota.

Kedua, berbagai macam standar dapat digunakan seperti:

— standar privasi;

— standar kota cerdas;

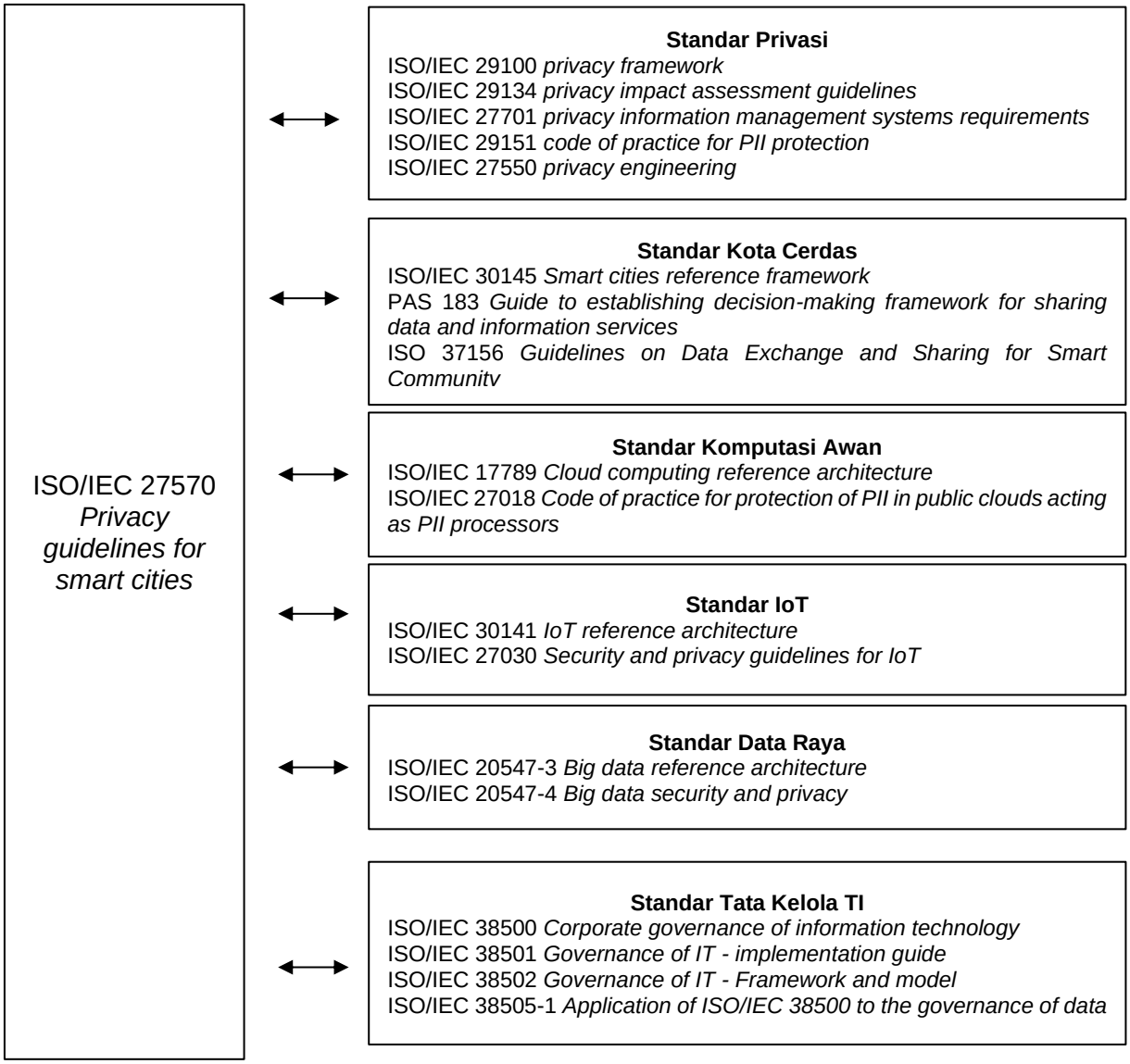
— standar komputasi awan;

— standar IoT;

— standar data raya; dan

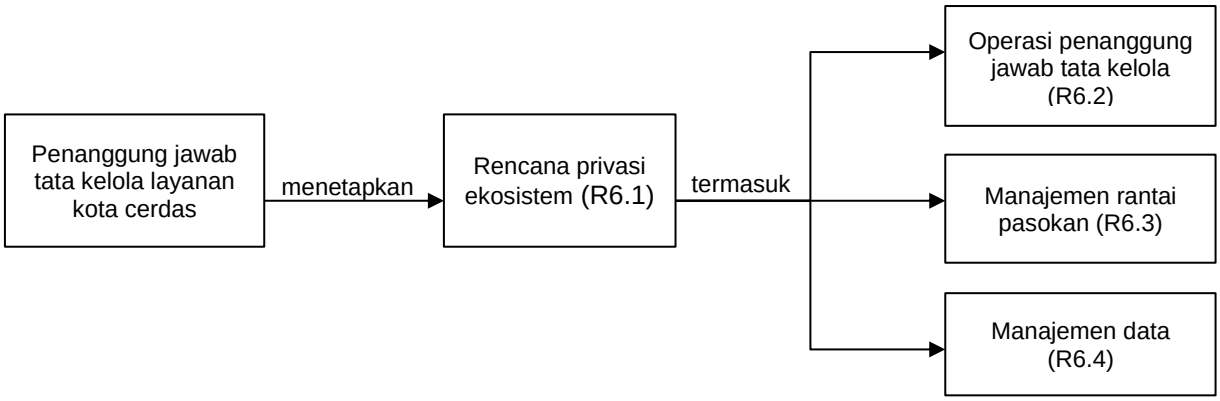
— standar tata kelola TI.

Gambar 1 menunjukkan contoh standar tersebut. Dokumen ini dengan demikian berfokus pada menyediakan panduan penggunaan standar, dengan tetap mempertimbangkan berbagai pemangku kepentingan dalam sebuah ekosistem kota cerdas.



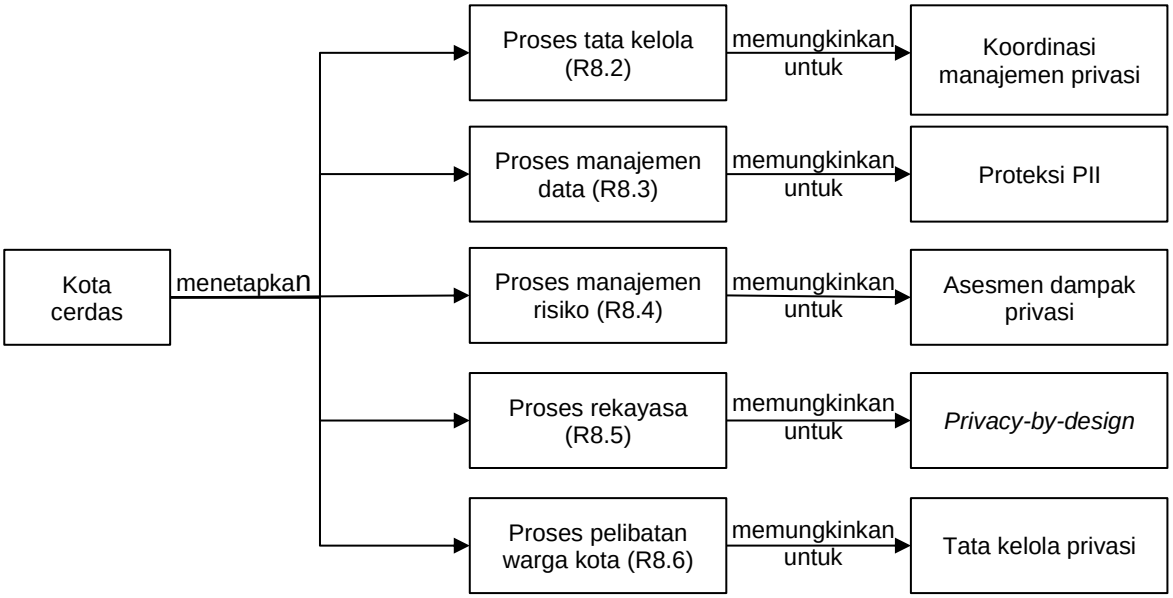
Gambar 1 — Contoh standar untuk referensi

Gambar 2 merangkum rekomendasi privasi untuk ekosistem kota cerdas dalam dokumen ini, yang selanjutnya diberi nomor R6.1, R6.2, R6.3, dan R6.4.



Gambar 2 — Panduan ekosistem untuk privasi

Gambar 3 merangkum rekomendasi privasi untuk proses kota cerdas dalam dokumen ini, yang selanjutnya diberi nomor R8.2, R8.3, R8.4, dan R8.5.



Gambar 3 — Panduan proses untuk privasi

Diperkirakan dokumen ini akan membuka jalan bagi standar privasi di masa depan untuk kota cerdas. Tabel 1 memberikan daftar kemungkinan standar di masa depan.

Tabel 1 — Contoh kemungkinan standar di masa depan

Kategori	Standar
Manajemen privasi untuk melacak dan memonitor aset PII yang dieksploitasi di kota cerdas	Kerangka kerja untuk manajemen privasi di kota cerdas Pedoman untuk komunikasi antar organisasi Pedoman untuk rencana manajemen privasi di kota cerdas Pedoman untuk penyusunan kebijakan privasi di kota cerdas termasuk retensi data Pedoman untuk laporan asesmen dampak privasi di kota cerdas Pedoman untuk manajemen persetujuan di kota cerdas Pedoman untuk manajemen akuntabilitas dan transparansi privasi di kota cerdas Pedoman untuk manajemen pelanggaran privasi di kota cerdas Pedoman untuk layanan *privacy-by-design* kota cerdas Pedoman untuk integrasi konsern privasi dalam perjanjian pertukaran data Asurans keamanan dan privasi layanan kota cerdas
Rekayasa privasi dalam ekosistem kota cerdas	Pedoman untuk rekayasa privasi[a] di kota cerdas
Kolaborasi dalam ekosistem kota cerdas	Pedoman untuk keterlibatan warga kota Pedoman untuk komunikasi antarorganisasi (untuk setiap tipe organisasi, misalnya administrasi)
Interoperabilitas untuk menghindari penguncian vendor	Model informasi manajemen privasi umum di kota cerdas Informasi asesmen dampak privasi umum di kota cerdas Deskripsi umum kapabilitas privasi di kota cerdas Deskripsi umum insiden privasi di kota cerdas

[a] Rekayasa privasi berfokus pada integrasi konsern privasi dalam rekayasa suatu sistem.

Proteksi privasi — Pedoman privasi untuk kota cerdas

1 Ruang lingkup

Dokumen ini mengambil sudut pandang dari multipel agensi dan juga sudut pandang yang berpusat pada warga kota.

Dokumen ini memberikan panduan tentang:
— proteksi privasi ekosistem kota cerdas;
— bagaimana standar dapat digunakan pada level global dan level organisasi untuk kepentingan warga kota; dan
— proses untuk proteksi privasi ekosistem kota cerdas.

Dokumen ini berlaku untuk semua tipe dan ukuran organisasi, termasuk perusahaan publik dan privat, entitas pemerintah, dan organisasi nirlaba yang memberikan layanan di lingkungan kota cerdas.

2 Acuan normatif

Tidak ada acuan normatif dalam dokumen ini.

3 Istilah dan definisi

Untuk tujuan dokumen ini, berlaku istilah dan definisi berikut.
ISO dan IEC memelihara basis data istilah untuk digunakan dalam standardisasi di alamat berikut:

— ISO *Online Browsing Platform* : tersedia di https://www.iso.org/obp

— IEC Electropedia: tersedia di https://www.electropedia.org/

3.1
aktivitas
serangkaian *tugas* (3.32) yang kohesif dari suatu *proses* (3.25)

[SUMBER: ISO/IEC/IEEE 15288:2015, 4.1.3]

3.2
agensi
organisasi (3.13) yang menyediakan layanan spesifik untuk suatu kota

3.3
availabilitas
properti yang dapat diakses dan digunakan atas permintaan oleh entitas yang terotorisasi

[SUMBER: ISO/IEC 27000:2018, 3.7]

3.4
warga kota
penduduk suatu kota

3.5
keterlibatan warga kota
keterlibatan *warga kota* (3.4) dalam pengambilan keputusan kebijakan publik

3.6
konfidensialitas
properti di mana informasi tidak dibuat tersedia atau diungkapkan kepada individu, entitas atau *proses* (3.25) yang takterotorisasi

[SUMBER: ISO/IEC 27000:2018, 3.10]

3.7
pejabat proteksi data
person yang ditunjuk oleh *pengontrol PII* (3.15) untuk memastikan, secara independen, kepatuhan terhadap persyaratan hukum/regulasi privasi

3.8
ekosistem
infrastruktur dan layanan yang berdasarkan jaringan *organisasi* (3.13) dan pemangku kepentingan

Catatan 1 untuk entri: Organisasi dapat mencakup badan publik.

3.9
rencana privasi ekosistem
pengaturan yang direncanakan untuk memastikan privasi dikelola secara adekuat di suatu *ekosistem* (3.8)

3.10
tata kelola
sistem pengarahan dan pengontrolan

[SUMBER: ISO 38500:2015, 2.8]

3.11
integritas
properti akurasi dan kelengkapan

[SUMBER: ISO/IEC 27000:2018, 3.36]

3.12
intervenabilitas
properti yang memastikan bahwa *PII principal* (3.16), *pengontrol PII* (3.15), *prosesor PII* (3.17) dan otoritas pengawas dapat melakukan intervensi dalam semua pemrosesan data yang relevan dengan privasi

Catatan 1 untuk entri: Sejauh mana para pemangku kepentingan tersebut dapat mengintervensi pemrosesan data dapat dibatasi oleh undang-undang atau regulasi yang relevan.

[SUMBER: ISO/IEC TR 27550:2019, 3.6]

3.13
organisasi
person atau sekelompok orang yang memiliki fungsi sendiri dengan tanggung jawab, otoritas, dan hubungan untuk mencapai tujuannya

Catatan 1 untuk entri: Konsep organisasi mencakup tetapi tidak terbatas pada pedagang tunggal, perusahaan, korporasi, firma, otoritas, kemitraan, lembaga amal, atau bagian dari atau gabungan di antaranya, baik yang berbadan hukum atau tidak, publik atau privat.

[[SUMBER: ISO 37100:2016, 3.2.3, dimodifikasi — Catatan 2 untuk entri telah dihilangkan.]

3.14
informasi pengidentifikasi personal (*personally identifiable information*)
PII
setiap informasi yang a)dapat digunakan untuk mengidentifikasi *PII principal* (3.16) yang terkait dengan informasi tersebut, atau b)terkait atau mungkin secara langsung atau tidak langsung terkait dengan PII *principal*

Catatan 1 untuk entri: Untuk menentukan apakah PII *principal* dapat diidentifikasi, semua upaya yang dapat digunakan secara wajar oleh pemangku kepentingan privasi yang memegang data, atau oleh pihak lain, sebai dipertimbangkan untuk mengidentifikasi orang perseorangan.

[SUMBER: ISO/IEC 29100:2011, 2.9.]

3.15
pengontrol informasi pengidentifikasi personal
pengontrol PII
pemangku kepentingan privasi (atau para pemangku kepentingan privasi) yang menentukan tujuan dan sarana untuk memproses *informasi pengidentifikasi personal* (3.14) selain orang perseorangan yang menggunakan data untuk tujuan pribadi

Catatan 1 untuk entri: Pengontrol PII terkadang menginstruksikan orang lain [misalnya *prosesor PII* (3.17)] untuk memproses PII atas nama mereka sedangkan tanggung jawab pemrosesan tetap berada di tangan pengontrol PII.

[SUMBER: ISO/IEC 29100:2011, 2.10.]

3.16
***principal* informasi pengidentifikasi personal**
PII *principal*
orang perseorangan yang terkait dengan *informasi pengidentifikasi personal* (3.14)

Catatan 1 untuk entri: Bergantung pada yurisdiksi dan undang-undang proteksi dan privasi PII tertentu, sinonim “subjek data” juga dapat digunakan sebagai pengganti istilah “PII *principal*”.

[SUMBER: ISO/IEC 29100:2011, 2.11]

3.17
prosesor informasi pengidentifikasi personal
prosesor PII
pemangku kepentingan privasi yang memproses *informasi pengidentifikasi personal* (3.14) atas nama dan sesuai dengan instruksi *pengontrol PII* (3.15)

[SUMBER: ISO/IEC 29100:2011, 2.12]

3.18
kebijakan
intensi dan arahan dari *organisasi* (3.13) sebagaimana dinyatakan secara formal oleh manajemen puncak

[SUMBER: ISO/IEC 20547-3:2020, 3.11]

3.19
pelanggaran privasi
situasi di mana *informasi pengidentifikasi personal* (3.14) diproses dengan melanggar satu atau lebih persyaratan proteksi privasi yang relevan

[SUMBER: ISO/IEC 29100:2011, 2.13]

3.20
privacy-by-design
pendekatan di mana privasi dipertimbangkan pada tahap desain awal dan sepanjang siklus hidup lengkap produk, proses, atau layanan yang melibatkan pemrosesan *informasi pengidentifikasi personal* (3.14)

3.21
perjanjian berbagi data privasi
pasal-pasal untuk proteksi privasi dalam perjanjian berbagi data

Catatan 1 untuk entri: perjanjian berbagi data privasi dapat melibatkan transfer data, pemrosesan data, dan pembagian PII di antara *pengontrol PII* (3.15) bersama (ISO/IEC 27701:2019 7.2.7)

3.22
prinsip privasi
serangkaian nilai bersama yang mengatur proteksi privasi *informasi pengidentifikasi personal* (3.14) ketika diproses dalam sistem teknologi informasi dan komunikasi

[SUMBER: ISO/IEC 29100:2011, 2.18]

3.23
risiko privasi
efek dari ketidakpastian pada privasi

Catatan 1 untuk entri: Risiko didefinisikan sebagai “efek ketidakpastian terhadap sasaran” dalam ISO Guide 73 dan ISO 31000.

Catatan 2 untuk entri: Ketidakpastian adalah keadaan, bahkan sebagian, dari kekurangan informasi yang terkait dengan, pemahaman atau pengetahuan tentang suatu peristiwa, konsekuensi atau kemungkinannya.

[SUMBER: ISO/IEC 29100:2011, 2.19]

3.24
aturan privasi
pernyataan yang menentukan apa yang diperbolehkan atau tidak mengenai privasi

3.25
proses
serangkaian aktivitas yang saling terkait atau berinteraksi yang mengubah input menjadi output

[SUMBER: ISO/IEC 27000:2018, 3.54]

3.26
pemrosesan PII
operasi atau serangkaian operasi yang dilakukan pada *informasi pengidentifikasi personal* (3.14)

Catatan 1 untuk entri: Contoh operasi pemrosesan PII termasuk, namun tidak terbatas pada, pengumpulan, penyimpanan, perubahan, pengambilan, konsultasi, pengungkapan, anonimisasi, pseudonimisasi, diseminasi atau sebaliknya menjadikan tersedia, penghapusan atau pemusnahan PII.

[SUMBER: ISO/IEC 29100:2011, 2.23]

3.27
kota cerdas
integrasi yang efektif antara sistem fisik, digital, dan manusia dalam lingkungan yang dibangun untuk mewujudkan masa depan yang berkelanjutan, sejahtera, dan inklusif bagi *warga kota* (3.27)

[SUMBER: BSI PAS 181:2014]

3.28
penanggung jawab tata kelola layanan kota cerdas
badan yang bertindak sebagai pengawas untuk rekomendasi atau regulasi privasi mengenai layanan *kota cerdas* (3.27)

3.29
rantai pasokan
jaringan *organisasi* (3.13) yang terlibat, melalui hubungan hulu dan hilir, dalam *proses* (3.25) dan aktivitas yang menghasilkan nilai dalam bentuk produk dan layanan di tangan konsumen terakhir

[SUMBER: ISO/TS 22318:2015, 3.3.5]

3.30
pemasok
organisasi (3.13) dari individu yang mengadakan perjanjian dengan pengakuisisi untuk pasokan produk layanan

Catatan 1 untuk entri: Istilah lain yang secara umum digunakan untuk pemasok adalah kontraktor, produsen, penjual, atau vendor.

Catatan 2 untuk entri: Pengakuisisi dan pemasok terkadang merupakan bagian dari organisasi yang sama.

[SUMBER: ISO/IEC/IEEE 15288:2015, 4.1.45]

3.31
sistem dari sistem-sistem
sistem besar yang memberikan kapabilitas unik, dibentuk dengan mengintegrasikan sistem-sistem yang bermanfaat secara independen

[SUMBER: ISO/IEC/IEEE 24765:2017, 2]

3.32
tugas
aksi yang dipersyaratkan, direkomendasikan, atau diperbolehkan, dimaksudkan untuk berkontribusi pada manfaat satu atau lebih hasil dari suatu *proses* (3.25)

[SUMBER: ISO/IEC/IEEE 15288:2015, 4.1.50]

3.33
pihak ketiga
pemangku kepentingan privasi selain *PII principal*, *pengontrol PII* (3.15) dan *prosesor PII* (3.17), dan orang perseorangan yang terotorisasi untuk memproses data di bawah otoritas langsung pengontrol PII atau prosesor PII

[SUMBER: ISO/IEC 29100:2011, 2.27]

3.34
transparansi
kemampuan untuk memastikan bahwa semua pemrosesan data yang relevan dengan privasi termasuk pengaturan hukum, teknis, dan organisasi dapat dipahami dan direkonstruksi

Catatan 1 untuk entri: Hal ini termasuk membuat informasi tentang pemrosesan PII tersedia bagi *PII principal* (3.15)

[SUMBER: ISO/IEC TR 27550:2019, 3.24, dimodifikasi — Catatan 1 untuk entri telah ditambahkan.]

3.35
unlinkability
kemampuan untuk memastikan bahwa *PII principal* (3.15) dapat membuat penggunaan multipel dari sumber daya atau layanan tanpa pihak lain dapat menghubungkan penggunaan tersebut secara bersama

[SUMBER: ISO/IEC TR 27550:2019, 3.25]

3.36
produk kerja
artefak yang diasosiasikan dengan eksekusi sebuah *proses* (3.25)

[SUMBER: ISO/IEC/IEEE 42020:2019, 3.26]

4 Istilah singkatan

KA	kecerdasan artifisial
TIK	teknologi informasi dan komunikasi
IoT	internet untuk segala (*internet of things*)
LINDDUN	keterhubungan, identifikasi, non-repudiasi, deteksi, pengungkapan informasi, ketidaksadaran, ketidakpatuhan (*linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance*)
OASIS	organisasi untuk kemajuan standar informasi yang terstruktur (*organization for the advancement of structured information standards*)
PIA	asesmen dampak privasi (*privacy impact assessment*)
STRIDE	pemalsuan identitas pengguna, perusakan, repudiasi, pengungkapan informasi, kegagalan layanan, peningkatan privilese (*spoofing of user identity, tampering, repudiation, information disclosure, denial of service, elevation of privilege*)

5 Privasi di kota cerdas

5.1 Umum

Kota cerdas bertujuan untuk mengintegrasikan sistem fisik, digital, dan manusia secara efektif ke dalam lingkungan yang dibangun untuk mewujudkan masa depan yang berkelanjutan, sejahtera, dan inklusif bagi warga kotanya. Ini merupakan visi bersama di antara para pemangku kepentingan kota untuk mencapai sejumlah manfaat yang diinginkan: kesejahteraan, transparansi, keberlanjutan, pembangunan ekonomi, efisiensi dan resiliensi, kolaborasi serta inovasi. Dalam visi ini, pembangunan ekonomi dan inovasi memanfaatkan TIK (misalnya IoT, data raya, KA, komputasi awan), dan mensyaratkan pandangan sistem dari sistem-sistem untuk memungkinkan integrasi dari sistem-sistem sektor tertentu (misalnya energi, transportasi, kesehatan). Integrasi privasi merupakan konsern utama. Panduan perlu diberikan mengenai bagaimana kota cerdas dapat mengikuti prinsip ISO/IEC 29100:

— persetujuan dan pilihan;

— legitimasi dan spesifikasi tujuan;

— limitasi pengumpulan;

— minimalisasi data;

— limitasi penggunaan, retensi, dan pengungkapan;

— akurasi dan kualitas;

— keterbukaan, transparansi, dan akses;

— akuntabilitas;

— keamanan informasi; dan

— kepatuhan privasi.

5.2 Integrasi privasi dalam kerangka kerja referensi kota cerdas

5.2.1 Kerangka kerja referensi TIK kota cerdas dalam seri ISO/IEC 30145

Gambar 4 mendeskripsikan kerangka kerja referensi TIK kota cerdas dalam seri ISO/IEC 30145. Ini terdiri dari 3 kerangka kerja:

— kerangka kerja proses bisnis yang menspesifikasikan proses esensial dalam bidang tata kelola, bisnis inti, dan dukungan;

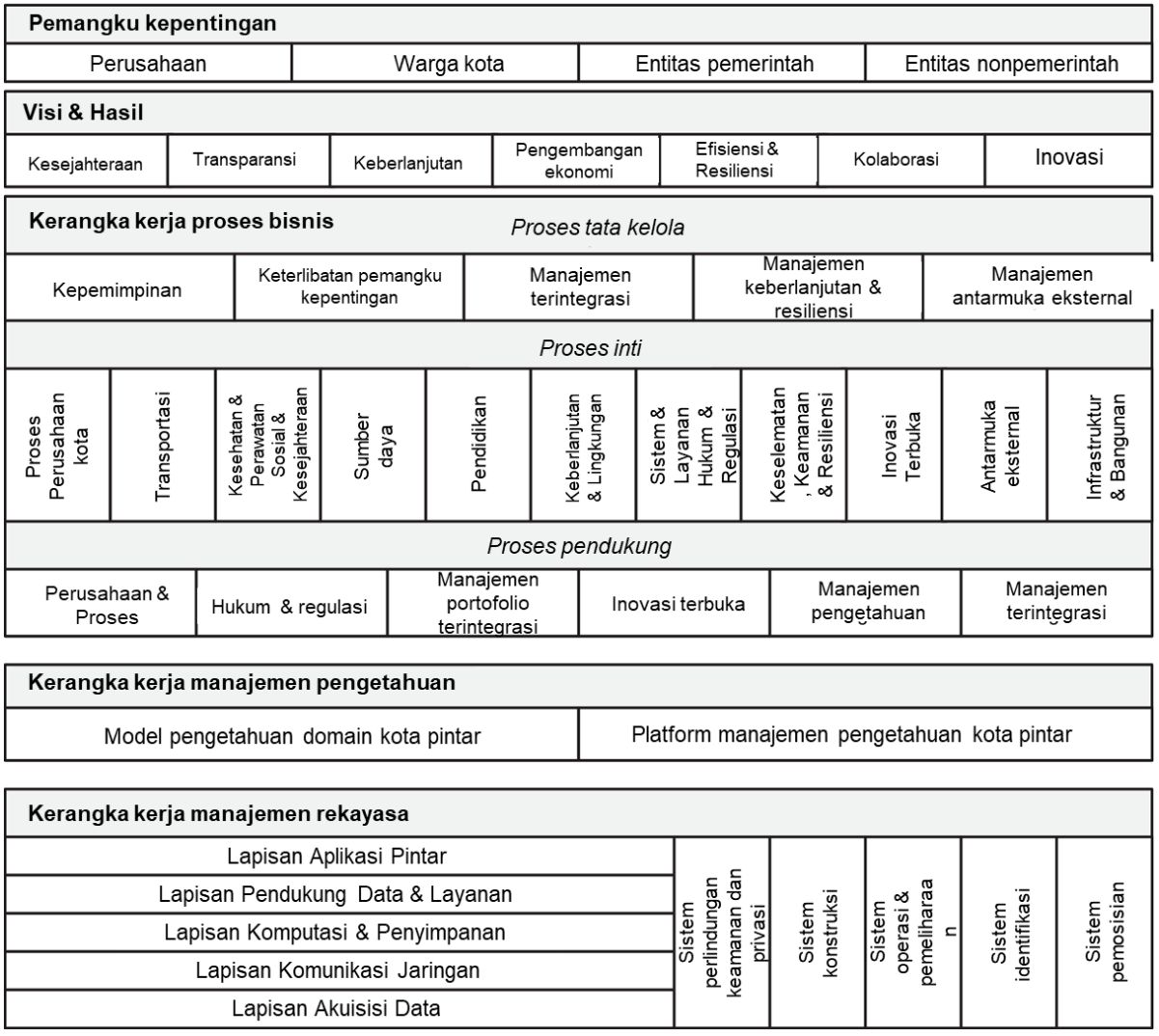
— kerangka kerja manajemen pengetahuan yang menyediakan panduan pada pemodelan dan manajemen pengetahuan untuk bisnis dan operasi kota cerdas; dan

— kerangka kerja manajemen rekayasa yang menyediakan serangkaian lapisan TIK untuk pengoperasian kota cerdas, yaitu lapisan aplikasi cerdas, lapisan pendukung data dan layanan, lapisan komunikasi dan penyimpanan, lapisan komunikasi jaringan, dan lapisan akuisisi data.

