INSO

17643

1st. Edition

2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران

۱۷۶۴۳

چاپ اول

۱۳۹۱

فن‌آوری اطلاعات- فنون امنیتی- چارچوب کاری کاری حریم خصوصی

Information technology - Security techniques - Privacy framework

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فن‌آوری اطلاعات- فنون امنیتی- چارچوب کاری کاری حریم خصوصی»

رئیس:	**سمت و/ یا نمایندگی**
صفایی، سپیده (کارشناس کامپیوتر)	کارشناس نرم‌افزار شرکت داده‌کاوان امن‌پرداز
دبیر:	
منافی، علیرضا (کارشناس ارشد کامپیوتر)	مدیر عامل شرکت امن‌افزار گستر شریف
اعضاء: (اسامی‌به ترتیب حروف الفبا)	
اخوان نیاکی، سید انوشیروان (کارشناس ارشد مدیریت IT)	مشاور مدیر عامل و مدیر مرکز مدیریت دانش و داده کاوی شرکت ایزایران
علی محمد ملایری، عصمت (کارشناس ارشد نرم‌افزار)	مدرس دانشگاه آزاد ملایر
مروجی، سجاد (کارشناس ارشد رایانه)	مدرس دانشگاه
مهدوی، سید علیرضا (کارشناس ارشد مدیریت IT)	مشاور شرکت داده‌پردازان آبشار
ولی،ناصر (کارشناس ارشد نرم‌افزار)	کارشناس IT کمیته امداد امام خمینی

فهرست مندرجات

پیش‌گفتار

استاندارد«فن‌آوری اطلاعات- فنون امنیتی- چارچوب کاری حریم خصوصی» که پیش نویس آن درکمیسیون‌های مربوط توسط شرکت امن افزار شریف تهیه و تدوین شده و در دویست و شصت و هفتمین اجلاسیه کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۱/۱۲/۸ مورد تصویب قرار گرفته است ، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ هم‌گامی‌و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 29100:2011(E)Information technology-Security techniques-Privacy framework

مقدمه

این استاندارد ملی چارچوب کاری کاری سطح بالایی را برای حفاظت اطلاعات شناسایی شخصی (PII) [1]در سامانه‌های فن‌آوری اطلاعات و ارتباطات (ICT) [2]ارائه می‌دهد. این استاندارد دارای ماهیت کلی است و جنبه‌های سازمانی، فنی و رویه ای را در یک چارچوب کاری کاری کلی حریم خصوصی قرار می‌دهد.

چارچوب کاری کاری حریم خصوصی، جهت کمک به سازمان‌هایی که الزامات حفظ حریم خصوصی مرتبط با PII خود را در یک محیط ICT به وسیله موارد زیر تعریف می‌کنند، در نظر گرفته شده است:

- مشخص کردن واژگان متداول حریم خصوصی؛
- تعریف فعالان و نقش آنها در پردازش PII؛
- شرح الزامات حفاظت حریم خصوصی؛ و
- مراجعه به اصول حریم خصوصی شناخته شده.

در برخی از حوزه‌های قضایی، عطف این استاندارد ملی به الزامات حفاظت حریم خصوصی ممکن است مکملی برای الزامات قانونی برای حفظ PII شناخته شود. به علت افزایش روز افزون تعداد فن‌آوری‌های اطلاعاتی و ارتباطاتی که PII را پردازش می‌کنند، داشتن استانداردهای ملی امنیت اطلاعات که درک عمومی را درمورد حفاظت PII ارائه می‌کند از اهمیت برخوردار است. این استاندارد ملی با افزودن تمرکزی مرتبط با پردازش PII جهت افزایش استانداردهای امنیتی موجود درنظر گرفته شده است.

استفاده تجاری و ارزش PII درحال افزایش، به اشتراک گذاری PII در میان حوزه‌های قانونی و پیچیدگی درحال افزایش سامانه‌های ICT، می‌تواند برای سازمان‌ها تضمین حریم خصوصی و دستیابی به مطابقت با قوانین گوناگون قابل اجرا را دشوار کند. ذی‌نفعان حریم خصوصی می‌توانند با اداره صحیح مسائل حریم خصوصی مانع عدم اطمینان و سوءظن ایجاد شده شوند و از موارد سوء استفاده از PII جلوگیری کنند.