Kerangka kerja proses bisnis termasuk:

— proses tata kelola, yang berfokus pada penetapan kebijakan, dan pemonitoran berkelanjutan atas implementasinya yang tepat oleh penanggung jawab tata kelola kota cerdas, misalnya otoritas publik lokal; dan

— proses bisnis inti dan pendukung, yang berfokus pada jalannya proses bisnis sesuai dengan kebijakan kota cerdas oleh agensi atau organisasi bisnis yang didelegasikan kota cerdas.



Gambar 4 — Kerangka kerja referensi TIK kota cerdas

Kerangka kerja manajemen rekayasa dideskripsikan pada Gambar 5. Ini termasuk:

— lapisan aplikasi cerdas berfokus pada aplikasi domain, pemerintahan cerdas, transportasi cerdas, pendidikan cerdas, layanan kesehatan cerdas, rumah cerdas, dan kampus cerdas yang semuanya mengandalkan pemrosesan data;

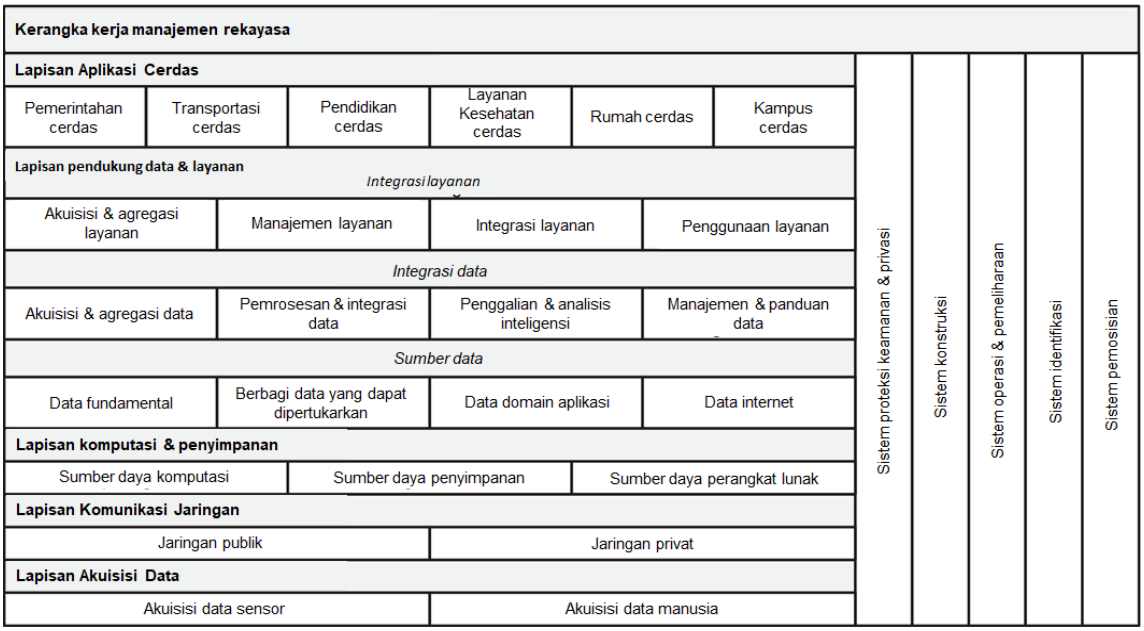
— lapisan pendukung data dan layanan berfokus pada sumber data, integrasi data, dan integrasi layanan;

— lapisan komputasi dan penyimpanan berfokus pada sumber daya komputasi, penyimpanan, dan perangkat lunak;

— lapisan komunikasi jaringan memberikan infrastruktur komunikasi pada kota cerdas dengan jaringan optik berkapasitas tinggi, *high-bandwidth*, dan keandalan tinggi serta jaringan pita lebar nirkabel metropolitan;

— lapisan akuisisi data memberikan kapabilitas untuk merasakan dunia dan mengambil tindakan; dan

— sistem vertikal termasuk sistem proteksi keamanan dan privasi, sistem konstruksi, sistem operasi dan pemeliharaan, sistem identifikasi, dan sistem pemosisian.



Gambar 5 — Kerangka kerja manajemen rekayasa kota cerdas

5.2.2 Aktivitas manajemen privasi dalam seri ISO/IEC 30145

Proses dari kerangka kerja referensi TIK kota cerdas dapat termasuk aktivitas manajemen privasi:

— dalam kerangka kerja proses bisnis, proses dapat termasuk aktivitas tambahan yang terkait dengan PII:

  — proses sistem dan layanan hukum dan regulatori dapat berurusan dengan kepentingan regulasi privasi untuk memastikan kepatuhan privasi;

  — proses keselamatan, keamanan, dan resiliensi dapat berurusan dengan insiden yang menyebabkan pelanggaran privasi;

  — proses kepemimpinan dan pengarahan dapat berurusan dengan tata kelola PII;

  — proses keterlibatan pemangku kepentingan dan fokus warga kota dapat menangani pertanyaan warga kota mengenai PII mereka;

— dalam kerangka kerja manajemen pengetahuan, basis pengetahuan dapat termasuk PII. Misalnya, pengetahuan tentang asal usul data dapat memberikan hubungan antara PII *principal* dan data;

— dalam kerangka kerja manajemen rekayasa, semua lapisan tertentu, yaitu lapisan aplikasi cerdas, lapisan pendukung data dan layanan, lapisan komputasi dan penyimpanan, lapisan komunikasi jaringan, dan lapisan akuisisi data dapat melibatkan data yang mengarah ke PII.

5.3 Aktor

Bergantung pada sudut pandang, aktor spesifik sebaiknya dipertimbangkan dalam visi kota cerdas yang memanfaatkan TIK (misalnya IoT, data raya, KA), dan yang mensyaratkan pandangan sistem dari sistem-sistem untuk memungkinkan integrasi sistem sektor spesifik (misalnya energi, transportasi, kesehatan). Bergantung pada sudut pandang (privasi, kota cerdas, komputasi awan, IoT, data raya), aktor spesifik sebaiknya dipertimbangkan dalam lingkungan kota cerdas.

Dalam aktivitas yang berkaitan dengan privasi, aktor berikut didefinisikan dalam ISO/IEC 29100:

— PII *principal*;

— pengontrol PII;

— prosesor PII; dan

— pihak ketiga.

Dalam aktivitas yang berkaitan dengan pertukaran dan berbagi data untuk infrastruktur komunitas cerdas, peran berikut didefinisikan dalam ISO 37156:

— kreator data, yang membuat, menangkap, mengumpulkan, atau mentransformasi data untuk misalnya kota atau layanan;

— pemilik data yang merupakan aktor yang ditentukan dan bertanggung jawab atas data terkait layanan kota. Mereka mendefinisikan, memvalidasi setiap atribut yang inheren pada data;

— kustodian data yang merupakan penjaga data untuk tujuan atau tugas spesifik yang berkaitan dengan penyediaan layanan di dalam kota;

— penerbit utama yang melakukan publikasi untuk semua data pada seluruh spektrum data;

— penerbit sekunder yang menciptakan nilai tambah dari data kota yang telah dipublikasikan; dan

— pengguna, misalnya organisasi kota, organisasi sektor ketiga, pengguna bisnis, warga kota, organisasi akademik atau kota lain.

Dalam aktivitas yang berkaitan dengan *cloud*, aktor berikut didefinisikan dalam ISO/IEC 17789:

— pelanggan layanan *cloud*;

— mitra layanan *cloud*; dan

— penyedia layanan *cloud*.

Pelanggan layanan *cloud* menggunakan layanan *cloud* untuk tujuan hubungan bisnis. Penyedia layanan *cloud* menyediakan layanan *cloud*. Mitra layanan *cloud* terlibat dalam mendukung, atau membantu, aktivitas penyedia layanan *cloud* atau pelanggan layanan *cloud*.

Dalam aktivitas berkaitan dengan IoT, aktor berikut didefinisikan dalam ISO/IEC 30141:

— pengguna IoT;

— penyedia layanan IoT; dan

— developer layanan IoT.

Peran pengguna IoT mengadministrasikan dan mengonsumsi layanan IoT. Peran penyedia layanan IoT mengelola dan mengoperasikan layanan IoT. Peran developer layanan IoT mengimplementasikan, menguji, dan mengintegrasikan layanan IoT.

Dalam aktivitas berkaitan dengan data raya, aktor berikut didefinisikan dalam ISO/IEC 20547-3:

— konsumen data raya;

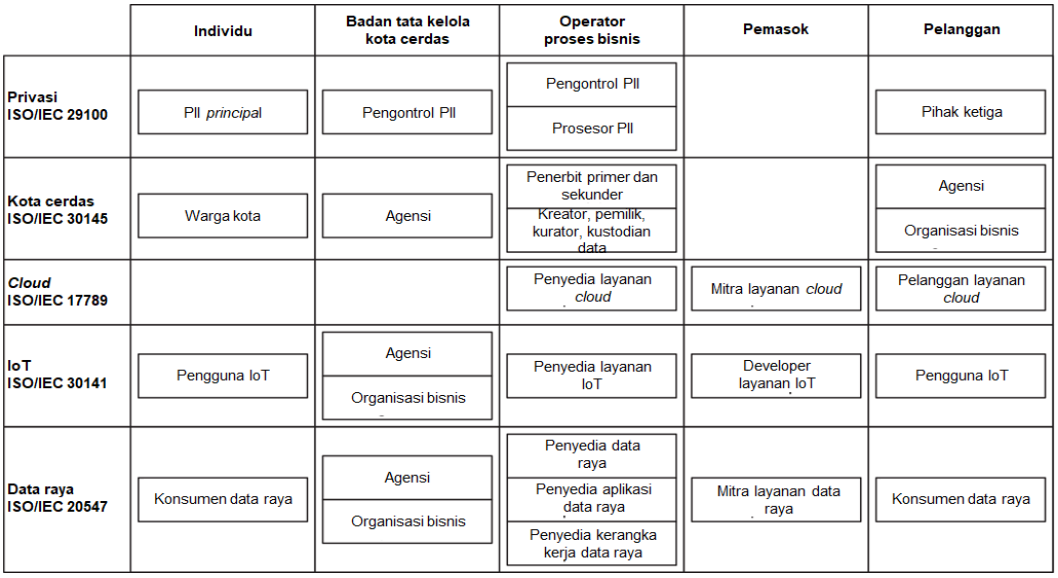
— penyedia data raya;

— penyedia aplikasi data raya;

— penyedia kerangka kerja data raya; dan

— mitra layanan data raya.

Peran konsumen data raya mengonsumsi nilai output dari sistem data raya. Peran penyedia data raya adalah untuk menyediakan data. Peran penyedia aplikasi data raya adalah melaksanakan manipulasi siklus hidup data. Peran penyedia kerangka kerja data raya adalah menyediakan infrastruktur data raya, platform data raya, dan pemrosesan data raya. Peran mitra layanan data raya adalah mendukung penyedia aplikasi data raya, penyedia data raya, dan konsumen data raya.



Gambar 6 — Pemangku kepentingan di kota cerdas dan hubungannya dengan mereka yang didefinisikan dalam standar relevan lainnya

Gambar 6 menunjukkan lima kategori pemangku kepentingan: individu, penanggung jawab tata kelola kota cerdas, operator proses bisnis, pemasok, dan pelanggan. Untuk setiap kategori, diberikan contoh aktor dan peran, dengan mengambil sudut pandang privasi (ISO/IEC 29100), sudut pandang kota cerdas (seri ISO/IEC 30145), sudut pandang *cloud* (ISO/IEC 17789), sudut pandang IoT (ISO/IEC 30141), dan sudut pandang data raya (ISO/IEC 20547-3):

- individu dapat merupakan:
  - PII *principal* yang terkena dampak pelanggaran privasi;
  - warga kota yang tergabung dalam atau yang mengunjungi kota cerdas;
  - pelanggan layanan *cloud*;
  - pengguna IoT dari layanan IoT; dan
  - konsumen data raya;
- penanggung jawab tata kelola kota cerdas dapat merupakan:
  - pengontrol PII yang menentukan tujuan dan sarana pemrosesan PII;
  - agensi yang melakukan tugas tata kelola secara keseluruhan;
  - agensi atau organisasi bisnis yang melakukan tugas tata kelola dalam layanan *cloud*;
  - agensi atau organisasi bisnis yang melakukan tugas tata kelola pada layanan IoT;
  - agensi atau organisasi bisnis yang melakukan tugas tata kelola pada layanan data raya;
- operator proses bisnis dapat merupakan:
  - pengontrol PII atau prosesor PII;
  - pemangku kepentingan yang terlibat dalam pertukaran dan berbagi data dengan peran seperti penerbit primer dan sekunder, kreator data, pemilik, kurator, kustodian;
  - penyedia layanan *cloud*;
  - penyedia layanan IoT; dan
  - penyedia data raya, penyedia aplikasi data raya, atau penyedia kerangka kerja data raya;
- pemasok dapat merupakan:
  - operator jaringan atau infrastruktur;
  - mitra layanan *cloud*;
  - developer layanan IoT;
  - mitra layanan data raya; dan

— pelanggan dapat merupakan:

  — warga kota atau pihak ketiga;

  — organisasi atau agensi pemerintah;

  — organisasi nonpemerintah;

  — organisasi bisnis;

  — konsumen layanan *cloud*;

  — pengguna IoT; dan

  — konsumen data raya.

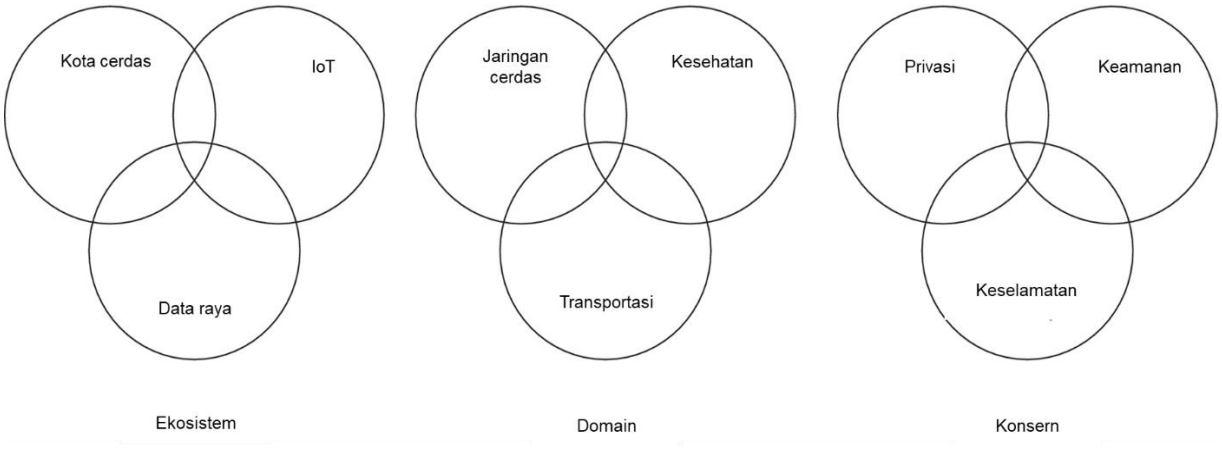
5.4 Tantangan

Gambar 7 mengilustrasikan integrasi permasalahan dalam kota cerdas:

— IoT dan data raya merupakan ekosistem teknologi yang harus diintegrasikan dalam ekosistem kota cerdas. Banyak aplikasi kota cerdas yang merupakan aplikasi data raya[1]. Banyak sistem TIK kota cerdas adalah sistem IoT. Sebagaimana dinyatakan oleh Andrea Zanella,[29] IoT memiliki kapabilitas “untuk memasukkan sejumlah besar sistem akhir yang berbeda dan heterogen secara transparan dan mulus, sekaligus menyediakan akses terbuka ke *subset* dari data terpilih untuk pengembangan sejumlah besar layanan digital”;

— integrasi antar domain yang berbeda, seperti jaringan cerdas, kesehatan, transportasi; dan

— menjaga kepercayaan pada layanan yang memerlukan integrasi konsern multipel seperti keamanan, privasi, keselamatan, dan resiliensi. Misalnya, meningkatnya kombinasi titik data dapat meningkatkan risiko pembuatan PII.



Gambar 7 — Contoh ekosistem, domain, dan konsern

[1] Misalnya di Amsterdam (https://data.amsterdam.nl/), Berlin (https://daten.berlin.de/), London (https://data.london.gov.uk/) atau Paris (https://opendata.paris.fr)

Kebutuhan untuk mengintegrasikan privasi berdampak pada hal-hal berikut:

— pendekatan tata kelola yang diasosiasikan dengan konsern seperti keselamatan, keamanan, dan privasi. Misalnya, otoritas proteksi data mungkin memberikan aturan tingkat tinggi (yaitu pernyataan tentang apa yang harus dilakukan mengenai privasi) dan kebijakan yang, pada gilirannya, digunakan oleh penanggung jawab tata kelola kota cerdas untuk memastikan langkah-langkah kepatuhan spesifik. Hal ini memastikan aturan dan kebijakan yang tepat dalam ekosistem kota cerdas;

— rantai pasokan yang diasosiasikan dengan menghasilkan, pengumpulan, agregasi, dan transportasi data di kota cerdas. Misalnya, data yang dikumpulkan oleh meteran cerdas dan selanjutnya diagregasikan untuk analisis data melibatkan sejumlah organisasi (misalnya pemanufaktur meteran cerdas, utilitas jaringan cerdas, analis data); dan

— ekosistem berbagi data yang diasosiasikan dengan analisis data di suatu kota cerdas. Misalnya, banyak organisasi dapat terlibat dalam berbagi data energi untuk meningkatkan penggunaannya di berbagai domain (misalnya transportasi, kesehatan, infrastruktur publik).

Isu berikut sebaiknya dipertimbangkan.

— Dalam pendekatan tata kelola, melacak daftar pengontrol PII dan prosesor PII untuk memenuhi prinsip akuntabilitas. Misalnya, terjadinya insiden privasi dapat mengharuskan tindakan yang berdampak pada pemangku kepentingan spesifik.

— Dalam rantai pasokan, mengidentifikasi bagaimana pemasok mendukung privasi dan berkomunikasi dengan mereka untuk menegakkan aturan dan kebijakan. TIK mencakup berbagai produk, produk akhir seperti sensor, peranti, peranti cerdas, solusi *cloud*, atau produk komponen seperti elektronik, modul keamanan, sistem operasi, perangkat tengah (*middleware*). Pemasok sebaiknya menyediakan tindakan teknis dan organisasi privasi yang sesuai. Misalnya, pemanufaktur sistem penyimpanan dapat menyertakan kontrol yang akan membantu pengontrol PII atau prosesor PII.
— Dalam ekosistem berbagi data, menegakkan perjanjian berbagi data privasi yang eksplisit ketika PII diproses dan dipertukarkan.

— Kebutuhan untuk mempertimbangkan ekspektasi individu termasuk hak untuk mendapatkan informasi, memberikan informasi, mengoreksi, memperbaiki, mengembalikan, dan memulihkan.

Tabel 2 menunjukkan contoh kerentanan bisnis di kota cerdas.

Tabel 2 — Contoh kerentanan bisnis di kota cerdas

Aspek bisnis	Kerentanan
Tata kelola	Penanggung jawab pengelola layanan kota cerdas tidak dapat melacak semua pengontrol PII atau prosesor PII. Misalnya, badan tersebut tidak dapat mengidentifikasi pengontrol PII atau prosesor PII yang menyebabkan pelanggaran.
	Penanggung jawab pengelola kota cerdas belum menetapkan aturan dan kebijakan yang jelas untuk privasi. Badan tersebut tidak dapat menegakkan kebijakan privasi diantara pengontrol PII dan prosesor PII.
Rantai pasokan	Asesmen dampak privasi yang diberikan pemasok tidak komplet atau tidak akurat. Misalnya, mereka dapat tidak menyadari beberapa risiko privasi.
	Pengontrol PII atau prosesor PII mengandalkan pemasok komponen yang tidak mendukung kontrol privasi yang diinginkan. Misalnya, sistem penyimpanan tidak menyertakan kapabilitas penghapusan otomatis.
Ekosistem berbagi data	Pemangku kepentingan dalam ekosistem berbagi data lalai dalam menegakkan kewajiban. Misalnya, seorang pemangku kepentingan memberikan PII kepada pemangku kepentingan lain tanpa menginformasikan kepada pemangku kepentingan tersebut tentang kewajibannya.
	Asesmen yang salah dari pemangku kepentingan bahwa itu bukan pengontrol PII atau prosesor PII. Misalnya, memublikasikan data terbuka yang tidak dianonimkan dengan benar, atau mengombinasikan dua *dataset* yang tidak berisi PII ke satu *dataset* yang berisi PII.

6 Panduan pada proteksi privasi ekosistem kota cerdas

6.1 Rencana privasi ekosistem

6.1.1 Rekomendasi R6.1

Penanggung jawab tata kelola kota cerdas sebaiknya menetapkan rencana privasi ekosistem.

6.1.2 Penjelasan

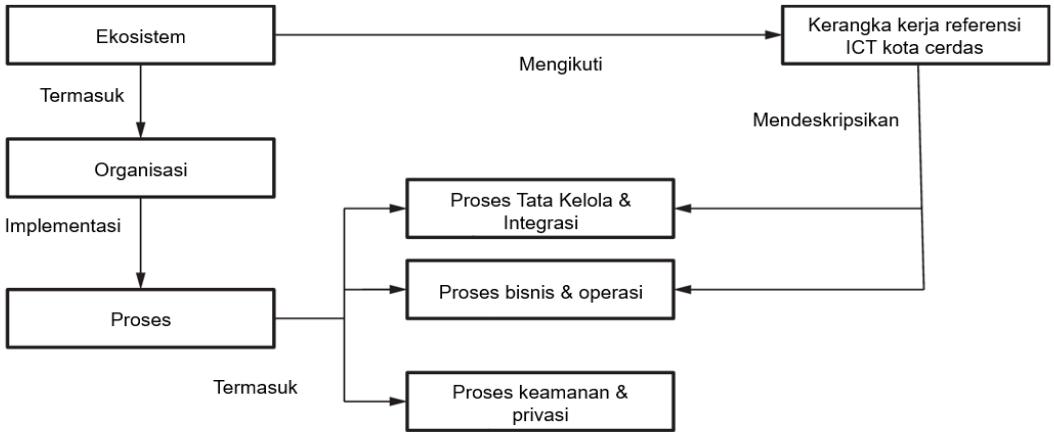
Gambar 8 mendeskripsikan hubungan di antara organisasi, proses, dan kerangka kerja referensi TIK kota cerdas sebagaimana dideskripsikan dalam 5.1 Umum:

— organisasi adalah bagian dari ekosistem yang mengikuti kerangka kerja referensi TIK cerdas;

— kerangka kerja referensi TIK cerdas mendeskripsikan proses tata kelola dan integrasi serta proses bisnis dan operasi;

— organisasi mengimplementasikan proses yang terkait dengan peran, aktivitas, dan komponen fungsional. Misalnya, sebuah organisasi dapat bertanggung jawab atas peran penyedia aplikasi data raya; dan

— organisasi mengimplementasikan proses dengan berfokus pada keamanan dan privasi. Hal ini diaplikasikan untuk melindungi aset di dalam kerangka referensi TIK kota cerdas dari kerentanan. Beberapa aset adalah spesifik untuk suatu organisasi, misalnya informasi sensitif yang komersial sementara informasi lain dibagikan dalam ekosistem, misalnya data terbuka. Organisasi dapat menunjuk pejabat proteksi data yang bertugas memastikan, secara independen, kepatuhan terhadap proses.

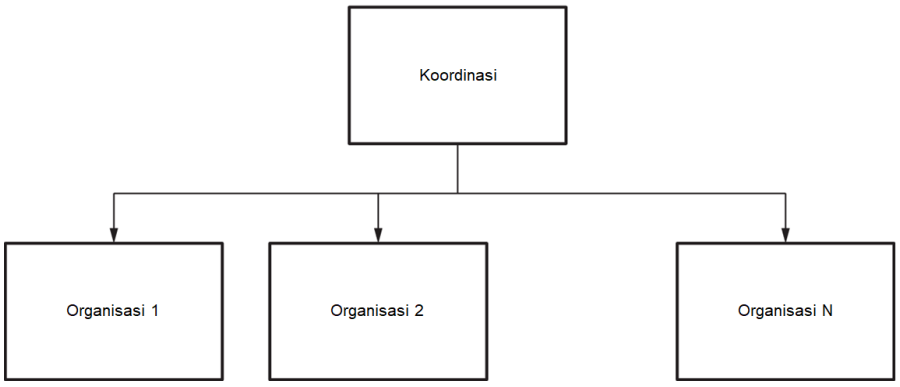


Gambar 8 — Organisasi dalam ekosistem kota cerdas

Terdapat kebutuhan untuk mengoordinasikan proses organisasi di dalam ekosistem kota cerdas, sebagaimana ditunjukkan pada Gambar 9:

— koordinasi keseluruhan oleh penanggung jawab pengelola layanan kota cerdas memastikan konsistensi setiap proses; dan

— setiap organisasi menjalankan prosesnya;



Gambar 9 — Koordinasi ekosistem organisasi

6.1.3 Produk kerja

Koordinasi dibangun melalui rencana privasi ekosistem kota cerdas. Lampiran A memberikan contoh struktur rencana privasi ekosistem.

6.2 Tata kelola

6.2.1 Rekomendasi R6.2

Rencana privasi ekosistem sebaiknya menentukan operasi penanggung jawab tata kelola.

6.2.2 Penjelasan

Koordinasi privasi dalam ekosistem kota cerdas dikelola oleh penanggung jawab pengelola. Penangung jawab pengelola dapat mengambil bentuk yang berbeda-beda, misalnya otoritas publik, organisasi khusus, aliansi. Mereka dapat dikhususkan untuk domain spesifik. Misalnya:

— organisasi yang terlibat dalam manajemen lalu lintas cerdas mengaplikasikan proses keamanan dan privasi yang dikoordinasikan oleh agensi transportasi kota;

— organisasi yang terlibat dalam data raya kesehatan mengaplikasikan proses keamanan dan privasi yang dikoordinasikan oleh agensi kesehatan kota; dan

— organisasi yang terlibat dalam layanan jaringan energi mengaplikasikan proses keamanan dan privasi yang dikoordinasikan oleh kelompok kerja *ad-hoc* yang berkoordinasi dengan agensi jaringan energi.

Koordinasi tersebut dapat melibatkan pejabat proteksi data dari penanggung jawab pengelola dan dari organisasi pada ekosistem.

6.2.3 Produk kerja

Rencana privasi ekosistem kota cerdas mendeskripsikan penanggung jawab tata kelola serta aturan dan prosedurnya.

6.3 Rantai pasokan

6.3.1 Rekomendasi R6.3

Rencana privasi ekosistem sebaiknya termasuk manajemen rantai pasokan.

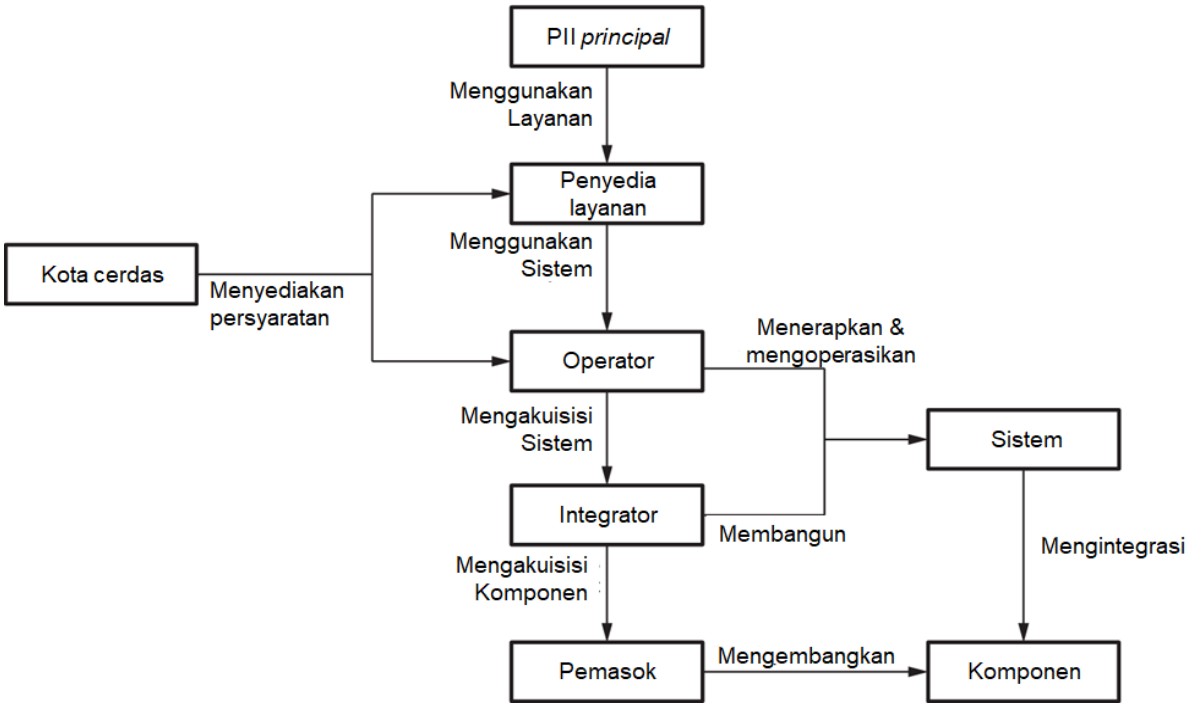
6.3.2 Penjelasan

Manajemen rantai pasokan memastikan bahwa pengaturan kontraktual mengenai privasi sudah memadai. Mereka memastikan hal-hal berikut:

— pengontrol PII dan prosesor PII dalam rantai pasokan menyadari aturan dan kebijakan privasi di dalam ekosistem kota cerdas;

— prosesor PII menerima instruksi yang tepat dari pengontrol PII (misalnya melalui perjanjian berbagi data privasi); dan

— pemasok kepada pengontrol PII dan prosesor PII mempertimbangkan aturan dan kebijakan privasi tersebut. (ditransmisikan, misalnya, melalui persyaratan kontraktual).



Gambar 10 — Contoh rantai pasokan kota cerdas

Gambar 10 menyediakan contoh rantai pasokan untuk pembuatan suatu sistem. Ini melibatkan pemangku kepentingan berikut:

— pemasok yang menyediakan komponen yang membentuk sistem, misalnya sensor, perangkat cerdas, sistem *cloud*;

— integrator yang membangun sistem, mengintegrasikan berbagai komponen yang diperoleh dari pemasok;

— operator yang menerapkan, mengoperasikan, dan memelihara sistem yang diperoleh dari integrator;

— penyedia layanan yang menggunakan sistem untuk memberikan layanan kepada pengguna akhir;

— otoritas kota cerdas yang memberikan persyaratan kepada penyedia dan operator aplikasi mengenai suatu layanan; dan

— PII *principal* yang menggunakan layanan yang disediakan oleh penyedia layanan.

Berikut ini adalah contoh aplikasi transportasi cerdas yang menyediakan advis lalu lintas waktu riil kepada warga kota. PII *principal* adalah penduduk suatu kota. Penyedia layanan adalah agensi transportasi kota. Operator adalah UKM lokal yang berasosiasi dengan operator *cloud* internasional yang besar. Integrator adalah perusahaan yang sangat besar dengan pengalaman membangun sistem yang kompleks. Pemasok adalah produsen perangkat lokal (misalnya sistem displai), perusahaan rintisan eksternal yang menyediakan fitur untuk advis waktu riil, dan penyedia sistem operasi yang besar.

Rantai pasokan dimodifikasi seperti ditunjukkan pada Gambar 11 ketika konsern privasi diintegrasikan:

— pemasok menyediakan komponen yang mengimplementasikan kontrol privasi yang sesuai dengan persyaratan pengontrol PII dan prosesor PII (misalnya teknik de-identifikasi);

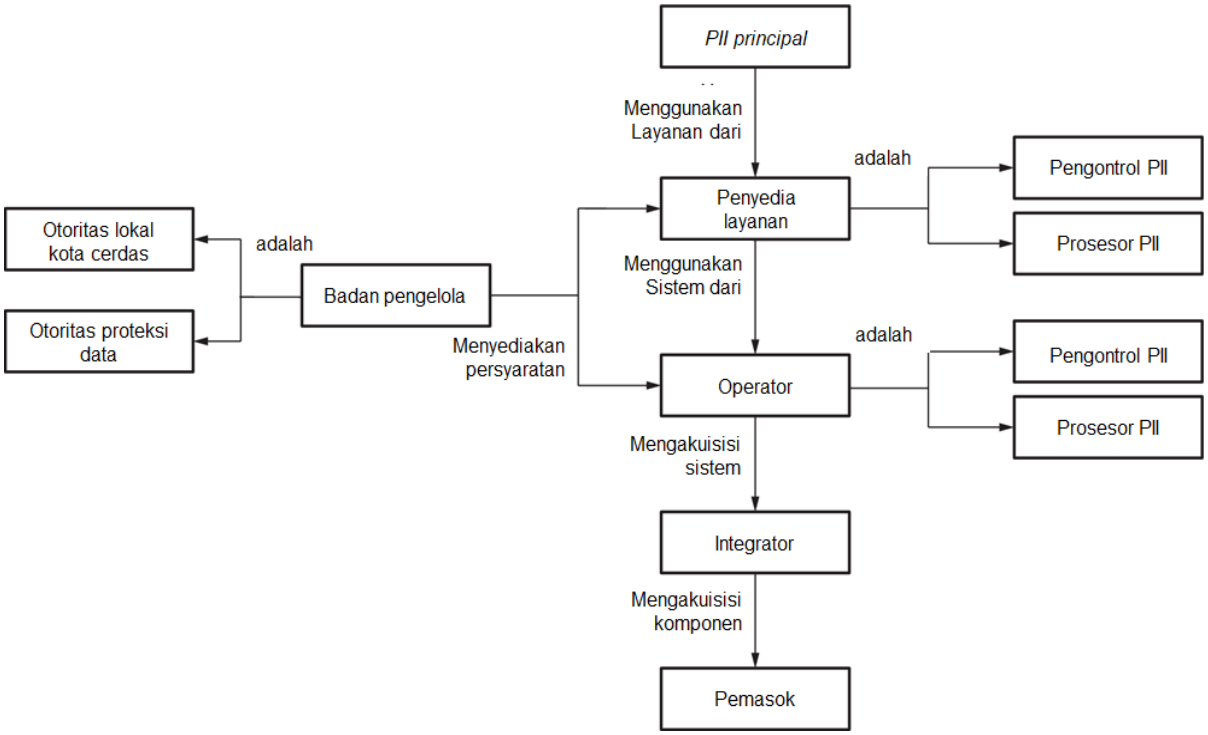
— integrator sebaiknya menyediakan keseluruhan kontrol privasi dengan mengintegrasikan kontrol yang disediakan oleh pemasok;

— pengontrol PII dan prosesor PII menjalankan operasi yang berkaitan dengan manajemen privasi (misalnya manajemen persetujuan, manajemen pelanggaran privasi);

— otoritas proteksi data dan otoritas lokal kota cerdas memberikan aturan dan kebijakan spesifik kepada pengontrol PII dan prosesor PII, misalnya beberapa pedoman analisis dampak privasi;

— penyedia layanan mendapatkan pedoman privasi dari otoritas proteksi data;

— PII *principal* yang menggunakan layanan tersebut dilindungi dengan baik sesuai dengan aturan dan kebijakan privasi.



Gambar 11— Contoh rantai pasokan kota cerdas yang mengintegrasikan privasi

6.3.3 Produk kerja

Rencana privasi ekosistem kota cerdas mendeskripsikan koordinasi rantai pasokan.

6.4 Manajemen data

6.4.1 Rekomendasi R6.4

Rencana privasi ekosistem sebaiknya mencakup manajemen data.

6.4.2 Penjelasan

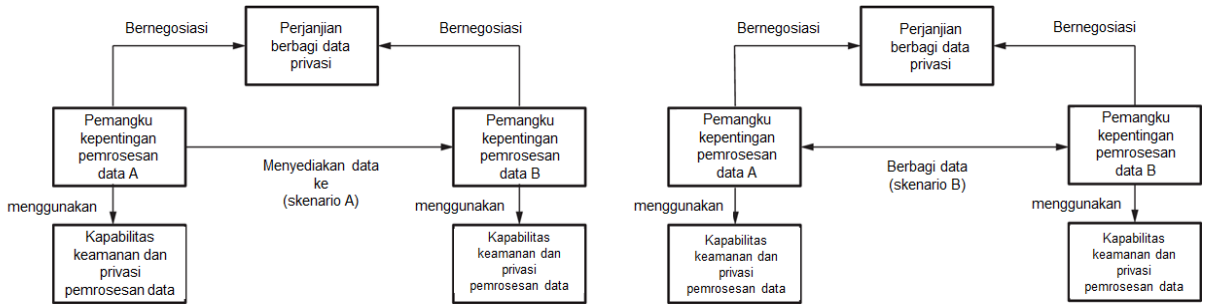
Pemangku kepentingan pemrosesan data selanjutnya terlibat dalam ekosistem berbagi data. Integrasi keamanan dan privasi dalam rantai nilai ini digambarkan oleh Gambar 12:

— dua pemangku kepentingan pemrosesan data A dan B menegosiasikan perjanjian berbagi data, dimana:

  — A adalah pengontrol PII dan menyediakan data kepada B yang adalah prosesor PII atau pengontrol PII (skenario A); atau

  — A dan B adalah pengontrol bersama (skenario B);

— perjanjian berbagi data privasi menetapkan kewajiban pada kapabilitas keamanan dan privasi pemrosesan data yang disediakan setiap pemangku kepentingan.



Gambar 12 — Perjanjian berbagi data dari sudut pandang keamanan dan privasi

Koordinasi privasi dalam manajemen data memastikan bahwa:

— pengontrol PII dan prosesor PII di dalam rantai pasokan menyadari aturan dan kebijakan privasi dalam ekosistem kota cerdas;

— prosesor PII menerima instruksi yang tepat dari pengontrol PII (misalnya melalui perjanjian berbagi data privasi);

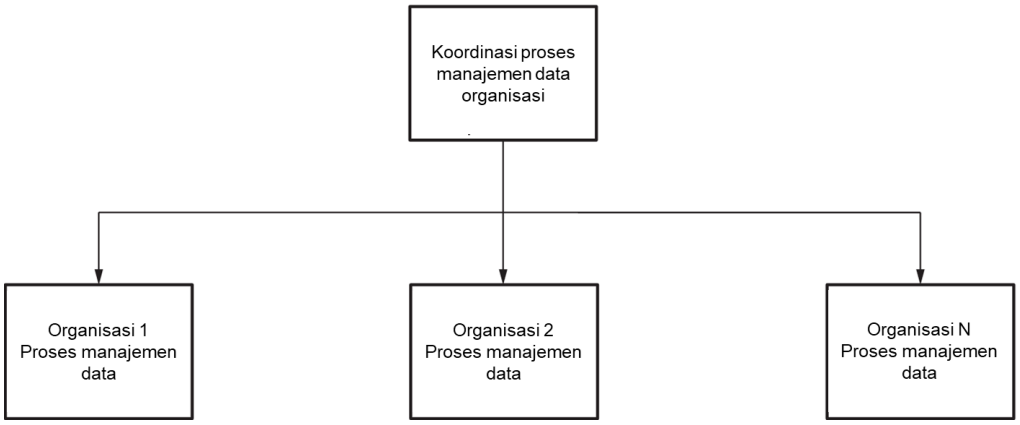
— pemasok kepada pengontrol PII dan prosesor PII mempertimbangkan aturan dan kebijakan privasi tersebut; dan

— jika verifikasi kepatuhan dipersyaratkan oleh proses tata kelola, tentukan pemangku kepentingan audit yang bertanggung jawab atas kepatuhan.

Misalnya, operator sistem IoT mengumpulkan data yang disediakan sebagai *dataset* ke penyedia layanan yang pada gilirannya menggabungkannya dengan sumber data lain dan memberikannya kepada konsumen data. Sebagaimana ditunjukkan pada Gambar 13:

— koordinasi keseluruhan proses manajemen data setiap organisasi untuk memastikan bahwa mereka mengikuti aturan dan kebijakan privasi yang kompatibel; dan

— setiap organisasi melakukan proses manajemen datanya sendiri.



Gambar 13 — Manajemen ekosistem berbagi data kota cerdas

6.4.3 Produk kerja

Rencana privasi ekosistem kota cerdas mendeskripsikan koordinasi manajemen data.

7 Panduan tentang standar proteksi privasi ekosistem kota cerdas

7.1 Umum

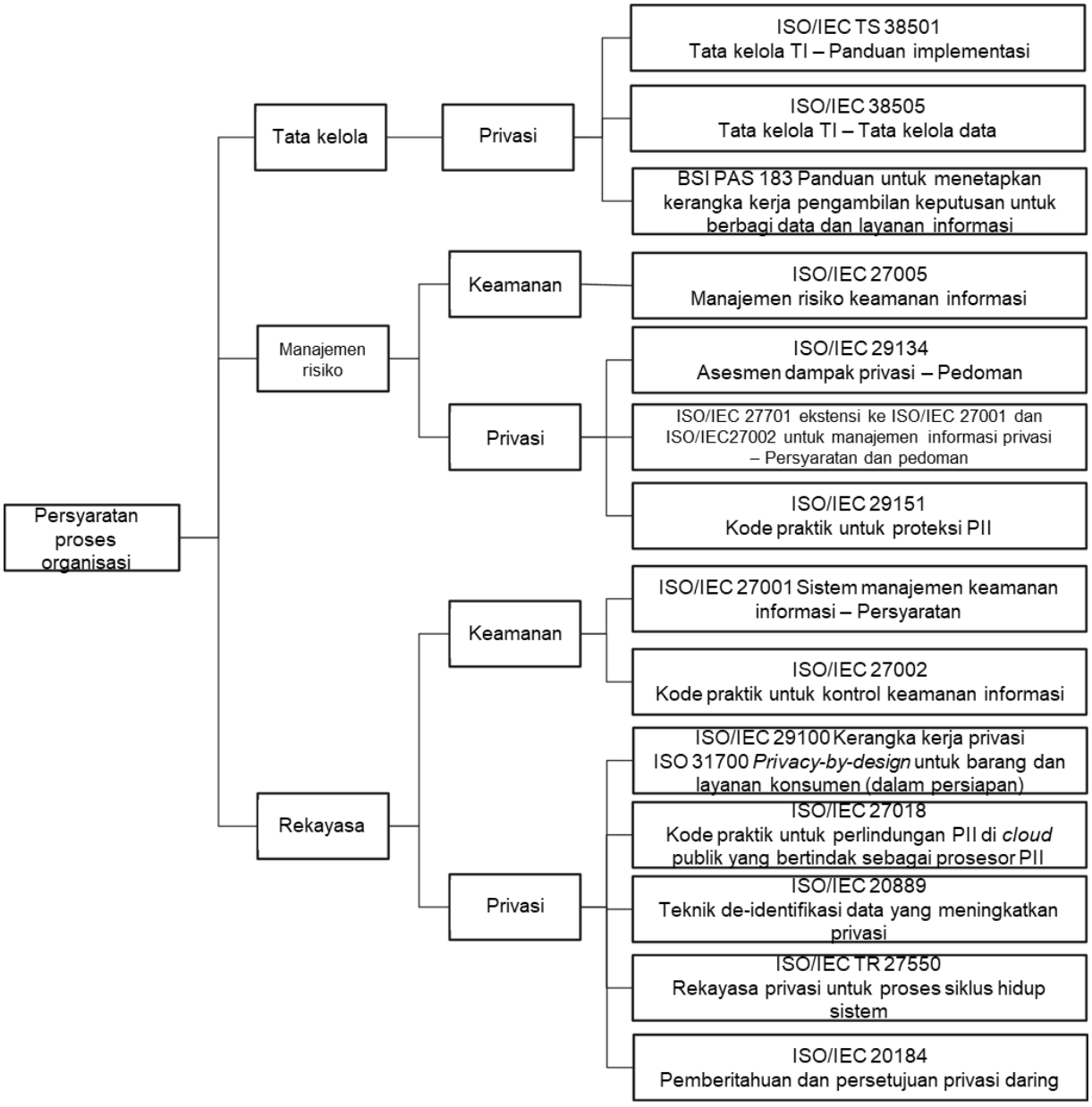
Gambar 14 menunjukkan berbagai standar yang dapat digunakan untuk memandu organisasi dalam mendukung keamanan dan privasi. Standar-standar tersebut mencakup standar untuk:

— proses tata kelola (8.2 Proses tata kelola);

— proses manajemen risiko (8.4 Proses manajemen risiko); dan

— proses rekayasa (8.5 Proses rekayasa).

CATATAN Standar-standar ini dapat dilengkapi dengan dokumen panduan lebih lanjut (misalnya standar lokal).



Gambar 14 — Standar untuk proses privasi organisasi

7.2 Tata kelola privasi

Proses privasi kota cerdas yang berurusan dengan tata kelola dapat mengikuti standar berikut:

— panduan implementasi tata kelola TI sebagaimana dideskripsikan pada ISO/IEC TS 38501;

— tata kelola TI untuk data sebagaimana dideskripsikan dalam ISO/IEC 38505 (semua bagian);

— panduan untuk menetapkan kerangka kerja pengambilan keputusan untuk berbagi data dan layanan informasi sebagaimana dideskripsikan dalam BSI PAS 183; dan

— koordinasi ekosistem sebagaimana dideskripsikan dalam dokumen ini.

7.3 Manajemen Risiko Privasi

Proses privasi kota cerdas yang berurusan dengan manajemen risiko dapat mengikuti standar berikut:

— manajemen risiko keamanan informasi sebagaimana dideskripsikan dalam ISO/IEC 27005;

— pedoman asesmen dampak privasi sebagaimana dideskripsikan dalam ISO/IEC 29134;

— persyaratan privasi sistem informasi kota cerdas sebagaimana dideskripsikan dalam ISO/IEC 27701;

— kode praktik untuk proteksi PII sebagaimana dideskripsikan dalam ISO/IEC 29151; dan

— koordinasi ekosistem sebagaimana dideskripsikan dalam dokumen ini

7.4 Rekayasa privasi

Proses privasi kota cerdas yang berurusan dengan rekayasa dapat mengikuti standar siklus hidup berikut:

— persyaratan keamanan sistem informasi kota cerdas sebagaimana dideskripsikan dalam ISO/IEC 27001;

— kode praktik untuk kontrol keamanan informasi sebagaimana dideskripsikan dalam ISO/IEC 27002;

— persyaratan privasi sistem kota cerdas yang dihasilkan dari penggunaan prinsip privasi sebagaimana dideskripsikan dalam ISO/IEC 29100;

— kode praktik untuk proteksi PII di *cloud* publik yang bertindak sebagai prosesor PII sebagaimana dideskripsikan dalam ISO/IEC 27018;

— teknik de-identifikasi data yang meningkatkan privasi sebagaimana dideskripsikan dalam ISO/IEC 20889;

— rekayasa privasi sebagaimana dideskripsikan dalam ISO/IEC TR 27550;

— pemberitahuan dan persetujuan privasi daring sebagaimana dideskripsikan dalam ISO/IEC 29184; dan

— koordinasi ekosistem sebagaimana dideskripsikan dalam dokumen ini.

8 Panduan tentang proses proteksi privasi ekosistem kota cerdas

8.1 Umum

Pasal ini memberikan pedoman privasi untuk pembuatan, desain, penerapan, dan operasi layanan kota cerdas, dengan berfokus pada proses berikut:

— tata kelola;

— manajemen data;

— manajemen risiko;

— rekayasa; dan

— keterlibatan warga kota.

Pedoman untuk setiap proses disediakan dengan konten berikut:

— rekomendasi;

— penjelasan mengenai aktivitas pada level ekosistem global;

— pedoman untuk koordinasi ekosistem (dilakukan oleh penanggung jawab tata kelola kota cerdas);

— pedoman untuk organisasi;

— standar dan metode yang dapat digunakan;

— contoh-contoh; dan

— produk kerja yang mendeskripsikan proses.

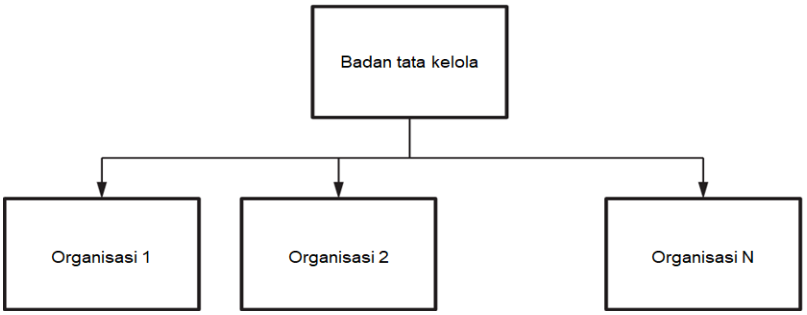
8.2 Proses tata kelola

8.2.1 Rekomendasi R8.2

Proses tata kelola sebaiknya ditetapkan oleh penanggung jawab tata kelola layanan kota cerdas untuk memastikan koordinasi manajemen privasi ekosistem kota cerdas.

8.2.2 Penjelasan

Proses tata kelola berfokus pada penetapan kebijakan privasi, dan pemonitoran berkelanjutan terhadap implementasinya yang tepat dalam layanan kota cerdas. Aktivitas ini dilakukan oleh penanggung jawab pengelola kota cerdas, serta oleh organisasi dalam ekosistem yang mengimplementasikan kebijakan privasi, seperti ditunjukkan pada Gambar 15.



Gambar 15 — Pemangku kepentingan proses tata kelola

8.2.3 Panduan tentang koordinasi ekosistem

Panduan berikut disediakan pada level ekosistem:

— mengases apakah pembuatan layanan kota cerdas memerlukan tata kelola privasi yang spesifik. Pada kasus ini:

— menspesifikasikan aturan dan kebijakan tata kelola privasi baru;

— menspesifikasikan tata kelola privasi yang mendeskripsikan persyaratan pengawasan, dan aktivitas pengawasan yang dihasilkan;

CATATAN 1 Aturan dan kebijakan termasuk pedoman untuk kebijakan retensi data antarorganisasi yang berbagi data.

— mengases apakah program kompetensi privasi (regulasi, teknis, dan organisasi) sebaiknya diimplementasikan dan menyertakan manfaat dari asesmen dalam proses tata kelola, manajemen risiko, manajemen data, rekayasa privasi, dan keterlibatan warga kota.

CATATAN 2 Contoh regulasi di Eropa adalah GDPR.

— mengidentifikasi organisasi yang diawasi untuk tata kelola privasi dan tanggung jawab mereka (misalnya pengontrol PII, prosesor PII, integrator, atau pemasok);

— menetapkan dan mengimplementasikan aktivitas komunikasi dan supervisi, memastikan bahwa aturan dan kebijakan dikomunikasikan dengan baik kepada organisasi dan diimplementasikan serta jika diperlukan berinteraksi dengan organisasi spesifik di dalam ekosistem (misalnya komplain warga kota, insiden pelanggaran privasi); dan

— menetapkan dan mengimplementasikan prosedur yang tepat untuk proteksi hak warga kota dan berinteraksi sepanjang proses dengan otoritas proteksi data.

CATATAN 3 Aktivitas komunikasi termasuk persyaratan pertukaran informasi, perjanjian mengenai kontrol yang diaplikasikan, dan kapabilitas audit.

8.2.4 Panduan untuk organisasi

Panduan berikut disediakan pada level organisasi:

— meminta pembuatan tata kelola privasi kepada penanggung jawab tata kelola kota cerdas atau, jika tata kelola sudah ada, meminta partisipasi dalam proses tata kelola;

— berpartisipasi dalam program kompetensi;

— berpartisipasi dalam aktivitas komunikasi dan supervisi;

— mengimplementasikan langkah-langkah yang memenuhi aturan dan kebijakan yang berasosiasi dengan tata kelola privasi dan, jika sesuai, berinteraksi dengan penanggung jawab tata kelola (misalnya komplain warga kota, insiden pelanggaran privasi); dan

— berinteraksi dengan penanggung jawab tata kelola untuk memberikan informasi yang dipersyaratkan untuk supervisi.

8.2.5 Standar dan metode

Standar dan metode berikut dapat digunakan:

— seri ISO/IEC 30145 digunakan sebagai kerangka kerja keseluruhan;

— ISO/IEC 38500 digunakan oleh penanggung jawab pengelola untuk mengatur penggunaan TI melalui tiga tugas; mengevaluasi, mengarahkan, dan memonitor;

— ISO/IEC TS 38501 digunakan untuk mendukung implementasi proses tata kelola, melalui siklus tiga aktivitas: membangun dan mempertahankan lingkungan yang kondusif, mengelola TI, dan melakukan reviu berkelanjutan;

— ISO/IEC TR 38502 digunakan untuk membangun kerangka kerja tata kelola. Hal ini termasuk hal-hal berikut: prinsip tata kelola yang baik, strategi dan kebijakan penggunaan TI, perencanaan bisnis TI, sistem manajemen TI, penggunaan TI oleh organisasi, akuntabilitas dan manajemen risiko; dan

— ISO/IEC 38505-1 dan ISO/IEC TR 38505-2 digunakan untuk membangun tata kelola spesifik data.