استفاده از این استاندارد ملی:

- به طراحی، اجرا، عملیات و حفاظت از سامانه‌های ICT که PII را اداره و محافظت می‌کنند کمک خواهد کرد؛
- راه حل‌های نوآورانه را جهت امکان پذیر کردن محافظت از PII در سامانه‌های ICT، تحریک خواهد کرد؛ و
- برنامه‌های حریم خصوصی سازمان‌ها را از طریق استفاده از تجربیات موفق بهبود خواهد بخشید.

چارچوب کاری کاری ارائه شده در این استاندارد ملی می‌تواند به عنوان مبنایی برای ابتکارات استانداردسازی حریم خصوصی، مانند موارد زیر عمل‌کرد داشته باشد:

- ساختار یک مرجع فنی؛
- اجرا و استفاده از فن‌آوری‌های خاص حریم خصوصی و مدیریت کلی حریم خصوصی؛
- کنترل حریم خصوصی برای پردازش‌های داده ای که مدیریت و تامین آن واگذار شده است؛

1- Personally Identifiable Information

2- information and communication technology

- ارزیابی‌های خطر حریم خصوصی؛ یا
- مشخصات خاص مهندسی.

برخی از حوزه‌ها ممکن است الزام مطابقت با یک یا چند سند ارجاع داده شده در ISO/IEC JTC 1/SC 27 WG 5 سند ثابت ۲ (WG 5 SD2)- منابع اسناد رسمی‌حریم خصوصی {۳} یا با دیگر مقررات و قوانین قابل اجرا را ایجاد کنند، اما این استاندارد ملی به عنوان یک خط‌مشی الگوی یک‌پارچه و یا یک چارچوب کاری کاری قانون‌گذار در نظر گرفته نشده است.

فن‌آوری اطلاعات- فنون امنیتی- چارچوب کاری کاری حریم خصوصی

۱ دامنه کاربرد

هدف از تدوین این استاندارد تعیین یک چارچوب کاری حریم خصوصی است که:

- واژگان متداول حریم خصوصی را مشخص می‌کند؛
- فعالان و نقش آنها در پردازش PII را تعریف می‌کند؛
- ملاحظات حفاظت حریم خصوصی را شرح می‌دهد؛ و
- منابع اصول حریم خصوصی شناخته شده را ارائه می‌دهد.

این استاندارد ملی برای افراد عادی و سازمان‌های دست اندرکار در مشخص کردن، تهیه، ساختار، طراحی، توسعه، آزمایش، حفاظت، مدیریت و عملیات سامانه‌ها و یا خدمت‌های فن‌آوری اطلاعات و ارتباطات که کنترل حریم خصوصی در آنها برای پردازش PII مورد نیاز است قابل اجرا است.

۲ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌رود:

یادآوری -به منظور تسهیل استفاده از خانواده ISO/IEC 27000 استانداردهای ملی در زمینه خاص حریم خصوصی و جهت یک‌پارچگی مفاهیم حریم خصوصی در زمینه ISO/IEC 27000، جدول پیوست A مفاهیم ISO/IEC 27000 را که با مفاهیم ISO/IEC 29100 مورد استفاده در این استاندارد ملی مطابقت دارد، ارائه می‌دهد.

۱-۲

گمنامی

خصوصیت اطلاعاتی که اجازه نمی‌دهد یک اطلاعات اصلی قابل شناسایی اشخاص به صورت مستقیم یا غیر مستقیم شناسایی شود

۲-۲

گمنام سازی

فرآیندی که در آن اطلاعات قابل شناسایی اشخاص (PII) به صورت برگشت ناپذیری به شکلی تغییر می‌کند که یک PIIی اصلی دیگر نتواند به صورت مستقیم یا غیر مستقیم، به وسیله کنترل کننده PII به تنهایی و یا با هم‌کاری بخش دیگر شناسایی شود.

۳-۲

داده گمنام سازی شده

داده ای که به عنوان خروجی یک فرآیند گمنام سازی اطلاعات قابل شناسایی اشخاص تولید شده است.