CONTOH Kota cerdas menerapkan sensor untuk mengumpulkan data cuaca, data lalu lintas, atau data penggunaan energi. Dua layanan, aplikasi lalu lintas cerdas dan manajemen sumber daya energi diimplementasikan. Pelayanan pertama dioperasikan langsung oleh agensi kota (A). Layanan lainnya dioperasikan oleh organisasi privat (B). Keseluruhan program mencakup ekosistem organisasi (C, D, E) yang mengumpulkan, mengolah, dan menganalisis data. Beberapa data mengandung PII, misalnya data yang dikumpulkan oleh sensor di kendaraan. Akibatnya, pemerintah kota menetapkan proses tata kelola berdasarkan dokumen ini: dokumen ini mengidentifikasi agensi pengawas (A), dan organisasi yang diawasi: A dan B adalah pengontrol PII, C, D adalah prosesor PII, dan E adalah pemasok sensor. Agensi kota A mengimplementasikan aktivitas komunikasi dan supervisi dalam menangani perjanjian manajemen data. Hal ini mencakup aturan untuk informasi publik (misalnya dokumentasi terkait sensor yang diinstal di kendaraan). Hal ini juga mencakup aturan dan kebijakan untuk retensi data. Aktivitas ini memerlukan pertemuan dan reviu tahunan secara berkala yang mengarah pada keputusan peningkatan berkelanjutan. Pertemuan dan reviu tersebut diadakan oleh agensi kota A.

8.2.6 Produk kerja

Rencana privasi ekosistem mendeskripsikan proses tata kelola.

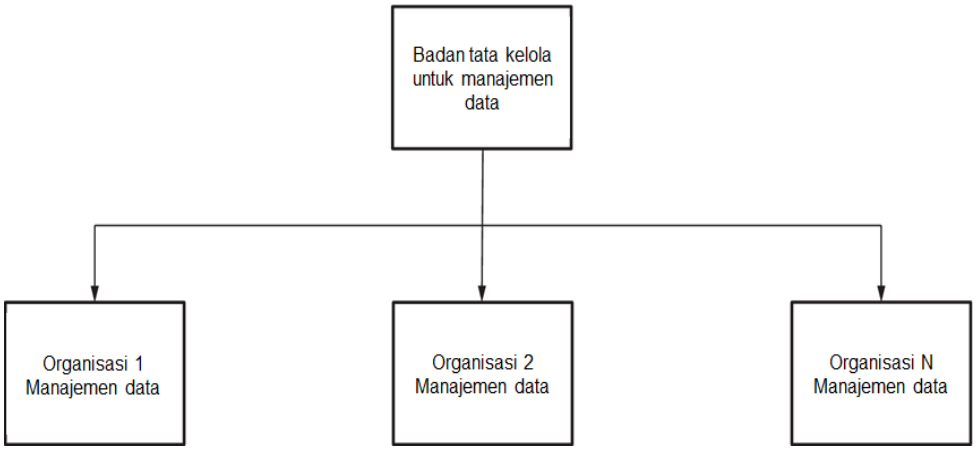
8.3 Proses manajemen data

8.3.1 Rekomendasi R8.3

Proses manajemen data sebaiknya ditetapkan oleh penanggung jawab tata kelola layanan kota cerdas untuk memastikan proteksi PII.

8.3.2 Penjelasan

Proses manajemen data berfokus pada manajemen privasi dalam pembuatan, penangkapan, pengumpulan, transformasi, pemublikasian, pengaksesan, pentransferan, dan pengarsipan data dalam layanan kota cerdas. Aktor dapat merupakan agensi kota cerdas atau pelaku bisnis. Aktivitas ini dilakukan oleh penanggung jawab pengelola kota cerdas, serta oleh organisasi di dalam ekosistem seperti yang ditunjukkan pada Gambar 16. Prasyarat untuk proses ini adalah sinkronisasi dengan proses tata kelola, manajemen risiko, dan rekayasa.



Gambar 16 — Pemangku kepentingan proses manajemen data

8.3.3 Panduan tentang koordinasi ekosistem

Panduan berikut disediakan pada level ekosistem:

— memulai proses tata kelola dan menunjukkan bahwa tujuan berbagi data adalah mematuhi kebijakan dan regulasi;

— memulai proses manajemen risiko seperti yang dipersyaratkan;

— memulai proses rekayasa seperti yang dipersyaratkan;

— menentukan templat asesmen dampak privasi dan perjanjian berbagi yang akan digunakan; dan

— menetapkan dan mengimplementasikan skema koordinasi di bidang ekosistem, mengenai:

  — partisipasi organisasi baru dalam komunitas berbagi data;

  — perluasan berbagi data ke aplikasi baru:

  — kepatuhan aplikasi berbagi data dengan kebijakan dan regulasi yang disepakati; dan

  — asurans dan audit praktik.

8.3.4 Panduan untuk organisasi

Panduan berikut disediakan pada level organisasi:

— memulai proses tata kelola seperti yang dipersyaratkan;

— memulai proses manajemen risiko seperti yang dipersyaratkan;

— memulai proses rekayasa seperti yang dipersyaratkan;

— menggunakan templat asesmen dampak privasi dan perjanjian berbagi yang direkomendasikan pada level koordinasi; dan

— melakukan aktivitas berbagi data sesuai dengan skema koordinasi ekosistem.

8.3.5 Standar dan metode

Standar dan metode berikut dapat digunakan:

— BSI PAS 183 digunakan untuk mengimplementasikan pendekatan yang transparan dalam pengambilan keputusan dan pembuatan perjanjian berbagi data yang spesifik;

— ISO 37156 menyediakan kerangka kerja untuk pertukaran dan berbagi data kepada entitas yang memiliki otoritas untuk mengembangkan dan mengoperasikan infrastuktur komunitas; dan

— ISO/IEC 29184 menyediakan kontrol, yang membentuk konten dan struktur pemberitahuan privasi daring serta proses meminta persetujuan untuk mengumpulkan dan memproses PII dari PII *principal*.

CONTOH 1 Agensi kota mengoperasikan infrastuktur untuk mengumpulkan data meteran cerdas untuk mengoptimalkan keseluruhan sumber daya energinya. Data dikumpulkan dengan persetujuan penduduk untuk tujuan studi energi secara unik. Data yang dikumpulkan tersedia bagi sejumlah perusahaan analisis data melalui perjanjian berbagi data yang secara eksplisit melarang organisasi di ekosistem berbagi data untuk menggunakan data tersebut untuk tujuan lain selain studi energi, dan menyatakan bahwa data yang dikirimkan akan dihapus setelah dianalisis. Agensi kota menetapkan proses manajemen data berdasarkan dokumen ini. Hal ini termasuk mekanisme pelaporan. Organisasi dalam ekosistem berbagi data melaporkan setiap tahunnya dengan menyediakan informasi seperti pembaruan laporan tahunan PIA, daftar pemrosesan yang dilakukan, dan tindakan pemindahan PII.

CONTOH 2 Agensi energi privat menerapkan layanan untuk optimalisasi manajemen energi di distrik ramah lingkungan yang terdiri dari beberapa bangunan cerdas. Persetujuan diberikan oleh penduduk untuk pengumpulan dan analisis data yang disediakan oleh berbagai meteran cerdas dan perangkat HVAC yang diinstal di gedung oleh pemasok berbeda. Agensi tersebut menetapkan proses manajemen data berdasarkan dokumen ini. Hal ini termasuk perjanjian kontrak yang menentukan tujuan pengumpulan dan pemrosesan data yang ditandatangani oleh pemangku kepentingan yang terotorisasi untuk mengakses data. Aktivitas manajemen data diterapkan sesuai dengan skema koordinasi ekosistem. Penyedia aplikasi baru ingin mengakses data untuk menyediakan layanan pemasaran. Karena aplikasi baru tidak mematuhi kebijakan kota cerdas, maka aplikasi tersebut tidak diperbolehkan untuk mengakses data yang dikumpulkan.

8.3.6 Produk kerja

Rencana privasi ekosistem kota cerdas mendeskripsikan proses manajemen data.

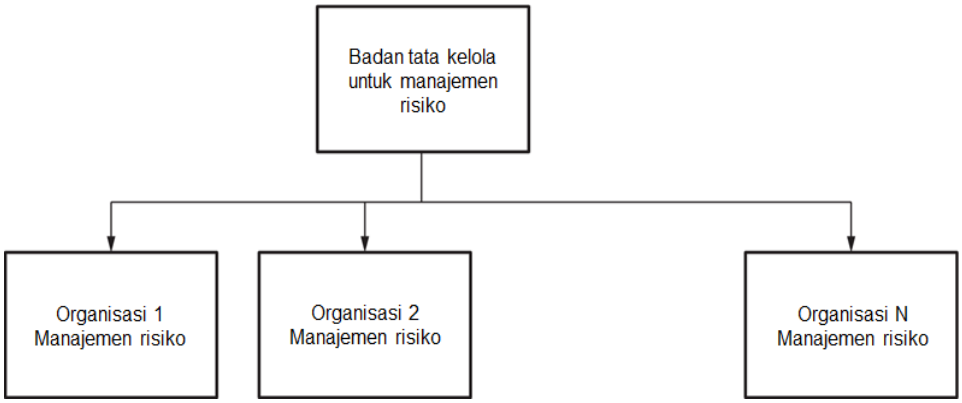
8.4 Proses manajemen risiko

8.4.1 Rekomendasi R8.4

Proses manajemen risiko sebaiknya ditetapkan oleh penanggung jawab tata kelola layanan kota cerdas untuk mengases dampak privasi.

8.4.2 Penjelasan

Proses manajemen risiko berkaitan dengan analisis dan perlakuan risiko terhadap privasi pada PII principal dalam layanan kota cerdas. Aktivitas tersebut dilakukan oleh penanggung jawab pengelola kota cerdas, serta oleh organisasi dalam ekosistem seperti yang ditunjukkan pada Gambar 17. Prasyarat untuk proses ini adalah sinkronisasi dengan proses tata kelola.



Gambar 17 — Pemangku kepentingan proses manajemen risiko privasi

8.4.3 Panduan tentang koordinasi ekosistem

Panduan berikut disediakan pada level ekosistem:

— memulai proses tata kelola privasi jika belum dilaksanakan;

— menetapkan dan mengimplementasikan skema koordinasi manajemen risiko yang spesifik di dalam ekosistem. Hal ini termasuk:

  — pemetaan sistem dari sistem-sistem ke organisasi pada ekosistem, dan spesifikasi perannya dalam proses manajemen risiko;

  — koordinasi aktivitas manajemen risiko termasuk analisis dan pemonitoran risiko, kepatuhan, asurans, dan audit praktis sistem dari sistem-sistem;

— menetapkan dan mengimplementasikan proses manajemen risiko layanan kota cerdas yang dipandang sebagai suatu sistem dari sistem-sistem. Hal ini termasuk:

  — identifikasi kerentanan dan ancaman pada privasi dalam sistem dari sistem-sistem;

  — identifikasi potensi risiko dan pelanggaran dalam sistem dari sistem-sistem;

  — evaluasi dampak potensial terhadap PII *principal*;

  — identifikasi kontrol untuk menangani risiko sistem dari sistem-sistem;

  — implementasi perlakuan risiko oleh organisasi ekosistem; dan

  — implementasi peningkatan berkelanjutan dan komunikasi yang terkait dengan peningkatan terhadap ekosistem.

CATATAN 1 Proses manajemen risiko sistem dari sistem-sistem dilakukan di bawah tanggung jawab pengontrol PII layanan kota cerdas yang dapat berbeda dari organisasi yang bertanggung jawab atas koordinasi ekosistem.

CATATAN 2 Asesmen risiko termasuk identifikasi peraturan perundang-undangan yang relevan dan kontrak yang berlaku.

8.4.4 Panduan untuk organisasi

Panduan berikut disediakan pada level organisasi:

— menetapkan dan mengimplementasikan proses analisis risiko pada sistem yang menjadi tanggung jawab organisasi. Proses tersebut termasuk:

  — identifikasi kerentanan dan ancaman sistem yang menjadi tanggung jawab organisasi;

  — identifikasi pemilik proses, pemilik risiko, dan individu yang terlibat dalam pemrosesan;

  — identifikasi risiko dan pelanggaran sistem;

  — evaluasi dampak potensial terhadap PII *principal*;

  — identifikasi kontrol yang diusulkan untuk menangani risiko sistem;

  — implementasi perlakuan risiko; dan

  — implementasi peningkatan yang berkelanjutan.

— menetapkan dan mengimplementasikan proses manajemen risiko sesuai dengan skema koordinasi ekosistem yang spesifik dan proses tata kelola yang dideskripsikan dalam 8.2 Proses tata kelola. Hal ini dapat mencakup implementasi metode asesmen dampak risiko keamanan informasi dan privasi.

CATATAN 1 Metode asesmen dampak risiko keamanan informasi dan privasi mencakup langkah-langkah berikut: penetapan konteks, asesmen risiko, perlakuan risiko, penerimaan risiko, komunikasi dan konsultasi risiko, pemonitoran dan reviu risiko.

CATATAN 2 Jika penerapan langkah asesmen risiko memberikan informasi yang memadai untuk secara efektif menentukan tindakan yang dipersyaratkan untuk memodifikasi risiko ke level yang dapat diterima, maka tugas tersebut selesai dan perlakuan risiko menyusul. Jika informasinya tidak memadai, dilakukan iterasi lain dari asesmen risiko dengan konteks yang telah direvisi (misalnya kriteria evaluasi risiko, kriteria penerimaan risiko, atau kriteria dampak), sesuai dengan siklus *plan-do-check-act* (PDCA).

8.4.5 Standar dan metode

Standar dan metode berikut sebaiknya digunakan:

— ISO/IEC 29134 untuk mendukung analisis risiko privasi;

— ISO/IEC 27701 digunakan untuk mendukung aktivitas identifikasi kontrol privasi untuk menangani risiko pada sistem.

Klasifikasi seperti STRIDE atau LINDDUN[27][28] dapat digunakan untuk mendukung aktivitas mengidentifikasi ancaman.

CONTOH Sebuah agensi transportasi kota cerdas menerapkan layanan peringatan tabrakan persimpangan. Layanan ini didasarkan pada kapabilitas kendaraan yang terhubung untuk menyiarkan pesan kesadaran kooperatif dengan frekuensi tinggi,[30] atau informasi tentang posisi, arah, atau kecepatannya. Pesan-pesan ini diterima oleh kendaraan lain serta unit pinggir jalan yang ditempatkan di persimpangan, dianalisis secara waktu riil untuk mendeteksi potensi tabrakan guna memicu tindakan penghindaran tabrakan. Ada selang waktu ketika pesan kooperatif berturut-turut dari kendaraan yang sama diterima. Kendaraan tidak dapat dilacak karena pesan dikirimkan dengan pseudonim. Untuk memastikan

autentikasi pesan, semua pseudonim tertanda dikirim dengan sertifikat kunci publik.[31] Ekosistem ini mencakup organisasi berikut: beberapa operator dengan kapabilitas kendaraan terhubung, beberapa operator unit pinggir jalan, beberapa penyedia sertifikat kunci publik, dan beberapa operator layanan.

8.4.6 Produk kerja

Rencana privasi ekosistem kota cerdas mendeskripsikan proses manajemen risiko.

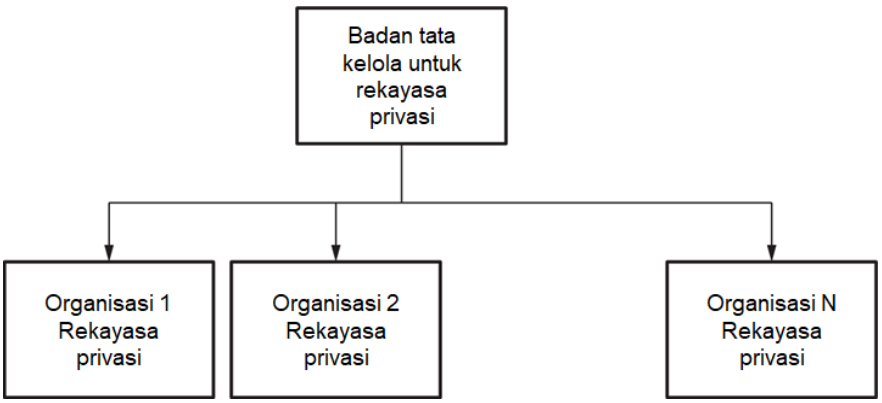
8.5 Proses rekayasa

8.5.1 Rekomendasi R8.5

Proses rekayasa sebaiknya ditetapkan oleh penanggung jawab tata kelola layanan kota cerdas untuk mempertimbangkan, kapanpun memungkinkan, pendekatan *privacy-by-design*.

8.5.2 Penjelasan

Proses rekayasa adalah serangkaian aktivitas yang berkaitan dengan siklus hidup layanan kota cerdas. Aktivitas ini dilakukan oleh penanggung jawab pengelola kota cerdas, serta oleh organisasi dalam ekosistem yang terkait dengan penyampaian, pemanfaatan ketersediaan layanan kota cerdas, seperti ditunjukkan Gambar 18. Prasyarat untuk proses ini adalah sinkronisasi dengan proses tata kelola dan manajemen risiko.



Gambar 18 — Pemangku kepentingan proses rekayasa privasi

8.5.3 Panduan tentang koordinasi ekosistem

Panduan berikut disediakan pada level ekosistem:

— memulai proses tata kelola privasi jika belum dilaksanakan;

— memulai proses manajemen risiko privasi jika belum dilaksanakan;

— menetapkan dan mengimplementasikan skema koordinasi rekayasa privasi yang spesifik dalam ekosistem. Hal ini termasuk:

  — pemetaan sistem dari sistem-sistem ke organisasi ekosistem, dan spesifikasi perannya dalam proses rekayasa privasi;

  — koordinasi aktivitas siklus hidup rekayasa privasi yang akan mengarah pada desain kontrol privasi sistem dari sistem-sistem yang sesuai; dan

— koordinasi aktivitas siklus hidup rekayasa privasi yang berkaitan dengan asurans, pendekatan kepatuhan, atau audit;

— menetapkan dan mengimplementasikan proses rekayasa privasi agar layanan kota cerdas dipandang sebagai sistem dari sistem-sistem. Hal ini termasuk:

  — spesifikasi model data sistem dari sistem-sistem, berfokus pada aset data, aliran data, dan pemrosesan PII;

  — proses manajemen risiko sistem dari sistem-sistem sebagaimana dideskripsikan dalam 8.4 Proses manajemen risiko;

  — aktivitas dalam siklus hidup sistem dari sistem-sistem rekayasa privasi yang akan mengarah pada spesifikasi kebijakan privasi, kriteria kesesuaian, persyaratan teknis privasi, kontrol privasi dan layanan privasi serta fungsi sistem dari sistem-sistem dan pemetaannya ke organisasi ekosistem;

  — aktivitas untuk peningkatan berkelanjutan yang melibatkan reviu berkala terhadap persyaratan dan tindakan serta pemetaannya ke organisasi ekosistem.

CATATAN 1 Aktivitas dalam proses rekayasa privasi dapat mencakup resolusi skenario konflik dan identifikasi kebijakan privasi yang dihasilkan. Tujuan dalam rekayasa produk atau layanan kota cerdas adalah untuk menemukan keseimbangan antara batasan dan kebutuhan semua organisasi dan pemangku kepentingan, serta hak privasi individu dalam fase desain, fase operasional, fase pemeliharaan, fase registrasi individu (jika ada) dan fase deregistrasi individu (jika ada).

CATATAN 2 Pemrosesan PII yang berkaitan dengan aset data dan aliran data dapat mencakup pengumpulan, retensi/pencatatan, pembangkitan/transformasi, pengungkapan/transfer, dan/atau pemusnahan. Istilah lain yang digunakan adalah data yang diam (*data at rest*), data yang bergerak (*data in motion*).

8.5.4 Panduan untuk organisasi

Panduan berikut disediakan pada level organisasi:

— menetapkan dan mengimplementasikan proses rekayasa privasi sistem yang menjadi tanggung jawab organisasi, termasuk:

  — spesifikasi model data;

  — analisis risiko;

  — aktivitas siklus hidup sistem;

  — dan definisi peningkatan berkelanjutan;

— menetapkan dan mengimplementasikan proses rekayasa privasi sesuai dengan skema koordinasi ekosistem yang spesifik yang dideskripsikan dalam 8.2 Proses tata kelola, termasuk fase desain, fase penggunaan, dan fase manajemen hubungan pelanggan.

CATATAN 1 Aktivitas yang berkaitan dengan manajemen hubungan pelanggan (*customer relationship management*/CRM) dapat mencakup akuisisi suatu produk dan/atau langganan suatu layanan, pengiriman suatu produk atau layanan, dukungan, layanan, pemeliharaan dan bantuan untuk suatu produk atau layanan, pemasaran evolusi produk atau layanan atau berita yang terkait dengan produk atau layanan, dan daur ulang atau pemusnahan suatu produk atau deregistrasi suatu layanan.

CATATAN 2 Layanan kota cerdas sering kali ditambahkan di atas layanan lain yang sudah ada. Dalam kasus seperti ini, *privacy-by-design* mempertimbangkan infrastruktur yang sudah ada.

8.5.5 Standar dan metode

ISO/IEC 29100 sebaiknya digunakan.

Hal ini memberikan prinsip untuk memberlakukan: persetujuan dan pilihan; legitimasi dan spesifikasi tujuan; limitasi pengumpulan; minimalisasi data; limitasi penggunaan, retensi, dan pengungkapan; akurasi dan kualitas; keterbukaan, transparansi dan akses; akuntabilitas; keamanan informasi; dan kepatuhan privasi.

Standar dan metode berikut dapat digunakan:

— model dan metodologi yang disediakan oleh OASIS PMRM[32] digunakan untuk mendukung proses rekayasa privasi sistem dari sistem-sistem. Ini digunakan untuk mendeskripsikan aset data dan aliran data serta memberikan gambaran semua domain, sistem, dan proses di mana PII digunakan; untuk menentukan kebijakan privasi dan kriteria kesesuaian; untuk melakukan analisis privasi yang mengarah pada identifikasi persyaratan; untuk menentukan kontrol privasi yang terkait dengan PII, termasuk kontrol privasi internal yang dibuat dalam domain/subdomain, namun juga kontrol privasi yang diwarisi dan diekspor ke/dari domain/subdomain lain; dan yang terakhir untuk menentukan layanan dan fungsi privasi yang akan diimplementasikan dalam mekanisme privasi teknis untuk rantai data dalam suatu ekosistem;

— ISO/IEC TR 27550 digunakan untuk mendukung proses rekayasa privasi sistem dari sistem-sistem. Standar ini mengidentifikasi properti keamanan dan privasi yang digunakan dalam proses seperti konfidensialitas, integritas, availabilitas, *unlinkability*, transparansi, atau intervenabilitas. Ini mengidentifikasi karakteristik desain rekayasa privasi yang digunakan dalam proses: strategi berorientasi data (meminimalkan, memisahkan, mengabstrakkan, menyembunyikan) dan strategi berorientasi proses (menginformasikan, mengontrol, menegakkan, menunjukkan);

— ISO/IEC 27701 digunakan untuk mendukung aktivitas identifikasi kontrol privasi untuk menangani risiko sistem;

— ISO/IEC 20889 digunakan untuk menentukan terminologi, klasifikasi teknik de-identifikasi sesuai dengan karakteristiknya dan penerapannya untuk mengurangi risiko identifikasi ulang.

CONTOH Kota cerdas menerapkan layanan kota cerdas untuk mengumpulkan berbagai data lingkungan seperti kondisi cuaca atau status pemeliharaan jalan. Hal ini memanfaatkan keberadaan ekosistem terbuka untuk penyediaan data kendaraan di mana warga kota menginstal kapabilitas pengumpulan data pada kendaraan mereka dan memperdagangkan data yang dikumpulkan melalui brankas data pribadi: data diagnosis diberikan kepada pemanufaktur mobil, data meteorologi diberikan kepada organisasi prakiraan cuaca lokal, dan kondisi jalan diberikan kepada organisasi pemeliharaan jalan.[33] Ekosistem mencakup organisasi berikut: beberapa penyedia layanan brankas data pribadi, operator pasar, penyedia layanan global dan lokal. Kota tersebut menetapkan skema koordinasi secara keseluruhan yang mencakup tata kelola, manajemen risiko, berbagi data, rekayasa privasi, dan keterlibatan warga kota sesuai dengan dokumen ini. Proses rekayasa privasi ekosistem termasuk asesmen berkala terhadap prinsip privasi untuk meminimalkan transfer data dari brankas data pribadi ke penyedia layanan. Koordinasi rekayasa privasi melibatkan penyedia layanan brankas data pribadi, operator pasar, dan penyedia layanan, yang mengidentifikasi kesesuaian untuk beralih ke teknik de-identifikasi baru, yang menyinkronkan dengan aktivitas

rekayasa privasi setiap organisasi.

8.5.6 Produk kerja

Rencana privasi ekosistem kota cerdas mendeskripsikan proses rekayasa.

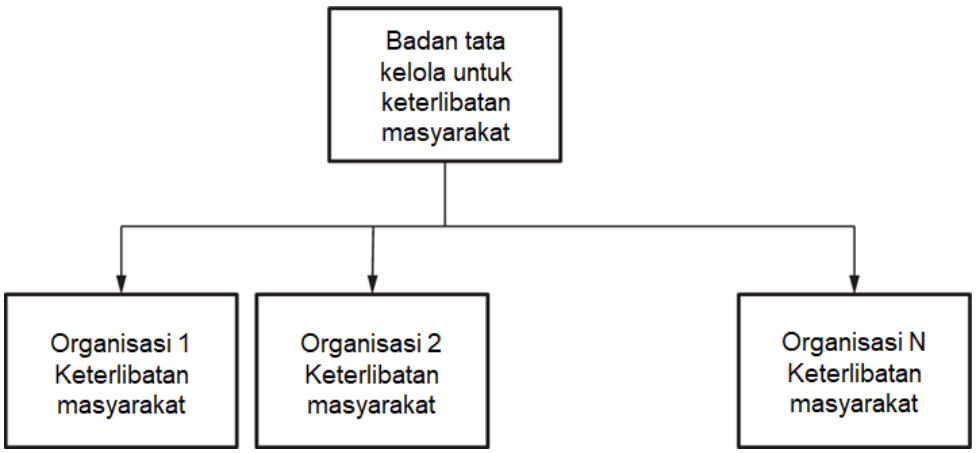
8.6 Proses keterlibatan warga kota

8.6.1 Rekomendasi R8.6

Proses keterlibatan warga kota yang mengintegrasikan privasi sebaiknya ditetapkan oleh penanggung jawab tata kelola layanan kota cerdas.

8.6.2 Penjelasan

Proses keterlibatan warga kota berfokus pada konsultasi dengan warga kota kota cerdas mengenai aturan dan kebijakan pada level tata kelola, dan pada dukungan terhadap penegakan aturan dan kebijakan terkait privasi layanan kota cerdas. Aktivitas ini dilakukan oleh penanggung jawab pengelola kota cerdas serta organisasi dalam ekosistem seperti yang ditunjukkan pada Gambar 19.



Gambar 19 — Pemangku kepentingan proses keterlibatan warga kota privasi

8.6.3 Panduan tentang koordinasi ekosistem

Panduan berikut disediakan pada level ekosistem:

— membangun dialog warga kota dan proses pengambilan keputusan bersama untuk penetapan peraturan dan kebijakan kota cerdas untuk privasi, sesuai dengan proses tata kelola yang dideskripsikan dalam 8.2 Proses tata kelola. Contoh topiknya adalah kebijakan kota cerdas untuk pemberitahuan persetujuan atau transparansi informasi tentang pemrosesan PII layanan kota cerdas;

— membangun aktivitas interaksi warga kota, termasuk misalnya acara informasi, pertanyaan dan komplain;

— untuk setiap layanan yang akan diterapkan, menentukan apakah diperlukan konsultasi warga kota yang akan mereviu tujuan layanan, etika, dan privasi;

— untuk setiap layanan yang akan diterapkan, mendorong terciptanya faktor pendukung untuk memfasilitasi keterlibatan warga kota (misalnya aplikasi privasi);

— melakukan reviu warga kota secara berkala terhadap layanan dan memberikan rekomendasi untuk amendemen jika diperlukan;

— melakukan reviu warga kota secara berkala terhadap aturan dan kebijakan kota cerdas;

— menetapkan persyaratan dialog warga kota dan pengambilan keputusan bersama yang sebaiknya dipenuhi oleh organisasi ekosistem; dan

— menetapkan skema koordinasi dalam ekosistem untuk organisasi yang memiliki persyaratan konsertasi warga kota.

CATATAN Aktivitas dalam proses keterlibatan warga kota dapat termasuk resolusi skenario konflik yang dibahas ketika mendefinisikan kebijakan privasi.

8.6.4 Panduan untuk organisasi

Panduan berikut disediakan pada level organisasi:

— mengidentifikasi apakah persyaratan dialog warga kota dan pengambilan keputusan bersama sebaiknya dipenuhi oleh organisasi;

— jika diperlukan, mengimplementasikan persyaratan dialog warga kota dan pengambilan keputusan bersama;

— jika diperlukan, berpartisipasi dalam reviu warga kota berkala terhadap layanan; dan

— mengimplementasikan amendemen.

CONTOH 1 Kota cerdas mengembangkan layanan kota cerdas yang bertujuan untuk merekomendasikan warga kota dan pengunjung kapan dan ke mana akan pergi, berdasarkan berbagai sumber data termasuk cuaca, lalu lintas, dan juga profil pribadi (misalnya data demografi, pola konsumsi, riwayat lokasi). Karena memproses PII akan membuat rekomendasi menjadi lebih baik, dan untuk menghindari publisitas yang buruk, mereka memutuskan untuk melibatkan warga kota agar memahami konsern privasi mereka dan menetapkan kebijakan privasi yang sesuai dalam proses keterlibatan warga, yang dimulai sejak awal proses pengembangan. Hal ini memungkinkan kota dan warga kotanya untuk memahami dan mengintegrasikan konsern privasi dan kebutuhan layanan, serta menilai apa yang ingin mereka bagikan untuk mendapatkan imbalannya. Bagian esensial dari proses dialog adalah laporan yang sering dibuat dalam skema koordinasi, yang mendorong transparansi, menjaga warga kota tetap mendapatkan informasi terkini, mengelola ekspektasi dan menciptakan kepercayaan.

Perhatian terhadap proyek ini juga mengarah pada reviu kebijakan untuk persetujuan, dan pendekatan untuk minimalisasi data. Manfaat dari reviu kebijakan persetujuan ada dua. Pertama, keputusan untuk memberikan skor yang lebih tinggi pada layanan di mana pengontrol PII menjadi bagian dari skema koordinasi ekosistem. Kedua, rekomendasi bahwa persetujuan di ruang publik di perkotaan, dalam banyak kasus, bukanlah dasar hukum yang tepat untuk diproses. Mengenai pendekatan minimalisasi data, manfaat yang paling penting adalah bahwa setiap pengumpulan data harus dikaitkan erat dengan tujuan yang jelas dan spesifik yang telah ditetapkan secara apriori.

CONTOH 2 Kota cerdas menginstal kamera video dengan tujuan mengidentifikasi pelat nomor kendaraan untuk memungkinkan pengumpulan alat otomatis. Persetujuan tidak diberikan oleh individu namun oleh tata kelola kota. Proses keterlibatan warga kota diterapkan untuk menyepakati prosedur pemberian informasi kepada individu mengenai perlakuan yang dilakukan, dan modalitas audit berkala terhadap pengoperasian sistem kamera video. Lampiran B memberikan pertimbangan lebih lanjut mengenai penggunaan kamera video di kota cerdas

8.6.5 Produk kerja

Rencana privasi ekosistem kota cerdas mendeskripsikan proses keterlibatan warga kota.

Lampiran A
(informatif)
Contoh struktur rencana privasi ekosistem

Tabel A.1 menyediakan contoh sebuah struktur rencana privasi ekosistem

Tabel A. 1 — Contoh struktur rencana privasi ekosistem

Bagian	Subbagian	Deskripsi atau konten
Identifikasi	Nama kota cerdas	Nama unik ekosistem kota cerdas
	Tanggung jawab	Nama dan tanda tangan person yang bertanggung jawab atas rencana privasi ekosistem
	Riwayat	Mencantumkan reviu dan evolusi rencana privasi. Juga termasuk kalender untuk rencana pembaruan.
	Konfidensialitas	Menyatakan konfidensialitas rencana, atau beberapa bagiannya. Rencana disusun sedemikian rupa sehingga ada bagian yang bersifat publik, dan bagian lainnya bersifat konfidensial namun dapat diakses untuk pengontrolan oleh pemangku kepentingan yang teridentifikasi.
	Repositori informasi	URL ke repositori informasi pada ekosistem kota cerdas. Dapat mencakup bagian publik, serta bagian privat.
Deskripsi layanan kota cerdas	Deskripsi layanan umum	Deskripsi layanan Deskripsi lingkungan operasional layanan (pemangku kepentingan, sistem) Deskripsi peraturan perundang-undangan yang berlaku, deskripsi standar penerapan
	Deskripsi ekosistem umum	Deskripsi rantai bisnis (tata kelola, rantai pasokan, manajemen data)
	Pemangku kepentingan	Daftar organisasi dalam ekosistem dan perannya
Deskripsi ekosistem kota cerdas	Penanggung jawab tata kelola	Deskripsi skema dan sasaran tata kelola, deskripsi penanggung jawab tata kelola Deskripsi aturan dan prosedur: nominasi anggota penanggung jawab tata kelola, pengoperasian Anggota penanggung jawab tata kelola
	Manajemen rantai pasokan	Deskripsi rantai pasokan Deskripsi sasaran manajemen Deskripsi prosedur koordinasi, pertukaran informasi, hak akses, dan pendekatan pemonitoran Identifikasi pemangku kepentingan dalam rantai pasokan yang memiliki pengaruh terhadap privasi (misalnya pengontrol dan prosesor PII, pemasok kontrol privasi)
	Manajemen data	Deskripsi aliran data dalam ekosistem Deskripsi tujuan manajemen Deskripsi prosedur koordinasi, informasi yang dipertukarkan, dan pendekatan pemonitoran Identifikasi pemangku kepentingan dalam ekosistem berbagi data yang memiliki pengaruh terhadap privasi (misalnya pengontrol dan prosesor

Bagian	Subbagian	Deskripsi atau konten
		PII)
Rencana manajemen privasi	Proses tata kelola	Deskripsi tentang bagaimana proses tata kelola (8.2) diterapkan dan dinilai kembali untuk peningkatan berkelanjutan Aturan dan kebijakan untuk tata kelola privasi Persyaratan dan aktivitas pengawasan Program kompetensi Aktivitas komunikasi dan pengawasan, persyaratan dasbor Prosedur proteksi hak warga kota Aktivitas interaksi dengan otoritas proteksi data
	Proses manajemen data	Deskripsi tentang bagaimana proses manajemen data (8.3) diterapkan dan dinilai kembali untuk peningkatan berkelanjutan Templat asesmen dampak privasi, templat perjanjian berbagi, standar yang akan digunakan Koordinasi manajemen data dalam pengoperasian ekosistem dan dasbor Langkah-langkah untuk asurans kepatuhan dan audit praktik
	Proses manajemen risiko	Deskripsi tentang bagaimana proses manajemen risiko (8.4) diterapkan dan dinilai kembali untuk peningkatan berkelanjutan Praktik yang akan diterapkan, standar yang akan digunakan Koordinasi manajemen risiko dalam pengoperasian ekosistem dan dasbor Langkah-langkah untuk asurans kepatuhan dan audit praktik
	Proses rekayasa	Deskripsi tentang bagaimana proses rekayasa (8.5) diterapkan dan dinilai kembali untuk peningkatan berkelanjutan Praktik yang akan diterapkan, standar yang akan digunakan Koordinasi aktivitas siklus hidup rekayasa privasi dalam pengoperasian ekosistem dan dasbor Langkah-langkah untuk asurans kepatuhan dan audit praktik
	Proses keterlibatan warga kota	Deskripsi tentang bagaimana proses keterlibatan warga kota (8.6) diterapkan dan dinilai kembali untuk peningkatan berkelanjutan Praktik yang akan diterapkan, standar yang akan digunakan Koordinasi aktivitas keterlibatan warga kota dalam pengoperasian ekosistem dan dasbor (misalnya pengambilan keputusan bersama) Langkah-langkah untuk asurans kepatuhan dan audit praktik

Lampiran B
(informatif)
Menggunakan kamera video di kota cerdas

B.1 Perlakuan aliran data kamera video

Kamera video adalah sensor yang mentransmisikan data video dan secara opsional data suara. Data video dapat ditransmisikan dalam spektrum tampak dan/atau dalam spektrum inframerah. Data tersebut kemudian dapat dianalisis, agregat dengan data lain, dan digunakan untuk mengekstrapolasi informasi.

Kota atau pemangku kepentingannya mungkin tertarik untuk menggunakan informasi ini untuk berbagai tujuan seperti manajemen lalu lintas, pengurangan energi, atau deteksi kejahatan. Misalnya, informasi tentang kecelakaan dan kemacetan lalu lintas dapat digunakan untuk memperingatkan polisi atau mengubah rute lalu lintas.

Tantangannya adalah kamera menghasilkan, segera setelah mengamati aktivitas manusia, informasi sensitif privasi, yang manajemennya sering kali diatur oleh peraturan nasional atau regional yang ketat.

Biasanya, instalasi dan pengoperasian kamera di area terbuka untuk umum tunduk pada otorisasi untuk tujuan yang ditentukan dan pemilik kamera juga merupakan pemilik data yang dihasilkan dan dengan demikian bertanggung jawab atas penggunaannya.

Ketentuan di bawah ini sebaiknya dianggap sebagai generik. Pelaksana kamera kota cerdas sebaiknya mengidentifikasi regulasi yang berlaku, yang dalam beberapa kasus, dapat melarang berbagi kamera antaraplikasi.

B.2 Konsern privasi

Konsern privasi muncul ketika data yang dikumpulkan, yang kemungkinan agregat dari berbagai sumber informasi, dapat digunakan untuk mengidentifikasi individu atau secara tidak langsung mengidentifikasi individu, misalnya dengan mengumpulkan nomor pelat kendaraan. Perlakuan yang dilakukan terhadap video mentah dapat memungkinkan pengenalan individu atau/dan pelat nomor kendaraan. Selanjutnya, gambar yang ditangkap dapat disimpan untuk durasi yang tidak diketahui.

B.3 Tujuan yang diintensikan

Tujuan pengumpulan data dan agregasi data sebaiknya selalu diidentifikasi dengan jelas. Keseimbangan antara keuntungan bagi kota atau pemangku kepentingannya dan kerugian bagi warga kota, jika ada, sebaiknya ditetapkan. Setelah keseimbangan yang tepat telah disepakati, tujuan yang dimaksudkan sebaiknya diiklankan. Aktivitas ini dapat didukung oleh proses tata kelola (8.2 Proses tata kelola), proses manajemen risiko (8.4 Proses manajemen risiko), dan proses keterlibatan warga kota (8.6 Proses keterlibatan warga kota) yang dideskripsikan dalam dokumen ini.

Selanjutnya, tujuan pengumpulan data dan agregasi data sebaiknya ditetapkan sebelum sistem didesain. Sebagai tambahan, langkah-langkah akuntabilitas sebaiknya ditentukan pada fase desain untuk meningkatkan keyakinan bahwa hanya tujuan yang dimaksudkan saja yang dapat dicapai. Aktivitas ini dapat didukung oleh proses manajemen data (8.3 Proses

manajemen data) dan proses rekayasa (8.5 Proses rekayasa) yang dideskripsikan dalam dokumen ini.

B.4 Tujuan yang tidak diintensikan

Data mentah dari kamera video sering ditransmisikan ke pusat data untuk dilakukan perlakuan sesuai dengan tujuan yang dimaksudkan. Namun pusat data juga dapat melakukan perlakuan yang tidak dimaksudkan. Perlakuan tambahan seperti itu sebaiknya dicermati. Keseimbangan antara keuntungan bagi kota atau pemangku kepentingannya dan kerugian bagi warga kota, jika ada, sebaiknya ditetapkan dan keseimbangan yang tepat sebaiknya disepakati mengenai:

— manusia (kamera dapat secara sederhana digunakan untuk menghitung jumlah orang atau mengidentifikasi wajah warga kota);

— kendaraan (kamera dapat secara sederhana menghitung jumlah kendaraan atau melacak pemiliknya dan menghitung jumlah orang yang duduk di kursi depan); atau

— area (kamera dapat secara sederhana digunakan untuk memonitor polusi udara atau merekam pergerakan kendaraan dan orang jika terjadi insiden di suatu area);

Satu masalah adalah untuk mendapatkan keyakinan bahwa tujuan spesifik penginstalan kamera pada awalnya tidak dialihkan nantinya ke tujuan lain yang belum diungkapkan (dan disetujui).

B.5 Berbagi data dengan pihak ketiga secara tidak sah

Perlakuan yang dapat dilakukan melalui pengambilan video biasanya berada di bawah tanggung jawab kota atau polisi kota. Ketika teknologi kota cerdas dialihdayakan ke korporasi privat, terdapat risiko bahwa PII dapat dibagikan secara tidak sah kepada pihak ketiga. Beberapa peralatan yang disediakan untuk mencapai tujuan yang dimaksudkan dapat berisi pintu belakang yang dapat diaktifkan selama pembaruan perangkat lunak. Jika aliran data yang digunakan sesuai dengan aliran data yang dipublikasikan, maka aliran data tersebut dapat dianalisis dan bahkan disaring untuk memastikan bahwa aliran data hanya mengirimkan data yang dimaksudkan. Jika tidak, kepercayaan penuh perlu diberikan pada pemanufaktur peralatan.

B.6 Persetujuan pengguna

Persetujuan pengguna adalah salah satu prinsip privasi utama. Namun, dalam kasus kamera video, persetujuan pengguna individu tidak dimungkinkan. Persetujuan tidak diberikan secara langsung oleh individu tetapi oleh pengelola kota atau pemerintah di negara tempat kamera tersebut diinstal. Secara umum disarankan agar individu yang merasa gambarnya telah direkam diberi akses dan kemungkinan untuk menyembunyikan atau menghapus data terkait. Beberapa kelompok konsumen dapat diundang melalui proses keterlibatan warga kota (8.6 Proses keterlibatan warga kota) untuk mengapresiasi keseimbangan antara manfaat bagi kota atau pemangku kepentingannya dan kerugian bagi individu. Langkah-langkah untuk memberi informasi kepada individu mengenai perlakuan yang dilakukan oleh kamera ini sebaiknya diimplementasikan.

Bibliografi

[1] ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

[2] ISO/IEC 17789:2014, *Information technology — Cloud computing — Reference architecture*

[3] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*

[4] ISO/IEC 20547-3, *Information technology — Big data reference architecture — Part 3: Reference architecture*

[5] ISO/IEC 20547-4, *Information technology — Big data reference architecture — Part 4: Security and privacy*

[6] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[7] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[9] ISO/IEC 27018:2019, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[10] ISO/IEC TR 27550:2019, *Information technology — Security techniques — Privacy engineering for system life cycle processes*

[11] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[12] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[13] ISO/IEC 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[14] ISO/IEC 29151:2017, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[15] ISO/IEC 29184:2020, *Information technology — Online privacy notices and consent*

[16] ISO/IEC 29190:2015, *Information technology — Security techniques — Privacy capability assessment model*

[17] ISO/IEC 30141:2018, *Internet of Things (loT) — Reference Architecture*

[18] ISO/IEC 30145 (all parts), *Information technology — Smart City ICT reference*

framework

[19] ISO/IEC 30182:2017, *Smart city concept model — Guidance for establishing a model for data interoperability*

[20] ISO 37156, *Smart community infrastructures — Guidelines on data exchange and sharing for smart community infrastructures*

[21] ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

[22] ISO/IEC TS 38501:2015, *Information technology — Governance of IT — Implementation guide*

[23] ISO/IEC TR 38502:2017, *Information technology — Governance of IT — Framework and model*

[24] ISO/IEC 38505 (all parts), *Information technology — Governance of IT — Governance of data*

[25] BSI PAS 183:2017, *Smart cities — Guide to establishing a decision-making framework for sharing data and information services*

[26] ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

[27] The STRIDE threat model[2], https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[28] LINDDUN privacy threat analysis methodology, https://www.linddun.org/

[29] ZANELLA A., BUI N., CASTELLANI A., VANGELISTA L., ZORZI M. IEEE Internet of Things for Smart Cities. IEEE Internet of things journal. Vol.1, N°1, February 2014. https://ieeexplore.ieee.org/document/6740844/

[30] SYSTEMS I.T. (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. ETSI TS 102 637-2 V1.2.1 (2011-03), https://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf

[31] SYSTEMS I.T. (ITS); Security; Pre-standardization study on pseudonym change management ETSI TR 103 415 V1.1.1 (2018-04), https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf

[32] ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS (OASIS). *Privacy Management Reference Model and Methodology (PMRM),* Version 1.0. July 2013, updated May 2016. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

[2] Halaman tersebut menyatakan sebagai berikut: “Dokumentasi ini diarsipkan dan tidak dipelihara”.

[33] Full prototype of cross-sectorial vehicle data services. AutoMat H2020 projects deliverable D5.3. January 2018. https://www.automat-project.eu/sites/default/files/automat/public/content-files/articles/AutoMat%20D5%203_Full%20Prototype%20of%20Cross-Sectorial%20Vehicle%20Data%20Services_final.pdf

Introduction

The growing integration of ICT technologies (e.g. cloud computing, IoT, big data, mobile networks, artificial intelligence and machine learning) in smart cities will allow for improved data sharing capabilities to achieve better services. But the growing complexity of the ICT infrastructure will also create vulnerabilities at security and privacy level. Security incidents can lead to essential services not operating properly, for instance a massive electricity supply shortage. Likewise, unauthorized access to personal data can lead to major privacy breaches, for instance access to personal health data records.

Ensuring that privacy is properly dealt within smart cities is a challenge. First, a wide variety of public and private stakeholders can be involved such as:

— agencies in charge of managing essential city services for instance administration services;

— business organizations in charge of operating services for instance electricity distribution:

— organizations in supply chains associated with the deployment of related infrastructure for instance transport systems; and

— associations representing the viewpoints of citizens.

Secondly, a wide variety of standards can be used such as:

— privacy standards;

— smart city standards;

— cloud computing standards;

— IoT standards;

— big data standards; and

— IT governance standards.

Figure1 shows examples of such standards. This document thus focuses on providing guidance on the use of standards, while taking into account the variety of stakeholders in a smart city ecosystem.

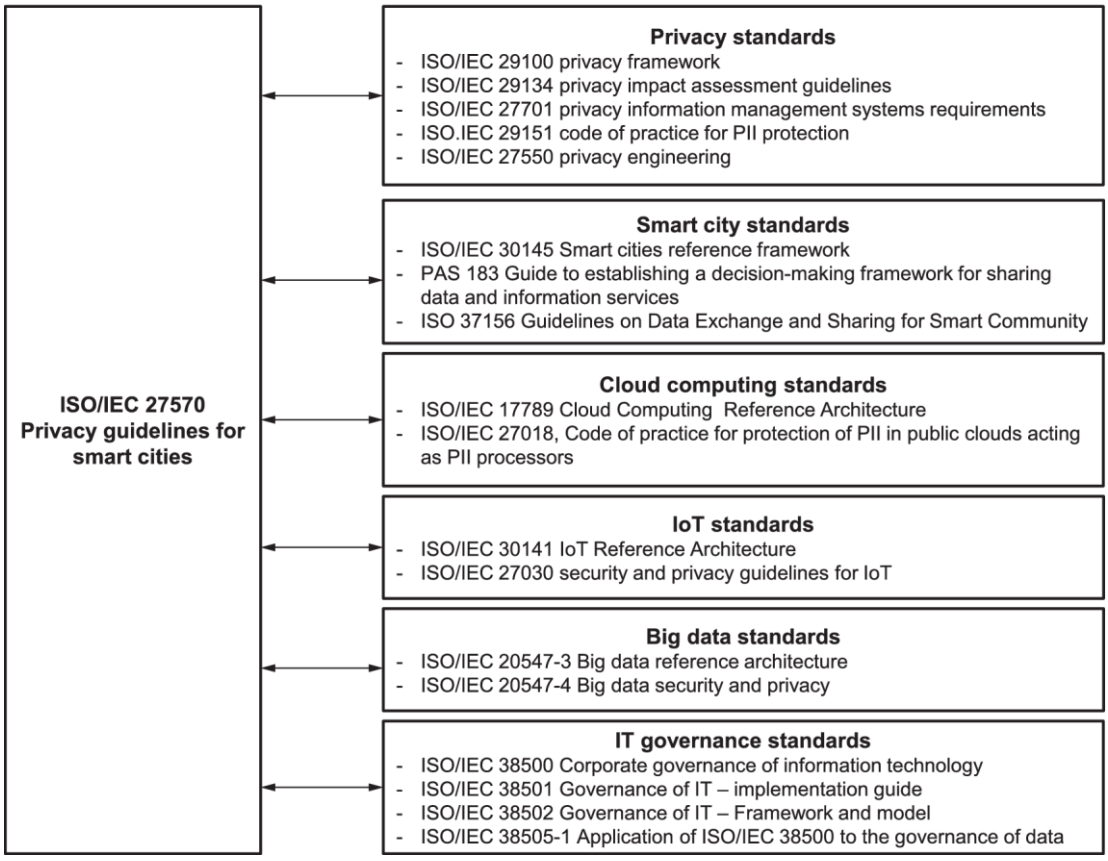


Figure 1 — Examples of standards to reference

Figure 2 summarizes privacy recommendations to smart cities ecosystems in this document, further numbered R6.1, R6.2, R6.3, and R6.4.

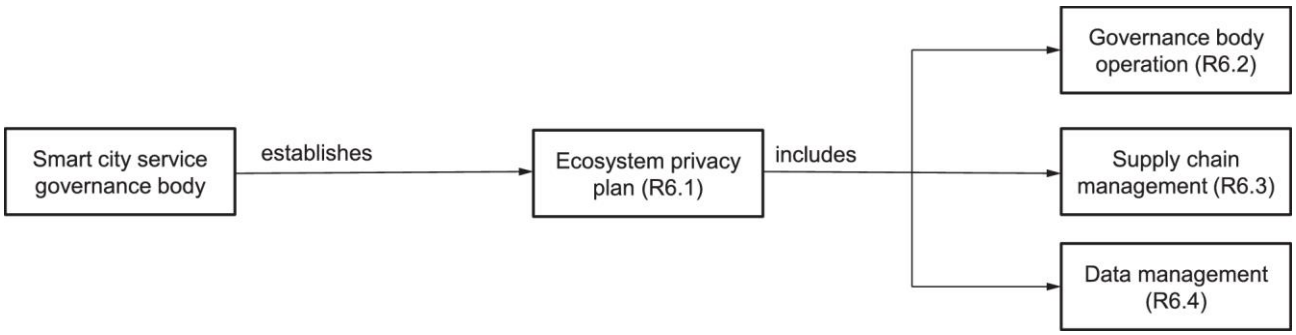


Figure 2 — Ecosystem guidance for privacy

Figure 3 summarizes privacy recommendations to smart cities processes in this document, further numbered R8.2, R8.3, R8.3, R8.4, and R8.5.

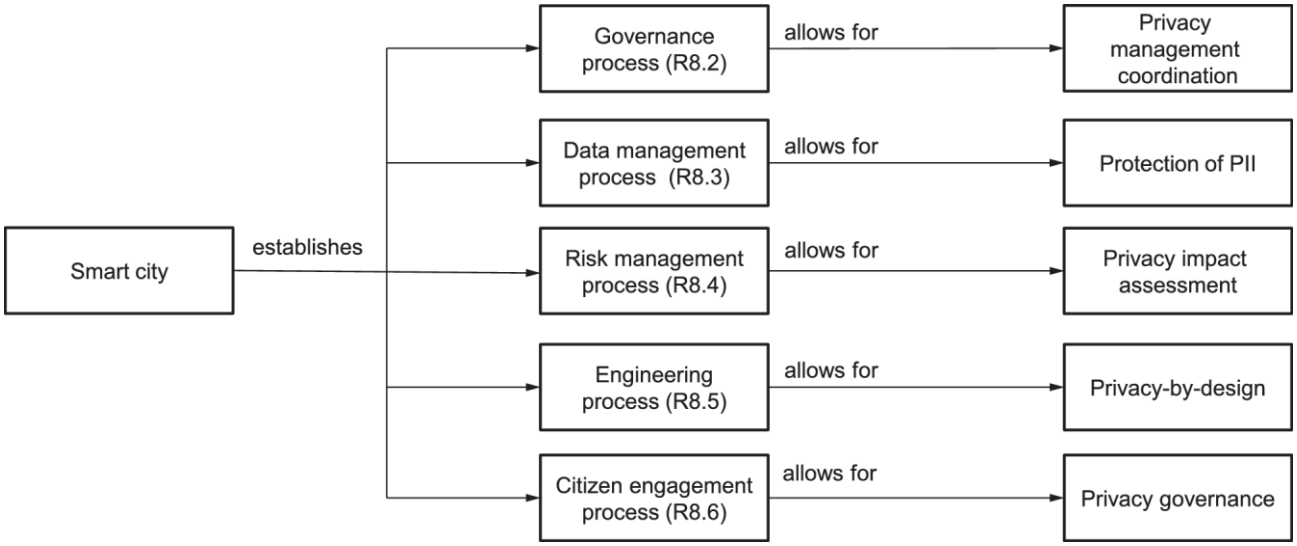


Figure 3 — Process guidance for privacy

It is foreseen that this document will pave the way to future privacy standards for smart cities. Table 1 provides a list of possible future standards.

Table 1 — Examples of possible future standards

Category	Standards
Privacy management to keep track and monitor PII assets that are exploited in smart cities.	Framework for privacy management in smart cities Guidelines for communication between organizations Guidelines for privacy management plans in smart cities Guidelines for privacy policy making in smart cities including data retention Guidelines for privacy impact assessment reports in smart cities Guidelines for consent management in smart cities Guidelines for privacy accountability and transparency management in smart cities Guidelines for privacy breach management in smart cities Guidelines for privacy-by-design of smart city services Guidelines for the integration of privacy concerns in data exchange agreements Smart city services security and privacy assurance
Privacy engineering in smart city ecosystems	Guidelines for privacy engineering[a] in smart cities
Collaboration in smart city ecosystems	Guidelines for citizen engagement Guidelines for communication between organizations (for each type of organization, e.g. administration)
Interoperability to avoid vendor lock-in	Common privacy management information model in smart cities Common privacy impact assessment information in smart cities Common description of privacy capabilities in smart cities Common description of privacy incidents in smart cities

[a] Privacy engineering focuses on the integration of privacy concerns in the engineering of a system.

Privacy protection — Privacy guidelines for smart cities

1 Scope

The document takes a multiple agency as well as a citizen-centric viewpoint.

It provides guidance on:

— smart city ecosystem privacy protection;

— how standards can be used at a global level and at an organizational level for the benefit of citizens; and

— processes for smart city ecosystem privacy protection

This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
activity
set of cohesive tasks (3.32) of a process (3.25)

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.3]

3.2
agency
organization (3.13) providing a specific service for a city

3.3
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.4
citizen
inhabitant of a city

3.5
citizen engagement
involvement of *citizens* (3.4) in the decision-making of public policies

3.6
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes (3.25)

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.7
data protection officer
person appointed by the *PII* controller (3.15) to ensure, in an independent manner, compliance with the privacy law/regulation requirements

3.8
ecosystem
infrastructure and services based on a network of organizations (3.13) and stakeholders

Note 1 to entry: Organizations can include public bodies.

3.9
ecosystem privacy plan
planned arrangements for ensuring that privacy is adequately managed in an ecosystem (3.8)

3.10
governance
system of directing and controlling

[SOURCE: ISO/IEC 38500:2015, 2.8]

3.11
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.12
intervenability
property that ensures that *PII principals* (3.16), *PII controllers* (3.15), *PII processors* (3.17) and supervisory authorities can intervene in all privacy-relevant data processing

Note 1 to entry: The extent to which any of these stakeholders can intervene in data processing can be limited by relevant legislation or regulation.

[SOURCE: ISO/IEC TR 27550:2019, 3.6]

3.13
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives
Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity of institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 37100:2016, 3.2.3, modified — Note 2 to entry has been omitted.]

3.14
personally identifiable information
PII
any information that a) can be used to identify the *PII principal* (3.16) to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9]

3.15
personally identifiable information controller
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (3.14) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.17)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.16
personally identifiable information principal
PII principal
natural person to whom the *personally identifiable information* (3.14) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.17
personally identifiable information processor
PII processor
privacy stakeholder that processes *personally identifiable information* (3.14) on behalf of and in accordance with the instructions of a *PII controller* (3.15)

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.18
policy
intentions and direction of an *organization* (3.13) as formally expressed by its top management

[SOURCE: ISO/IEC 20547-3:2020, 3.11]

3.19
privacy breach
situation where *personally identifiable information* (3.14) is processed in violation of one or more relevant privacy safeguarding requirements

[SOURCE: ISO/IEC 29100:2011, 2.13]

3.21
privacy-by-design
approach in which privacy is considered at the initial design stage and throughout the complete lifecycle of products, processes or services that involve processing *personally identifiable information* (3.14)

3.22
privacy data sharing agreement
clauses for privacy protection in a data sharing agreement

Note 1 to entry: a privacy data sharing agreement can involve data transfer, data processing, and sharing of PII between joint *PII controllers* (3.15) (ISO/IEC 27701:2019 7.2.7)

3.20
privacy principles
set of shared values governing the privacy protection of *personally identifiable information* (3.14) when processed in information and communication technology systems

[SOURCE: ISO/IEC 29100:2011, 2.18]

3.23
privacy risk
effect of uncertainty on privacy

Note 1 to entry: Risk is defined as the “effect of uncertainty on objectives” in ISO Guide 73 and ISO 31000.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[SOURCE: ISO/IEC 29100:2011, 2.19]

3.24
privacy rule
statement specifying what is allowed or not concerning privacy

3.25
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO/IEC 27000:2018, 3.54]

3.26
processing of PII
operation or set of operations performed upon *personally identifiable information* (3.14)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO/IEC 29100:2011, 2.23]

3.27
smart city
effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its *citizens* (3.4)

[SOURCE: BSI PAS 181:2014]

3.28
smart city service governance body
body that acts as a supervisor for privacy recommendations or regulations concerning a *smart city* (3.27) service

3.29
supply chain
network of *organizations* (3.13) that are involved, through upstream and downstream linkages, in the *processes* (3.25) and activities that produce value in the form of products and services in the hands of the ultimate consumer

[SOURCE: ISO/TS 22318:2015, 3.3.5]

3.30
supplier
organization (3.13) of an individual that enters into an agreement with the acquirer for the supply of a product of services

Note 1 to entry: Other terms commonly used for supplier are contractor, producer, seller or vendor.

Note 2 to entry: The acquirer and the supplier sometimes are part of the same organization.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.45]

3.31
system of systems
large system that delivers unique capabilities, formed by integrating independently useful systems

[SOURCE: ISO/IEC/IEEE 24765:2017, 2]

3.32
task
required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a *process* (3.25)

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.50]

3.33
third party
privacy stakeholder other than the *personally identifiable information principal*, the *PII controller* (3.15) and the *PII processor* (3.17), and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor

[SOURCE: ISO/IEC 29100:2011, 2.27]

3.34
transparency
ability to ensure that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed

Note 1 to entry: This includes making information on PII processing available to *PII principals* (3.15).

[SOURCE: ISO/IEC TR 27550:2019, 3.24, modified — Note 1 to entry has been added.]

3.35
unlinkability
ability to ensure that a *PII principal* (3.15) may make multiple uses of resources or services without others being able to link these uses together

[SOURCE: ISO/IEC TR 27550:2019, 3.25]

3.36
work product
artifact associated with the execution of a *process* (3.25)

[SOURCE: ISO/IEC/IEEE 42020:2019, 3.26]

4 Abbreviated terms

AI	artificial intelligence
ICT	information and communication technology
IoT	internet of things
LINDDUN	linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance
OASIS	organization for the advancement of structured information standards
PIA	privacy impact assessment
STRIDE	spoofing of user identity, tampering, repudiation, information disclosure, denial of service, elevation of privilege

5 Privacy in smart cities

5.1 General

A smart city aims at the effective integration of physical, digital and human systems in the built environment to deliver a sustainable, prosperous and inclusive future for its citizens. It is a shared vision among city stakeholders to achieve a number of desired outcomes: well-being, transparency, sustainability, economic development, efficiency and resilience, collaboration and innovation. In this vision, economic development and innovation leverage ICT technology (e.g. IoT, big data, AI, cloud computing), and require a system of systems view to enable the integration of sector-specific systems (e.g. energy, transport, health). The integration of privacy

is a major concern. Guidance needs to be provided on how smart cities can follow the ISO/IEC 29100 principles:

— consent and choice;

— purpose legitimacy and specification;

— collection limitation;

— data minimization;

— use, retention and disclosure limitation;

— accuracy and quality;

— openness, transparency and access;

— accountability;

— information security; and

— privacy compliance.

5.2 Integration of privacy in the smart city reference framework

5.2.1 Smart city ICT reference framework in the ISO/IEC 30145 series

Figure 4 describes the smart city ICT reference framework in the ISO/IEC 30145 series. It consists of three frameworks:

— a business process framework which specifies the essential processes in the areas of governance, core business and support;

— a knowledge management framework which provides guidance on the modelling and management of knowledge for smart city business and operations; and

— an engineering management framework which provides a set of ICT layers for smart cities operation, i.e. the smart application layer, the data and service supporting layer, the communication and storage layer, the network communication layer and data acquisition layer.

The business process framework includes:

— governance processes, which focus on the establishment of policies, and the continuous monitoring of their proper implementation by governing bodies of a smart city, e.g. local public authorities; and

— core business and support processes, which focus on the running of business processes according to the smart city policies by smart city agencies or delegated business organizations.

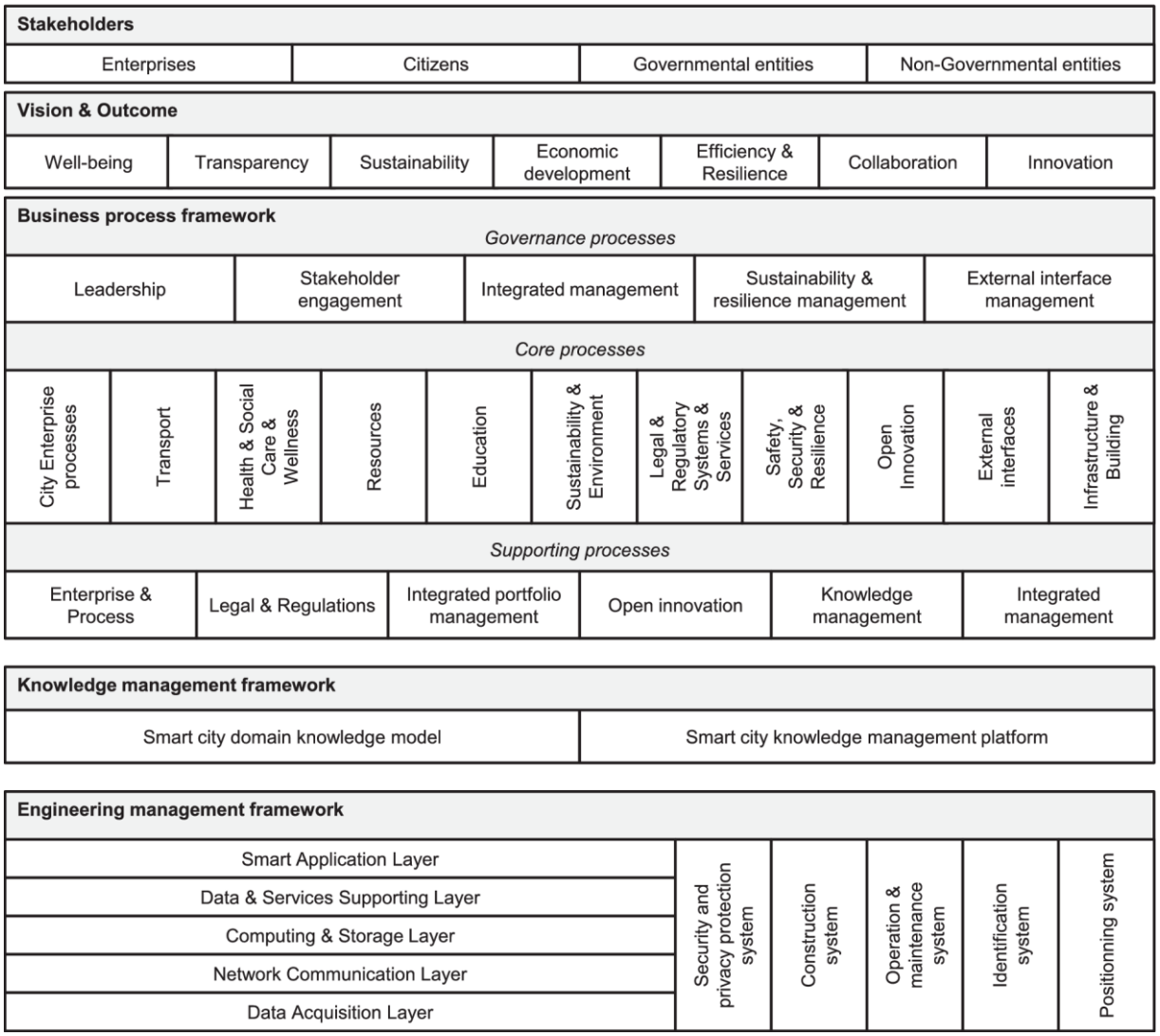


Figure 4 — Smart city ICT reference framework

The engineering management framework is described in Figure 5. This includes:

— the smart application layer focuses on domain applications, smart government, smart transportation, smart education, smart healthcare, smart home and smart campus which all rely on data processing;

— the data and services supporting layer focuses on data sources, data integration and service integration;

— the computing and storage layer focusses on computing, storage and software resources;

— the network communication layer provides communication infrastructure to smart cities with a high-capacity, high-bandwidth and high reliable optical networks and metropolitan wireless broadband network;

— the data acquisition layer provides the capability to sense the world and take actions; and

— vertical systems including the security and privacy protection system, the construction system, the operation and maintenance system, the identification system and the positioning system.

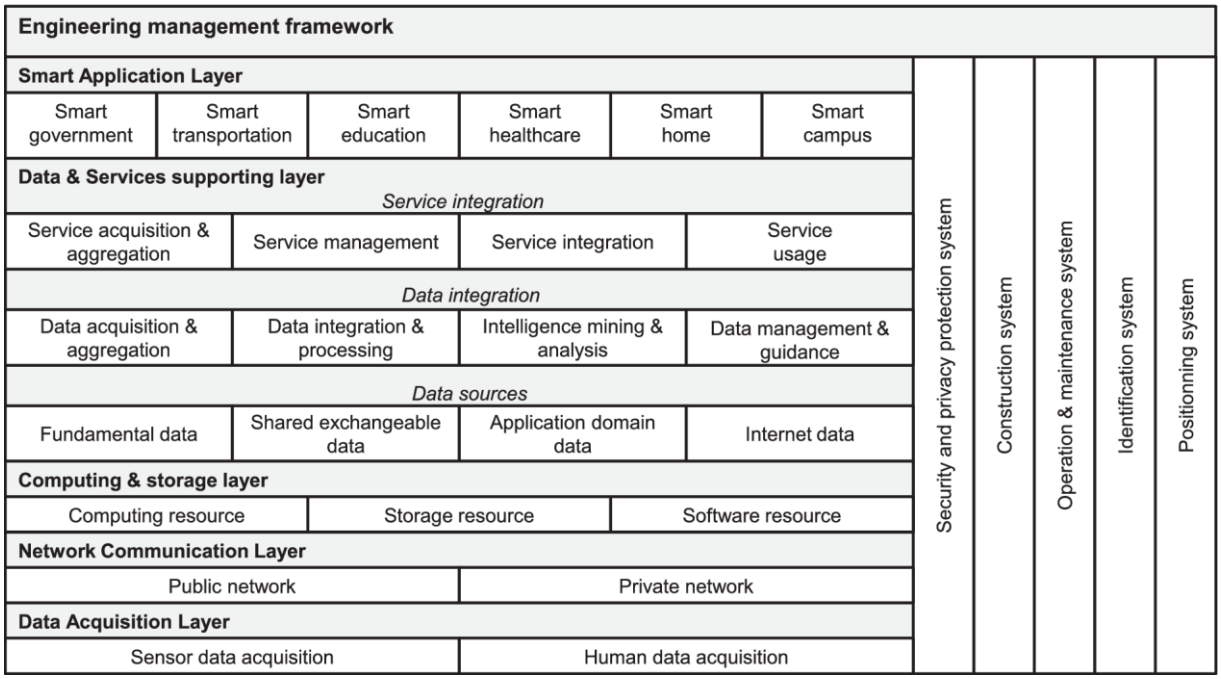


Figure 5 — Smart city engineering management framework

5.2.2 Privacy management activities in the ISO/IEC 30145 series

Processes of the smart city ICT reference framework can include privacy management activities:

— in the business process framework, processes can include additional activities related to PII:

  — the legal and regulatory systems and services process can deal with privacy regulation matters in order to ensure privacy compliance;

  — the safety, security and resilience process can deal with incidents causing privacy breaches;

  — the leadership and direction process can deal with governance of PII;

  — the stakeholder engagement and citizen focus process can deal with citizen queries concerning their PII;

— in the knowledge management framework, the knowledge base can include PII. For instance, knowledge about the provenance of data can provide links between PII principals and data:

— in the engineering management framework, all specified layers, i.e. the smart application layer, the data and services supporting layer, the computing and storage layer, the network communication layer, and the data acquisition layer can involve data leading to PII

5.3 Actor

Depending on the viewpoints, specific actors should be considered in a smart city vision which leverages ICT technology (e.g. IoT, big data, AI), and which requires a system of systems view to enable the integration of sector-specific systems (e.g. energy, transport, health). Depending

on the viewpoints (privacy, smart city, cloud computing, IoT, big data), specific actors should be considered in a smart city environment.

In activities related to privacy, the following actors are defined in ISO/IEC 29100:

— PII principals;

— PII controllers;

— PII processors; and

— third parties.

In activities related to data exchange and sharing for smart community infrastructures, the following roles are defined in ISO 37156:

— data creators, who create, capture, collect or transform data for e.g. a city or services;

— data owners who are the designated actors responsible for the data related to a city service. They define, validate each inherent attribute of the data;

— data custodians who are the custodians of a data for a specific purpose or task related to the provision of a service within the city;

— primary publishers who perform the publication for all data across the data spectrum;

— secondary publishers who create additional value from the city data that has been published; and

— users, e.g. city organizations, third sector organizations, business users, citizens, academic organizations or other cities.

In activities related to the cloud, the following actors are defined in ISO/IEC 17789:

— cloud service customers;

— cloud services partners; and

— cloud service providers.

The cloud service customer uses cloud services for the purpose of a business relationship. The cloud service provider makes cloud services available. The cloud service partner is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer.

In activities related to IoT, the following actors are defined in ISO/IEC 30141:

— IoT users;

— IoT service providers; and

— IoT service developers.

The role of IoT users is to administer and consume IoT services. The role of IoT service providers is to manage and operate IoT services. The role of IoT service developers is to implement, test and integrate IoT services.

In activities related to big data, the following actors are defined in ISO/IEC 20547-3:

— big data consumers;

— big data providers;

— big data application providers;

— big data framework providers; and

— big data service partners.

The role of big data consumers is to consume the value output of big data systems. The role of big data providers is to make data available. The role of big data application providers is to execute the manipulations of the data lifecycle. The role of big data framework providers is to provide a big data infrastructure, a big data platform, and big data processing. The role of big data service partners it to support big data application providers, big data providers and big data consumer.

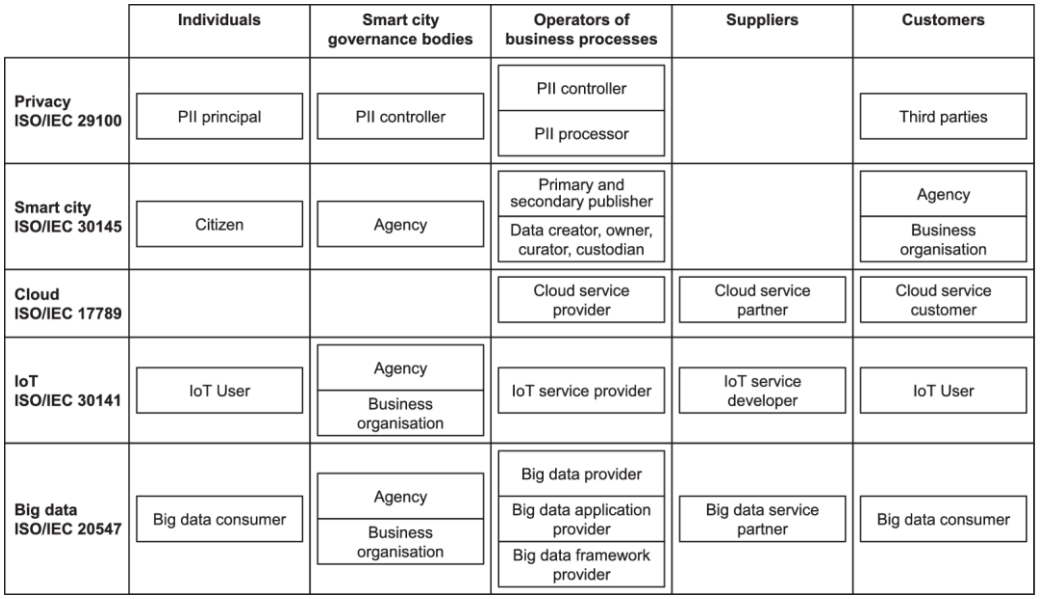


Figure 6 — Stakeholders in smart cities and their relationship with those defined in other relevant standards

Figure 6 shows five categories of stakeholders: individuals, smart city governance bodies, operators of business processes, suppliers and customers. For each category, examples of actors and roles are provided, taking a privacy viewpoint (ISO/IEC 29100), a smart city viewpoint (ISO/IEC 30145 series), a cloud viewpoint (ISO/IEC 17789) an IoT viewpoint (ISO/IEC 30141) and a big data viewpoint (ISO/IEC 20547-3):

— individuals can be:

  — PII principals who are impacted by privacy breaches;

  — citizens belonging to or visiting a smart city;

  - cloud service customers;
  - IoT users of an IoT service; and
  - big data consumers;
- smart city governance bodies can be:
  - PII controllers who determine the purposes and means for processing of PII;
  - agencies who perform overall governance duties;
  - agencies or business organizations who perform governance duties on cloud services;
  - agencies or business organizations who perform governance duties on IoT services;
  - agencies or business organizations who perform governance duties on big data services;
- operators of business processes can be:
  - PII controllers or PII processors;
  - stakeholders involved in data exchange and sharing with roles such as primary and secondary publisher, data creator, owner, curator, custodian;
  - cloud service providers;
  - IoT service providers; and
  - big data providers, big data application providers or big data framework providers;
- suppliers can be:
  - network or infrastructure operators;
  - cloud service partners;
  - IoT service developers;
  - big data service partners; and
- customers can be:
  - citizens or third parties;
  - government organizations or agencies;
  - non-government organizations;
  - business organizations;
  - cloud service customers;
  - IoT users; and

— big data consumers..

5.4 Challenges

Figure 7 illustrates integration problems in smart cities:

— IoT and big data are technology ecosystems which have to be integrated in the smart city ecosystem. Many smart cities applications are big data applications[3]. Many smart cities ICT systems are IoT systems. As stated by Andrea Zanella,[29] the Iot has the capability “to incorporate transparently and seamlessly a large number of different and heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services”;

— integration between different domains, such as smart grids, health, transport; and

— maintaining trust in services where the integration of multiple concerns such as security, privacy, safety and resilience is needed. For instance, the increasing combination of data points can raise the risk of creating PII.

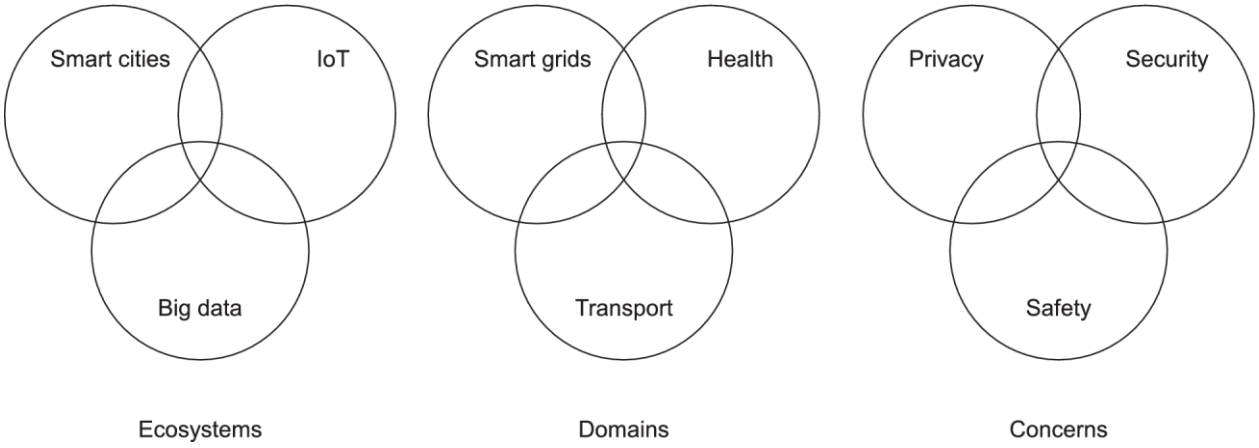


Figure 7 — Examples of ecosystems, domains and concerns

The need to integrate privacy has on impact on the following:

— the governance approach that is associated with concerns such as safety, security and privacy. For instance, a data protection authority might provide high-level rules (i.e. statement about what to do concerning privacy) and policies which, in turn, are used by smart city governance bodies to ensure specific compliance measures. These ensure proper rules and policies within the smart city ecosystem;

— the supply chain that is associated with the harvesting, collection, aggregation and transport of data in a smart city. For instance, data collected by a smart meter and further aggregated for data analysis involve a number of organizations (e.g. the manufacturer of a smart meter, the smart grid utility, the data analysts); and

— the data sharing ecosystem that is associated with data analysis in a smart city. For instance, multiple organizations can be involved in sharing energy data to improve its usage in different domains (e.g. transport, health, public infrastructures).

[1] For instance in Amsterdam (https://data.amsterdam.nl/), Berlin (https://daten.berlin.de/), London (https://data.london.gov.uk/) or Paris (https://opendata.paris.fr)

The following issues should be taken into account.

— In the governance approach, tracking the list of PII controllers and PII processors in order to address the accountability principle. For instance, the occurrence of a privacy incident can necessitate an action that impacts a specific stakeholder.

— In the supply chain, identifying how suppliers support privacy and communicating with them in order to enforce rules and policies. ICT technology includes a variety of products, end products such as sensors, devices, smart devices, cloud solutions or component products such as electronics, security modules, operating systems, middleware. Suppliers should provide appropriate privacy technical and organizational measures. For instance, a manufacturer of a storage system can include controls that would help PII controllers or PII processors.

— In the data sharing ecosystem, enforcing explicit privacy data sharing agreements when PII is processed and exchanged.

— The need to take into account individuals expectations including the right to be informed, to inform, correct, redress, restore and recover.

Table 2 shows examples of business vulnerabilities in smart cities.

Table 2 — Examples of business vulnerabilities in smart cities

Business aspect	**Vulnerabilities**
Governance	Smart city service governing body is not able to track all PII controllers or PII processors. For instance, it is not able to identify the PII controllers or PII processors that caused a breach.
	Smart city governing body has not defined clear rules and policies for privacy. It is not able to enforce privacy policies amongst PII controllers and PII processors.
Supply chain	Privacy impact assessments provided by suppliers are incomplete or inaccurate. For instance, they can be unaware of some privacy risks.
	PII controllers or PII processors rely on suppliers of components that do not support some desired privacy controls. For instance, a storage system does not include automated deletion capabilities.
Data sharing ecosystem	A stakeholder in the data sharing ecosystem is negligent on the enforcement of obligations. For instance, a stakeholder provides PII to another stakeholder without informing him about its obligations.
	Wrong assessment from a stakeholder that it is not a PII controller or PII processor. For instance, publishing open data that is not properly anonymized, or combining two datasets which do not contain PII into a dataset which contains PII.

6 Guidance on smart city ecosystems privacy protection

6.1 Ecosytem privacy plan

6.1.1 Recommendation R6.1

The smart city governance body should establish an ecosystem privacy plan.

6.1.2 Explanation

Figure 8 describes the relationships between organizations, processes and a smart city ICT reference framework as described in 5.1:

— an organization is a part of an ecosystem which follows the smart ICT reference framework;

— the smart ICT reference framework describes governance and integration processes as well as business and operation processes

— an organization implements processes that are related to roles, activities and functional components. For instance, an organization can be in charge of the big data application provider role; and

— an organization implements processes focusing on security and privacy. They are applied to protect assets in the smart city ICT reference frameworks against vulnerabilities. Some assets are specific to an organization, e.g. commercially sensitive information while others are shared within the ecosystems, e.g. open data. The organization can appoint a data protection officer in charge of ensuring, in an independent manner, compliance with the processes.

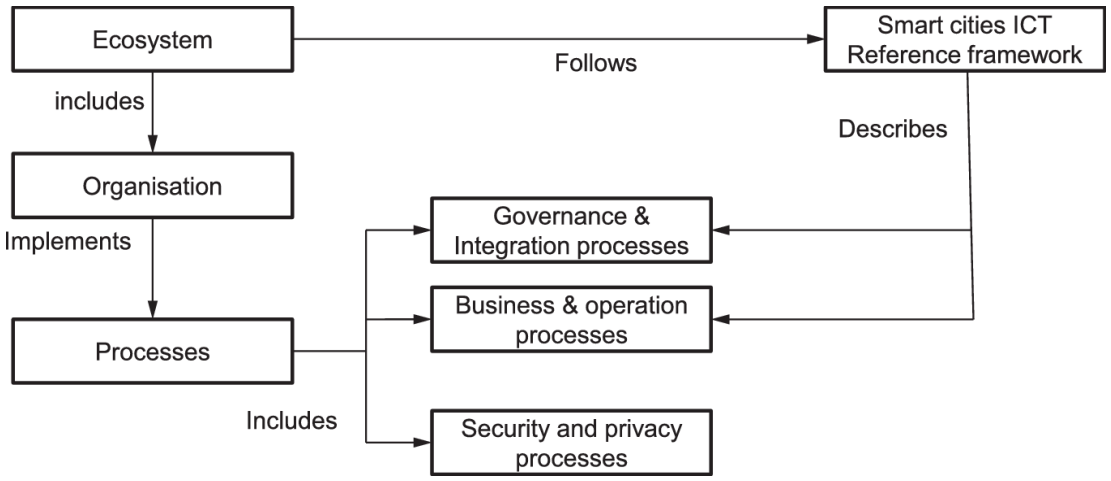


Figure 8 — Organizations in smart city ecosystems

There is a need to coordinate the processes of the organizations in a smart city ecosystem, as showed in Figure 9:

— an overall coordination by the smart city service governing body ensures consistency of each individual process; and

— each organization carries out its processes;

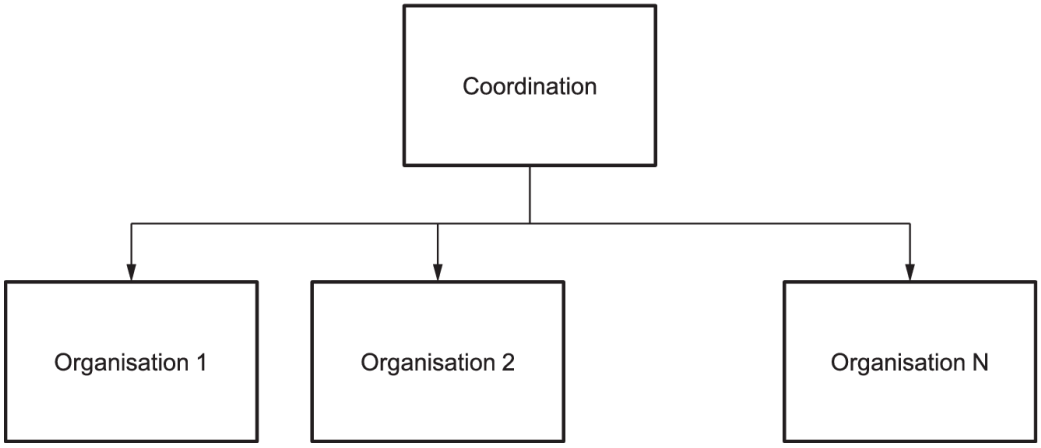


Figure 9 — Ecosystem coordination of organizations

6.1.3 Work product

The coordination is established through a smart city ecosystem privacy plan. Annex A provides an example of ecosystem privacy plan structure

6.2 Governance

6.2.1 Recommendation R6.2

The ecosystem privacy plan should specify the governance body operation.

6.2.2 Explanation

The coordination of privacy in smart city ecosystems is managed by a governing body. The governing body can take different forms, e.g. a public authority, a dedicated organization, an alliance. They can be dedicated to specific domains. For instance:

— organizations involved in smart traffic management apply security and privacy processes that are coordinated by a city transport agency;

— organizations involved in healthcare big data apply security and privacy processes that are coordinated by a city health agency; and

— organizations involved in energy grid service apply security and privacy processes that are coordinated by an ad-hoc working group in coordination with a city energy grid agency.

The coordination can involve data protection officers from the governing body and from the organizations of the ecosystem.

6.2.3 Work product

The smart city ecosystem privacy plan describes the governance body and its rules and procedures.

6.3 Supply chain

6.3.1 Recommendation R6.3

The ecosystem privacy plan should include supply chain management.

6.3.2 Explanation

The supply chain management ensures that contractual arrangements on privacy are sufficient. It ensures the following:

— PII controllers and PII processors in the supply chain are aware of the privacy rules and policies in the smart city ecosystem;

— PII processors receive proper instruction by PII controllers (e.g. through privacy data sharing agreements); and

— suppliers to the PII controllers and PII processors take into account those privacy rules and policies. (transmitted, for example, through contractual requirements).

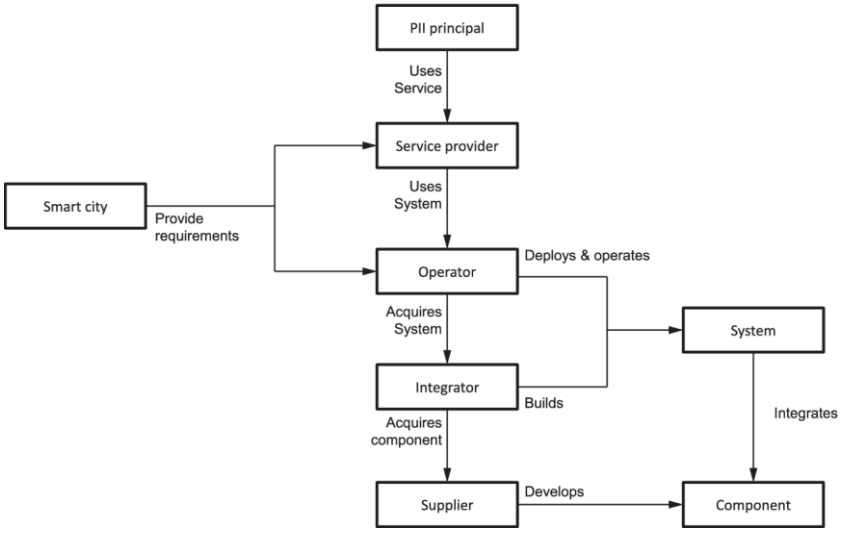


Figure 10 — Example of smart city supply chain

Figure 10 provides an example of supply chain for the creation of a system. It involves the following stakeholders:

— suppliers who provide the components making up a system, e.g. a sensor, a smart device, a cloud system;

— integrators who build the system, integrating the various components acquired from suppliers;

— operators who deploy, operate and maintain the system acquired from integrators;

— service providers who use the system to provide a service to end users;

— smart city authorities who provide requirements to application providers and operators concerning a service; and

— PII principals who use a service provided by the service provider.

Here is an example for a smart transport application providing real-time traffic advice to citizens. PII principals are the inhabitants of a city. The service provider is the city transport agency. The operator is a local SME associated with a major international cloud operator. The integrator is a very large company with experience in building complex systems. The suppliers are local producers of devices (e.g. a display system), an external start-up providing features for real-time advice, and a major operating system provider.

The supply chain is modified as showed in Figure 11 when privacy concerns are integrated:

— suppliers provide components that implement privacy controls that meet the requirements of the PII controllers and PII processors (e.g. de-identification techniques);

— integrators should provide the overall privacy controls integrating those provided by suppliers;

— PII controllers and PII processors carry out privacy management related operations (e.g. consent management, privacy breach management);

— data protection authorities and the smart city local authorities provide specific rules and policies to PII controllers and PII processors, for instance some specific privacy impact analysis guidelines;

— service providers get privacy guidelines from the data protection authorities;

— PII principals using the service are properly protected according to the rules and policies for privacy.

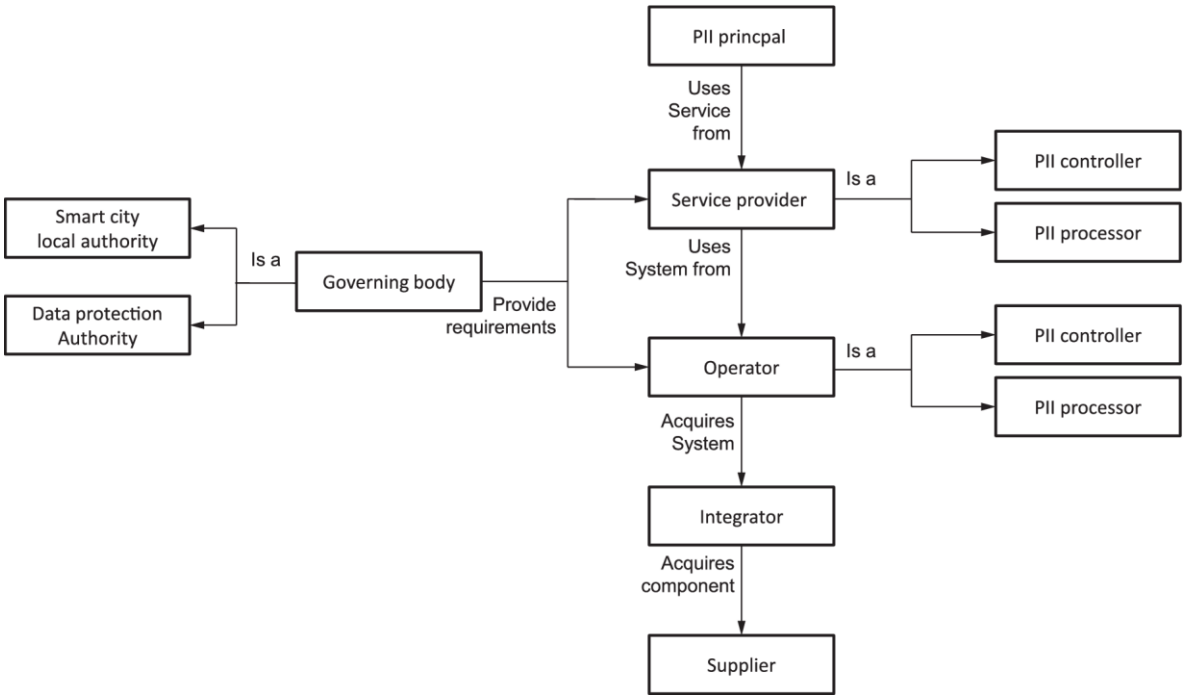


Figure 11 — Example of smart city supply chain integrating privacy

6.3.3 Work product

The smart city ecosystem privacy plan describes supply chain coordination.

6.4 Data management

6.4.1 Recommendation R6.4

The ecosystem privacy plan should include data management.

6.4.2 Explanations

Data processing stakeholders are further involved in a data sharing ecosystem. The integration of security and privacy in this value chain is depicted by Figure 12:

— two data processing stakeholders A and B negotiates a privacy data sharing agreement, where:

  — A is a PII controller and provides data to B which is a PII processor or a PII controller (scenario A); or

  — A and B are joint controllers (scenario B);

— the privacy data sharing agreement sets out obligations on data processing security and privacy capabilities provided by each stakeholder.

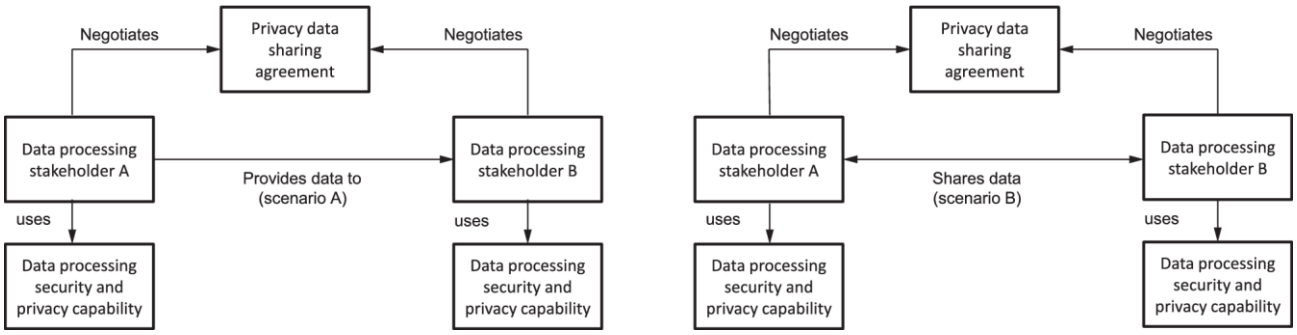


Figure 12 — Data sharing agreement from a security and privacy viewpoint

The coordination of privacy in data management ensures that:

— PII controllers and PII processors in the supply chain are aware of the privacy rules and policies in the smart city ecosystem;

— PII processors receive proper instruction by PII controllers (e.g. through privacy data sharing agreements);

— Suppliers to the PII controllers and PII processors take into account those privacy rules and policies; and

— if compliance verification is required by the governance process, determine the auditing stakeholders in charge of compliance.

For instance, an IoT system operator collects data that is provided as a dataset to a service provider which in turn combines it with other sources of data and provides it to a data consumer. As showed in Figure 13:

— an overall coordination of each organization’s data management processes to ensure that they follow compatible privacy rules and policies; and

— each organization carries out its own data management process.

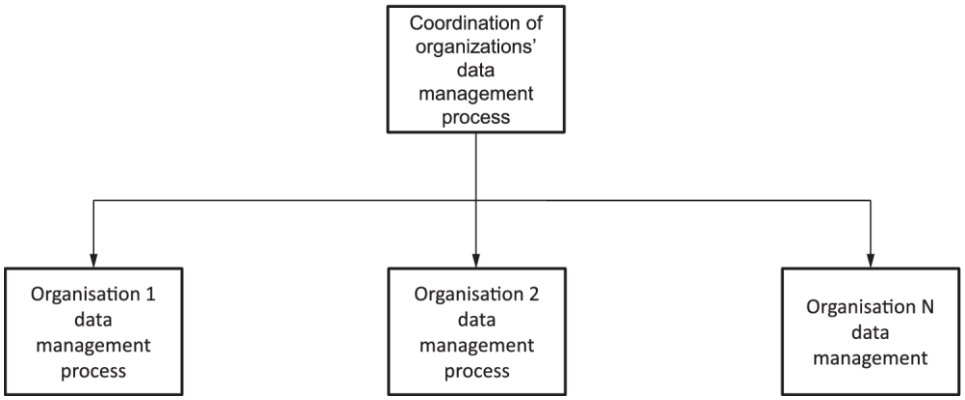


Figure 13 — Smart city management of data sharing **ecosystem**

6.4.3 Work product

The smart city ecosystem privacy plan describes data management coordination.

7 Guidance on standards for smart city ecosystems privacy protection

7.1 General

Figure 14 shows the various standards that can be used to guide organizations in the support of security and privacy. They cover the standards for:

— the governance process (8.2);

— the risk management process (8.4); and

— the engineering process (8.5).

NOTE These standards can be completed with further guidance documents (e.g. local standards).

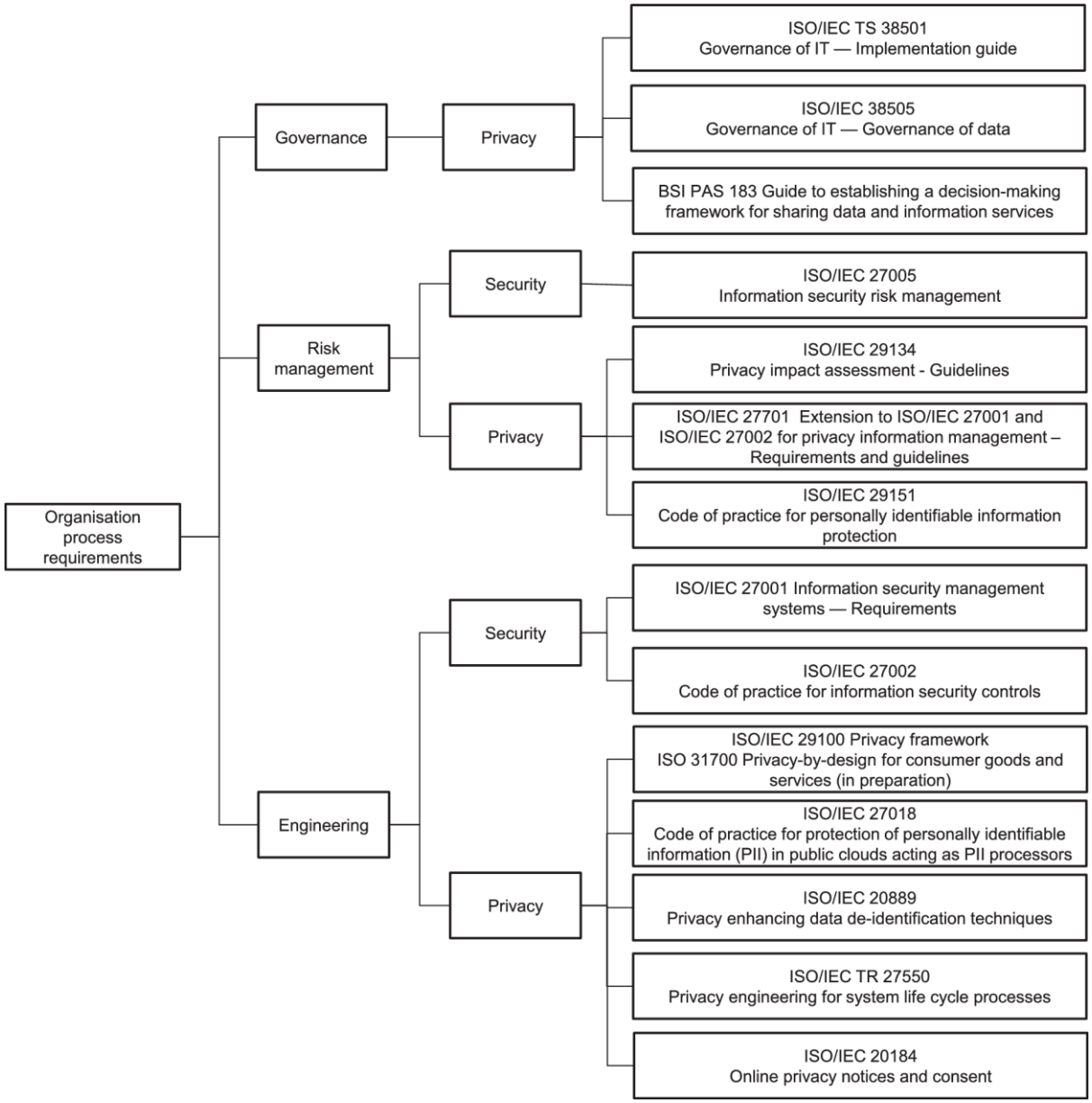


Figure 14 — Standards for organizations' privacy processes

7.2 Privacy governance

Smart city privacy processes dealing with governance can follow the following standards:

— implementation guide for IT governance as described in ISO/IEC TS 38501;

— IT governance for data as described in ISO/IEC 38505 (all parts);

— guide to establishing a decision-making framework for sharing data and information services as described in BSI PAS 183; and

— ecosystem coordination as described in this document.

7.3 Privacy risk management

Smart city privacy processes dealing with risk management can follow the following standards:

— information security risk management as described in ISO/IEC 27005;

— privacy impact assessment guidelines as described in ISO/IEC 29134;

— privacy requirements of smart city information systems as described in ISO/IEC 27701;

— code of practice for PII protection as described in ISO/IEC 29151; and

— ecosystem coordination as described in this document.

7.4 Privacy requirements

Smart city privacy processes dealing with engineering can follow the following lifecycle standards:

— security requirements of smart city information systems as described in ISO/IEC 27001;

— code of practice for information security controls as described in ISO/IEC 27002;

— privacy requirements of smart city systems resulting from the use of privacy principles as described in ISO/IEC 29100;

— code of practice for protection of PII in public clouds acting as PII processors as described in ISO/IEC 27018;

— privacy enhancing data de-identification techniques as described in ISO/IEC 20889;

— privacy engineering as described in ISO/IEC TR 27550;

— online privacy notices and consent as described in ISO/IEC 29184; and

— ecosystem coordination as described in this document.

8 Guidance on processes for smart city ecosystem privacy protection

8.1 General

This clause provides privacy guidelines for the creation, design, deployment and operation of a smart city service, focusing on the following processes:

— governance;

— data management;

— risk management;

— engineering; and

— citizen engagement.

Guidelines for each process are provided with the following content:

— a recommendation;

— an explanation of the activities at a global ecosystem level;

— guidelines for ecosystem coordination (carried out the smart city governance body);

— guidelines for organizations;

— standards and methods that can be used;

— examples; and

— the work product which describes the process.

8.2 Governance process

8.2.1 Recommendation R8.2

A governance process should be established by the smart city service governance body to ensure privacy management coordination of smart city ecosystems.

8.2.2 Explanations

The governance process focuses on the establishment of privacy policies, and the continuous monitoring of their proper implementation in a smart city service. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem which implement the privacy policies, as shown in Figure 15.

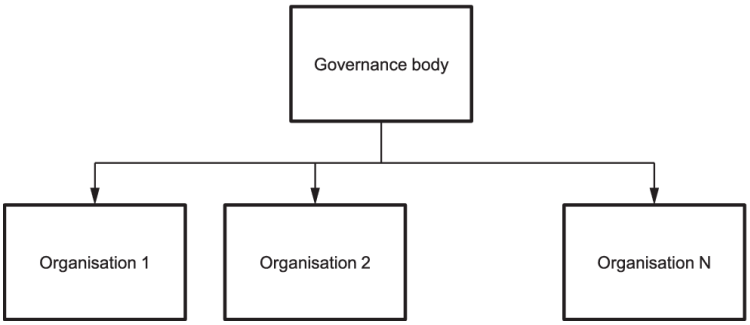


Figure 15 — Governance process stakeholders

8.2.3 Guidance on ecosystem coordination

The following guidance is provided at the ecosystem level:

— assess whether the creation of a smart city service requires specific privacy governance. In this case:

  — specify the rules and policies of the new privacy governance;

  — specify a privacy governance describing supervision requirements, and the resulting supervision activity;

  NOTE 1 Rules and policies includes guidelines for data retention policies between organizations sharing data.

— assess whether a privacy competence program (regulation, technical and organizational) should be implemented and include the outcome from the assessment in the governance, risk management, data management, privacy engineering and citizen engagement processes.

NOTE 2 An example of regulation in Europe is GDPR.

— identify the supervised organizations for privacy governance and their responsibilities (e.g. PII controllers, PII processors, integrators or suppliers);

— establish and implement a communication and supervision activity, ensure that rules and policies are well communicated to organizations and implemented and if appropriate interact with specific organizations in the ecosystem (e.g. citizen complaints, privacy breach incidents); and

— establish and implement appropriate procedures for the protection of citizens' rights and interact throughout the process with data protection authorities.

NOTE 3 The communication activity includes requirements on information exchanged, agreement on controls applied and auditing capabilities.

8.2.4 Guidance for organizations

The following guidance is provided at the organization level:

— request the creation of privacy governance to the smart city governance body or, if governance already exists, request participation to the governance process;

— participate in the competence program;

— participate in the communication and supervision activity:

— implement the measures that meet the rules and policies associated with the privacy governance and, if appropriate, interact with the governance bodies (e.g. citizen complaints, privacy breach incidents); and

— interact with the governance body to provide information required for supervision.

8.2.5 Standards and methods

The following standards and methods can be used:

— ISO/IEC 30145 series is used as an overall framework;

— ISO/IEC 38500 is used by the governing body to govern the use of IT through three tasks: evaluate, direct and monitor;

— ISO/IEC TS 38501 is used to support the implementation of the governance process, through a cycle of three activities: establish and sustain enabling environment, govern IT and continual review;

— ISO/IEC TR 38502 is used to build a governance framework. This includes the following: principles for good governance, strategies and policies for the use of IT, business planning for IT, management systems for IT, the organization's use of IT, accountabilities and risk management; and

— ISO/IEC 38505-1 and ISO/IEC TR 38505-2 are used to build a data specific governance.

EXAMPLE A smart city deploys sensors to collect weather data, traffic data or energy usage data. Two services, a smart traffic application and an energy resource management are implemented. The first service is operated directly by a city agency (A). The other service is operated by a private organization (B). The whole program includes an ecosystem of organizations (C, D, E) collecting, treating and analysing data. Some data contain PII, for instance data collected by sensors in vehicles. Consequently, the city establishes a governance process according to this document: it identifies a supervising agency (A), and supervised organizations: A and B are PII controllers, C, D are PII processors, and E is a supplier of sensors. City agency A implements a communication and supervision activity addressing agreements on data management. This includes rules for public information (e.g. documentations associated with sensors being installed in vehicles). It also includes rules and policies for data retention. The activity requires periodic annual meetings and reviews leading to continual improvement decisions. The meetings and reviews are organized by city agency A.

8.2.6 Work product

The ecosystem privacy plan describes the governance process.

8.3 Data management process

8.3.1 Recommendation R8.3

A data management process should be established by the smart city service governance body to ensure protection of PII.

8.3.2 Explanations

The data management process focuses on the management of privacy in the creating, capturing, collecting, transforming, publishing, accessing, transferring and archiving of data within a smart city service. Actors can be smart city agencies or businesses. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem as showed in Figure 16. A prerequisite to this process is the synchronization with the governance, risk management and engineering processes.

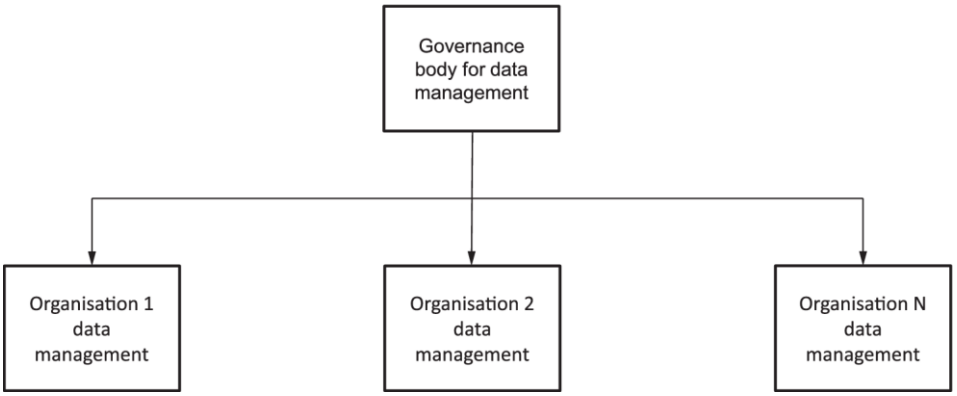


Figure 16 — Data management process stakeholders

8.3.3 Guidance on ecosystem coordination

The following guidance is provided at the ecosystem level:

— initiate the governance process and demonstrate that the data sharing purpose is compliant with policies and regulations;

— initiate the risk management process as required;

— initiate the engineering process as required;

— specify the privacy impact assessment and sharing agreement templates to use; and

— establish and implement coordination schemes in the ecosystem, concerning:

  — the participation of new organizations to a data sharing community;

  — the extension of data sharing to new applications:

  — the compliance of data sharing applications with agreed policies as well as regulation; and

  — assurance and audit of practice.

8.3.4 Guidance for organizations

The following guidance is provided at the organization level:

— initiate the governance process as required;

— initiate the risk management process as required;

— initiate the engineering process as required,

— use the privacy impact assessment and sharing agreement templates recommended at coordination level; and

— carry out data sharing activities in accordance with the ecosystem coordination scheme.

8.3.5 Standards and methods

The following standards and methods can be used:

— BSI PAS 183 is used to implement a transparent approach to making decisions and creating specific data sharing agreements;

— ISO 37156 provides a framework for data exchange and sharing to entities having authority to develop and operate community infrastructure; and

— ISO/IEC 29184 provides controls, which shape the content and the structure of online privacy notice as well as the process of asking consent to collect and process PII from PII principals.

EXAMPLE 1 A city agency operates an infrastructure to collect smart meters data in order to optimize its overall energy resources. Data is collected with the consent of the inhabitants for

the purpose of energy study uniquely. The collected data is made available to a number of data analytics companies through a data sharing agreement which explicitly forbids organizations in the data sharing ecosystem to use the data for another purpose than energy study, and states that transmitted data is removed after analysis. The city agency establishes a data management process according to this document. This includes a reporting mechanism. Organizations in the data sharing ecosystem report annually providing information such as PIA annual report update, the list of processing carried out and the PII removal actions.

EXAMPLE 2 A private energy agency deploys a service for energy management optimization in an eco-district consisting of multiple smart buildings. Consent is provided by inhabitants for the collection and analysis of data provided by the various smart meters and HVAC devices installed in the buildings by different suppliers. The agency establishes a data management process according to this document. This includes a contractual agreement specifying the purpose for collecting and processing data signed by the stakeholders authorized to access data. Data management activities are deployed in accordance with the ecosystem coordination scheme. A new application provider wants to access to data in order to provide marketing services. As the new application does not comply with the smart city policy, it is not allowed to access collected data.

8.3.6 Work product

The smart city ecosystem privacy plan describes the data management process.

8.4 Risk management process

8.4.1 Recommendation R8.4

A risk management process should be established by the smart city service governance body to assess privacy impact.

8.4.2 Explanations

The risk management process deals with the analysis and the treatment of risks to the privacy on PII principals in a smart city service. The activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem as showed in Figure 17. A prerequisite to this process is the synchronization with the governance process.

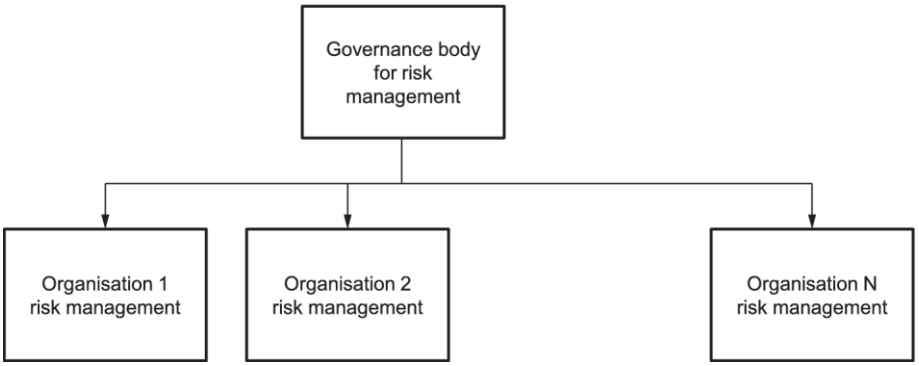


Figure 17 — Privacy risk management process stakeholders

8.4.3 Guidance on ecosystem coordination

The following guidance is provided at the ecosystem level:

— initiate the privacy governance process if it is not in place yet;

— establish and implement specific risk management coordination schemes in the ecosystem. This includes:

  — a mapping of the system of systems to the organizations of the ecosystem, and the specification of their roles in the risk management process;

  — the coordination of the risk management activities including the system of systems risk analysis and monitoring, compliance, assurance and audits of practice;

— establish and implement the risk management process of the smart city service viewed as a system of systems. This includes:

  — the identification of the vulnerabilities and threats to privacy in the system of systems;

  — the identification of the potential risks and breaches in the system of systems;

  — the evaluation of the potential impact to the PII principal;

  — the identification of controls to treat the risks of the system of systems;

  — the risk treatment implementations by the organizations of the ecosystem; and

  — the implementation of continual improvement and the related communications of improvements to the ecosystem.

NOTE 1 The system of systems risk management process is carried out under the responsibility of the smart city service PII controller who can be different from the organization in charge of ecosystem coordination.

NOTE 2 The risk assessment includes the identification of relevant legislation and contracts applicable.

8.4.4 Guidance for organizations

The following guidance is provided at the organization level:

— establish and implement a risk analysis process of the system(s) the organization is responsible for. The process includes:

  — the identification of the vulnerabilities and threats of the system(s) which the organization is responsible for;

  — the identification of process owners, risks owners and individuals that are involved in the processing;

  — the identification of the risks and breaches of the system(s);

  — the evaluation of the potential impact to the PII principal;

  — the identification of proposed controls to treat the risks of the system(s);

  — the risk treatment implementations; and

  — the implementation of continual improvement.

— establish and implement a risk management process in accordance with the specific ecosystem coordination schemes and the governance process described in 8.2. This can include the implementation of an information security and privacy risk impact assessment method.

NOTE 1 The information security and privacy risk impact assessment method includes the following steps: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, risk monitoring and review.

NOTE 2 If the application of the risk assessment step provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete and the risk treatment follows. if the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) is conducted, corresponding to the plan–do–check–act (PDCA) cycle.

8.4.5 Standards and methods

The following standards and methods should be used:

— ISO/IEC 29134 to support privacy risk analysis;

— ISO/IEC 27701 is used to support the identification activity of privacy controls to treat the risks of the system.

Classifications such as STRIDE or LINDDUN[27][28] can be used to support the activity of identifying threats.

EXAMPLE A smart city transportation agency deploys a service for intersection collision warning. The service is based on connected vehicles capabilities to broadcast at a high frequency cooperative awareness messages,[30] or information about their position, direction or speed. These messages are received by other vehicles as well by road side units deployed in intersections, analysed in real-time to detect case of potential collisions in order to trigger collision avoidance actions. There is a lapse of time when consecutive cooperative messages from the same vehicle are received. The vehicle cannot be tracked because messages are transmitted with pseudonyms. In order to ensure authentication of messages, all pseudonyms are signed sent with a public key certificate.[31] The ecosystem includes the following organizations: multiple operators of connected vehicle capabilities, multiple operators of road side units, multiple public key certificate providers and multiple operators of the service.

8.4.6 Work product

The smart city ecosystem privacy plan describes the risk management process.

8.5 Engineering process

8.5.1 Recommendation R8.5

An engineering process should be established by the smart city service governance body to take in consideration, whenever possible, a privacy-by-design approach.

8.5.2 Explanations

The engineering process is a set of activities related to the lifecycle of a smart city service. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem concerned with the delivery, the use of the availability of a

smart city service, as showed in Figure 18. A prerequisite to this process is the synchronization with the governance and the risk management processes.

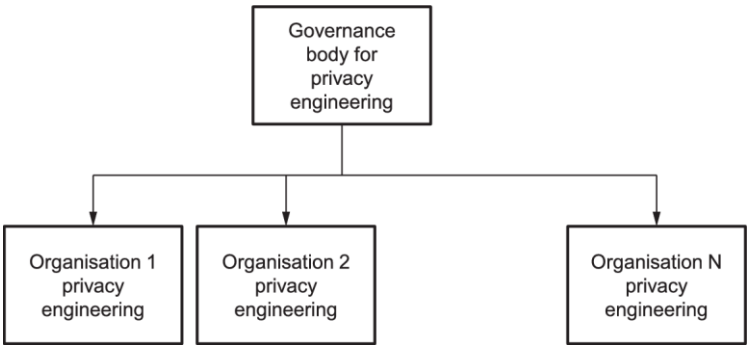


Figure 18 — Privacy engineering process stakeholders.

8.5.3 Guidance on ecosystem coordination

The following guidance is provided at the ecosystem level:

— initiate the privacy governance process if not in place;

— initiate the privacy risk management process if not in place;

— establish and implement specific privacy engineering coordination schemes in the ecosystem. This includes:

  — a mapping of the system of systems to the organizations of the ecosystem and the specification of their roles in the privacy engineering process;

  — the coordination of the privacy engineering lifecycle activities that will lead to the design of appropriate system of systems privacy controls; and

  — the coordination of the privacy engineering lifecycle activities related to assurance, compliance approach, or audit;

— establish and implement the privacy engineering process for the smart city service viewed as a system of systems. This includes:

  — a specification of the data model of the system of systems, focusing on data assets, data flows and processing of PII;

  — a risk management process of the system of systems as described in 8.4;

  — the activities in the privacy engineering systems of system lifecycle that will lead to the specification of privacy policies, conformance criteria, privacy technical requirements, privacy controls and privacy service and functions of the systems of system and their mapping to the organizations of the ecosystem;

  — the activities for continual improvement involving a periodic review of requirements and measures and their mapping to the organizations of the ecosystem.

NOTE 1 The activities in the privacy engineering process can include the resolution of conflict scenarios and the identification of resulting privacy policies. The goal in the engineering of a smart city product or service is to find a balance between the constraints and the needs of all the organizations and

stakeholders, and the individual's privacy rights in the design phase, operational phase, maintenance phase, registration phase of the individuals (if any) and deregistration phase of the individuals (if any).

NOTE 2 PII processing related to data assets and data flows can include collection, retention/logging, generation/transformation, disclosure/transfer and/or disposal. Other terms used are data at rest, data in motion.

8.5.4 Guidance for organizations

The following guidance is provided at the organization level:

— establish and implement a privacy engineering process of the system(s) the organization is responsible for, including:

  — the specification of the data model;

  — the risk analysis;

  — the activities of the system(s) lifecycle;

  — and the definition of continual improvement;

— establish and implement a privacy engineering process in accordance with the specific ecosystem coordination schemes and the governance process described in 8.2, including the design phase, the usage phase, and the customer relationship management phase.

NOTE 1 The activities concerned by the customer relationship management (CRM) can include the acquisition of a product and/or the subscription to a service, the delivery of a product or a service, the support, service, maintenance and assistance for a product or a service, the marketing of the evolutions of the product or of the service or news related to the products or the services, and the recycling or disposal of a product or de-registration to a service.

NOTE 2 Smart city services are often added on top of other existing services. In such a case, privacy-by-design takes into account that existing infrastructure.

8.5.5 Standards and methods

ISO/IEC 29100 should be used.

It provides the principles to apply: consent and choice; purpose legitimacy and specification; collection limitation; data minimization; use, retention and disclosure limitation; accuracy and quality; openness, transparency and access; accountability; information security; and privacy compliance.

The following standards and methods can be used:

— the model and methodology provided by OASIS PMRM[32] is used to support the system of systems privacy engineering process. It is used to describe data assets and data flows and provide a picture of all domains, systems, and processes in which PII is used; to specify privacy policies and conformance criteria; to conduct a privacy analysis leading to the identification of requirement; to specify the privacy controls associated with PII, including internal privacy controls created within the domain/sub domain, but also privacy controls inherited and exported to/from other domains/subdomains; and finally to define privacy services and functions to be implemented in technical privacy mechanisms for data chains within an ecosystem;

— ISO/IEC TR 27550 is used to support the system of systems privacy engineering process. It identifies security and privacy properties that are used in the process such as confidentiality, integrity, availability, unlinkability, transparency or intervenability. It identifies privacy engineering design properties that are used in the process: data-oriented strategies (minimize, separate, abstract, hide) and process oriented strategies (inform, control, enforce, demonstrate);

— ISO/IEC 27701 is used to support the identification activity of privacy controls to treat the risks of the system; and

— ISO/IEC 20889 is used to specify terminology, a classification of de-identification techniques according to their characteristics and their applicability for reducing the risk of re-identification.

EXAMPLE A smart city deploys a smart city service to collect a variety of environment data such as weather conditions or road maintenance status. It takes advantage of the existence of an open ecosystem for provisioning vehicle data where citizens install a data collecting capability on their vehicles and trade collected data through personal data vaults: diagnosis data are provided to car manufacturers, meteorological data are provided to a local weather forecast organization and road conditions data are provided to the road maintenance organization.[33] The ecosystem includes the following organizations: multiple personal data vaults service providers, market place operators, global and local service providers. The city establishes an overall coordination scheme covering governance, risk management, data sharing, privacy engineering and citizen engagement according to this document. The ecosystem privacy engineering process includes the periodic assessment of privacy principles for minimizing data transfer from personal data vaults to service providers. The privacy engineering coordination involves the personal data vaults service providers, the market place operators, and the service providers, it identifies the suitability to switch to a new de-identification technique, synchronizing with the privacy engineering activities of each organization.

8.5.6 Work product

The smart city ecosystem privacy plan describes the engineering process.

8.6 Citizen engagement process

8.6.1 Recommendation R8.6

A citizen engagement process that integrates privacy should be established by the smart city service governance body.

8.6.2 Explanations

The citizen engagement process focuses on consultation with smart city citizens on rules and policies at governance level, and on the support on the enforcement of these rules and policies concerning the privacy of a smart city service. These activities are carried out by the governing bodies of a smart city, as well as by the organizations in the ecosystem as showed in Figure 19.

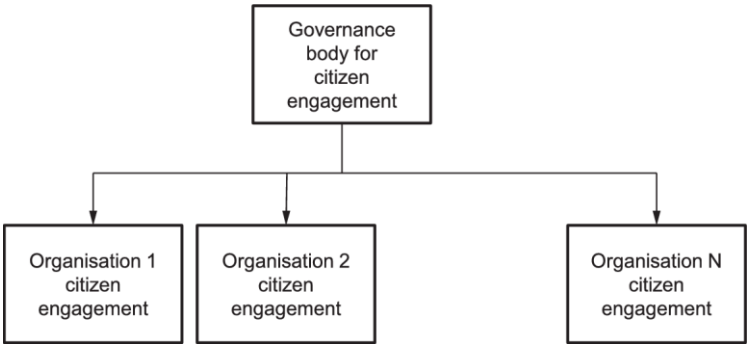


Figure 19 — Privacy citizen engagement process stakeholders

8.6.3 Guidance on ecosystem coordination

The following guidance is provided at the ecosystem level:

— establish a citizen dialogue and co-decision process for the establishment of smart city rules and policies for privacy, in accordance with the governance process described in 8.2. Examples of topics are smart city policies for consent notice or transparency of information on smart city services PII processing;

— establish a citizen interaction activity, including for instance information events, enquiries and complaints;

— for each service to be deployed, determine whether a citizen consultation is needed that will review service purpose, ethics and privacy;

— for each service to be deployed, foster the creation of enablers to facilitate citizens engagement (e.g. privacy apps);

— carry out periodic citizen review of services and provide recommendations for amendment when appropriate;

— carry out periodic citizen review of the smart city rules and policies;

— establish citizen dialogue and co-decision requirements that organizations of the ecosystem should meet; and

— establish coordination schemes in the ecosystem for organizations that have citizen concertation requirements.

NOTE The activities in the citizen engagement process can include conflict scenarios resolutions which are addressed when defining privacy policies.

8.6.4 Guidance for organizations

The following guidance is provided at the organization level:

— identify whether citizen dialogue and co-decision requirements should be met by the organization;

— if appropriate, implement citizen dialogue and co-decision requirements;

— if appropriate, participate in periodic citizen review of services; and
— implement amendments.

EXAMPLE 1 A smart city develops a smart city service that aims at recommending citizens and visitors where to go at what time, based on different data sources including weather, traffic but also personal profiles (e.g. demographical data, consumption patterns, location history). Because processing PII will make the recommendations better, and to avoid bad publicity, they decide to engage with citizens to understand their privacy concerns and to establish appropriate privacy policies in a citizen engagement process, which is instigated from the very beginning of the development process. This allows the city and citizens to understand and integrate privacy concerns and service needs, and to assess what they are willing to share in order to get what in return. Essential parts of the dialogue process are frequent reports established in the coordination scheme, which foster transparency, keep the public up to date, manage expectations and create trust.

This attention on the project also led to review policies for consent, and approaches for data minimization. The outcome of the review of consent policies is twofold. First, a decision to provide a higher score to services where the PII controller is part of the ecosystem coordination scheme. Second, the recommendation that in public spaces in cities consent is, in many cases, not the right legal ground for processing. Regarding data minimisation approaches, the most important outcome was that any data collection needs to be tightly linked to clear and specific purposes defined a priori.

EXAMPLE 2 A smart city installs video cameras with the objective of identifying vehicle license plates to enable automated tool collection. Consent is not given by the individuals but by the governance of the city. A citizen engagement process is applied in order to agree on the procedures for informing individuals on the treatments that are made, and on the modalities for periodic audit of the system video cameras operation. Annex B provides further considerations on the use of video cameras in smart cities.

8.6.5 Work product

The smart city ecosystem privacy plan describes the citizen engagement process.

Annex A
(informative)
Example of ecosystem privacy plan structure

Table A.1 provides an example of an ecosystem privacy plan structure

Table A.1 — Example of an ecosystem privacy plan structure

Section	Subsection	Description or content
Identification	Smart city name	Unique name of smart city ecosystem
	Responsibility	Name and signature of person responsible for ecosystem privacy plan
	History	Lists the reviews and evolutions of the privacy plan. Also includes a calendar for update plans.
	Confidentiality	Express the confidentiality of the plan, or of some of its section. Plan is structured so that there are sections that are public, and others that confidential but accessible for control by identified stakeholders.
	Information repository	URL to repository of information on smart city ecosystem. Can include a public part, as well as a private part.
Description of smart city service	General service description	Description of the service Description of the operational environment of the service (stakeholders, systems) Description of applicable laws and regulation, description of application standards
	General ecosystem description	Description of business chains (governance, supply chain, data management)
	Stakeholders	List of organizations in ecosystems and roles
Description of smart city ecosystem	Governance body	Description of governance scheme and objectives, description of governance body Description of rules and procedures: nomination of members of the governance body, operations Members of the governance body
	Supply chain management	Description of supply chain Description of management objectives Description of coordination procedures, information exchanged, access rights and monitoring approach Identification of stakeholders in supply chain that have an influence on privacy (e.g. PII controllers and processors, suppliers of privacy controls)
	Data management	Description of data flow in ecosystem Description of management objectives Description of coordination procedures, information exchanged and monitoring approach Identification of stakeholders in data sharing ecosystem that have an influence on privacy (e.g. PII controllers and processors)
Privacy management plan	Governance process	Description of how the governance process (8.2) is applied and reassessed for continual improvement Rules and policies for privacy governance Supervision requirements and activity Competence program

Section	Subsection	Description or content
		Communication and supervision activity, dashboard requirements Procedures for the protection of citizens' rights Interaction activity with data protection authorities
	Data management process	Description of how the data management process (8.3) is applied and reassessed for continual improvement Privacy impact assessment templates, sharing agreement templates, standards to be used Coordination of data management in ecosystem and dashboard operation Measures for compliance assurance and audit of practice
	Risk management process	Description of how the risk management process (8.4) is applied and reassessed for continual improvement Practices to be applied, standards to be used Coordination of risk management in ecosystem and dashboard operation Measures for compliance assurance and audit of practice
	Engineering process	Description of how the engineering process (8.5) is applied and reassessed for continual improvement Practices to be applied, standards to be used Coordination of privacy engineering lifecycle activities in ecosystem and dashboard operation Measures for compliance assurance and audit of practice
	Citizen engagement process	Description of how the citizen engagement process (8.6) is applied and reassessed for continual improvement Practices to be applied, standards to be used Coordination of citizen engagement activities in ecosystem and dashboard operation (e.g. on co-decisions) Measures for compliance assurance and audit of practice

Annex B
(informative)
Using video cameras in smart cities

B.1 Data flow treatment of video cameras

Video cameras are sensors that transmit video data and optionally sound data. Video data can be in transmitted in the visible spectrum and/or in the infra-red spectrum. They can then be analysed, aggregated with other data and used in order to extrapolate information.

Cities or its stakeholders can be interested in using this information for multiple objectives like traffic management, energy reduction or crime detection. For instance, information about accidents and traffic jams can be used to alert the police or to reroute traffic.

The challenge is that cameras produce, as soon as they observe human activities, privacy sensitive information, the management of which is often covered by strict national or regional regulations.

Typically, installation and operation of a camera in areas open to the public is subject to an authorization for a designated purpose and the owner of the camera is also the owner of the data produced and as such liable on their usage.

The provisions below should accordingly be considered as generic. The implementer of smart city cameras should identify applicable regulations which, in some cases, can prohibit any camera sharing between applications.

B.2 Privacy concerns

Privacy concerns arise when collected data, possibly aggregated from multiple information sources can be used to identify an individual or to indirectly identify an individual, e.g. by collecting vehicle license plate numbers. Treatments made on raw video data can enable the recognition of individuals or/and vehicle license plate numbers. Further, captured images can be kept for unknown duration.

B.3 Intended purpose

The intended purpose of data collection and data aggregation should always be clearly identified. A balance between the advantages for the city or its stakeholders and the drawbacks for the citizens, if any, should be established. Once a proper balance has been agreed, the intended purpose should be advertised. These activities can be supported by the governance process (8.2), the risk management process (8.4) and the citizen engagement process (8.6) described in this document.

Further, the intended purpose of data collection and data aggregation should be established before a system is designed. In addition, accountability measures should be specified during the design phase to increase confidence that only the intended purpose is being addressed. These activities can be supported by the data management process (8.3) and the engineering process (8.5) described in this document

B.4 Non - intended purpose

Raw data from video cameras is often transmitted to a data centre to perform a treatment corresponding to an intended purpose. But the data centre can also be in a position to perform non-intended treatments. Such additional treatments should be scrutinized. A balance between the advantages for the city or its stakeholders and the drawbacks for the citizens, if any, should be established and proper balance should be agreed concerning:

— human beings (cameras can simply be used to count the number of people or to identify the citizen faces);

— vehicles (cameras can simply count the number of vehicles or track their owners and count the number of people sitting in the front seats); or

— areas (cameras can simply be used to monitor air pollution or to record the movement of vehicles and people in case an incident happens in an area).

One problem is to get confidence that the specific purpose for which cameras were initially installed is not diverted later to another purpose that has not been disclosed (and approved).

B.5 Unlawfully data sharing with third parties

Treatments that can be made of video captures are usually under the responsibility of the city or of the police of the city. When smart city technology is outsourced to private corporations, there are risks that PII can be unlawfully shared with third parties. Some of the equipment provided to achieve the intended purpose can contain backdoors which can be activated during a software update. If the data flows that are used correspond to published data flows, then they can be analysed and even filtered to make sure that they only transmit the intended data. Otherwise, full confidence needs to be placed in the equipment manufacturer.

B.6 User consent

User consent is one of the major privacy principles. However, in the case of video cameras, individual user consent is not possible. Consent is not given directly by individuals but by the governance of the cities or of the governments of the countries where the cameras are installed. It is generally recommended that individuals who think that their image has been recorded be given access and possibility to get the relevant data masked or erased. Some consumer groups can be invited through the citizen engagement process (8.6) to appreciate the balance between the benefits for the city or its stakeholders and the drawbacks for the individuals. Measures for informing individuals on the treatments that are made by these cameras should be implemented.

Bibliography

[1] ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

[2] ISO/IEC 17789:2014, *Information technology — Cloud computing — Reference architecture*

[3] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*

[4] ISO/IEC 20547-3, *Information technology — Big data reference architecture — Part 3: Reference architecture*

[5] ISO/IEC 20547-4, *Information technology — Big data reference architecture — Part 4: Security and privacy*

[6] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[7] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[9] ISO/IEC 27018:2019, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[10] ISO/IEC TR 27550:2019, *Information technology — Security techniques — Privacy engineering for system life cycle processes*

[11] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[12] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[13] ISO/IEC 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[14] ISO/IEC 29151:2017, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[15] ISO/IEC 29184:2020, *Information technology — Online privacy notices and consent*

[16] ISO/IEC 29190:2015, *Information technology — Security techniques — Privacy capability assessment model*

[17] ISO/IEC 30141:2018, *Internet of Things (IoT) — Reference Architecture*

[18] ISO/IEC 30145 (all parts), *Information technology — Smart City ICT reference framework*

[19] ISO/IEC 30182:2017, *Smart city concept model — Guidance for establishing a model for data interoperability*

[20] ISO 37156, *Smart community infrastructures — Guidelines on data exchange and sharing for smart community infrastructures*

[21] ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

[22] ISO/IEC TS 38501:2015, *Information technology — Governance of IT — Implementation guide*

[23] ISO/IEC TR 38502:2017, *Information technology — Governance of IT — Framework and model*

[24] ISO/IEC 38505 (all parts), *Information technology — Governance of IT — Governance of data*

[25] BSI PAS 183:2017, *Smart cities — Guide to establishing a decision-making framework for sharing data and information services*

[26] ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

[27] The STRIDE threat model[4], https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[28] LINDDUN privacy threat analysis methodology, https://www.linddun.org/

[29] ZANELLA A., BUI N., CASTELLANI A., VANGELISTA L., ZORZI M. IEEE Internet of Things for Smart Cities. IEEE Internet of things journal. Vol.1, N°1, February 2014. https://ieeexplore.ieee.org/document/6740844/

[30] SYSTEMS I.T. (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. ETSI TS 102 637-2 V1.2.1 (2011-03), https://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf

[31] SYSTEMS I.T. (ITS); Security; Pre-standardization study on pseudonym change management ETSI TR 103 415 V1.1.1 (2018-04), https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf

[32] ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS (OASIS). *Privacy Management Reference Model and Methodology (PMRM),* Version 1.0. July 2013, updated May 2016. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

[2] The page states the following: "This documentation is archived and is not being maintained".

[33] Full prototype of cross-sectorial vehicle data services. AutoMat H2020 projects deliverable D5.3. January 2018. https://www.automat-project.eu/sites/default/files/automat/public/content-files/articles/AutoMat%20D5%203_Full%20Prototype%20of%20Cross-Sectorial%20Vehicle%20Data%20Services_final.pdf

Informasi pendukung terkait perumus standar

[1] Komtek perumus SNI
Komite Teknis 35-04 Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi

[2] Susunan keanggotaan Komtek perumus SNI
Ketua : Soetedjo Joewono
Sekretaris : Didik Utomo
Anggota : 1. Bety Hayat Susanti
2. Bisyron Wahyudi
3. Chandra Yulistia
4. Pedro Libratu Putu Wirya
5. Pratama Dahlian Persadha
6. Sari Agustini Hafman
7. Sarwono Sutikno
8. Satriyo Wibowo
9. Sugi Guritman
10. Wisnoe Prasetyo Pribadi
11. Zaenal Arifin

[3] Konseptor rancangan SNI
Gugus Kerja 5 – Komtek 35-04:
Ketua : Satriyo Wibowo
Wakil Ketua : Wisnoe Prasetyo Pribadi
Sekretaris : Ratih Mumpuni Arti
Anggota : 1. Mika Isaac Kriyasa
2. Andri Pancoro
3. Rachmad Erwanto
4. Eka Rahayu Melani Wulandari
5. Arini Muhafidzah

[4] Sekretariat pengelola Komtek perumus SNI
Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara (BSSN)