۴-۲

موافقت

توافق‌نامه خاص و آگاهانه اطلاعات اصلی قابل شناسایی اشخاص PII که آزادانه جهت پردازش PIIی آنها ارائه می‌شود

۵-۲

قابلیت شناسایی

موقعیتی که به شناسایی شدن اطلاعات اصلی قابل شناسایی اشخاص (PII) به صورت مستقیم یا غیر مستقیم برمبنای مجموعه ای معین از PII منجر می‌شود

۶-۲

شناسایی

برقراری پیوند میان یک اطلاعات اصلی قابل شناسایی اشخاص (PII) و PII یا مجموعه ای از PII

۷-۲

هویت

مجموعه ای از ویژگی‌ها که شناسایی اطلاعات اصلی قابل شناسایی اشخاص را امکان پذیر می‌کند

۸-۲

انتخاب کردن در

فرآیند یا نوع خطمشی‌ای که به موجب آن اطلاعات اصلی قابل شناسایی اشخاص (PII) مستلزم اقدامی‌جهت بیان روشن، موافقت پیشین برای PII جهت پردازش برای یک هدف مشخص است

یادآوری- یک اصطلاح متفاوت که اغلب با اصل ‘موافقت و انتخاب’ حریم خصوصی مورد استفاده قرار می‌گیرد "صرف نظر کردن" است. این اصطلاح یک فرآیند یا نوع خطمشی که به موجب آن اطلاعات اصلی قابل شناسایی اشخاص (PII) مستلزم اقدامی‌جداگانه به منظور ممانعت یا صرفنظر کردن از موافقت، یا مخالفت با یک نوع خاص از پردازش است را توصیف می‌کند. استفاده از یک خطمشی صرف نظر، مسلم می‌داند که کنترل کننده PII دارای حق پردازش PII به روش در نظر گرفته شده است. این حق می‌تواند به وسیله برخی از اقدامات اصل PII متفاوت از موافقت متضمن شود (برای مثال، سفارش دادن در یک فروشگاه برخط).

۹-۲

اطلاعات قابل شناسایی اشخاص

PII

هر اطلاعاتی که (الف) می‌تواند جهت شناسایی اصل PII که چنین اطلاعاتی به آنها مرتبط است مورد استفاده قرار گیرد، یا (ب) مستقیم و یا غیر مستقیم به یک اصل PII مرتبط است و یا ممکن است مرتبط باشد.

یادآوری- جهت تعیین این‌که آیا یک اصل PII قابل شناسایی است و یا خیر، حساب باید از تمام امکاناتی که می‌توانند به صورت معقول به وسیله ذی‌نفع حریم خصوصی که دارنده داده است، یا به وسیله هر گروه دیگر جهت شناسایی آن فرد حقیقی استفاده کند.

۲-۱۰

کنترل کننده PII

ذی‌نفع حریم خصوصی (یا ذی‌نفع‌های حریم خصوصی) که اهداف و ابزارهایی را برای پردازش اطلاعات قابل شناسایی اشخاص (PII) متفاوت از افراد حقیقی که از داده برای اهداف شخصی استفاده می‌کنند تعیین می‌کند

یادآوری- یک کنترل کننده PII برخی مواقع کنترل کننده‌های دیگر را (برای مثال پردازنده‌های PII) جهت پردازش PII به جای آن درحالی که مسئولیت پردازش با کنترل کننده PII باقی می‌ماند را تعلیم می‌دهد.

۲-۱۱

PIIی اصلی

فرد عادی که اطلاعات قابل شناسایی اشخاص (PII) به آن مربوط می‌شود

یادآوری- بسته به حوزه و قانون‌گذاری حریم خصوصی و حفاظت از داده خاص، مترادف "موضوع داده" نیز می‌تواند به جای اصطلاح "PIIی اصلی مورد استفاده قرار گیرد.

۲-۱۲

پردازنده PII

ذی‌نفع حریم خصوصی که اطلاعات قابل شناسایی اشخاص (PII) را به جای و مطابق با ساختارهای یک کنترل کننده PII پردازش می‌کند

۲-۱۳

نقض حریم خصوصی

موقعیتی که در آن اطلاعات قابل شناسایی اشخاص در تخطی از یک یا چند الزام حفاظت از حریم خصوصی مرتبط، پردازش می‌شود

۲-۱۴

کنترل‌های حریم خصوصی

اقداماتی که خطرات حریم خصوصی را با کاهش احتمال آنها یا عواقب آنها تهدید می‌کند

یادآوری ۱-کنترل‌های حریم خصوصی شامل اقدامات سازمانی، فنی و فیزیکی، برای مثال، خطمشی‌ها، رویه‌ها، رهنمودها، قراردادهای قانونی، عمل‌کردهای مدیریتی یا ساختارهای سازمانی.

یادآوری ۲-کنترل همچنین به عنوان مترادف برای حفاظت یا پیشگیری مورد استفاده قرار می‌گیرد.

۲-۱۵

فن‌آوری پیشرفته حریم خصوصی[1]

کنترل حریم خصوصی، شامل اقدامات، محصولات یا خدمات فن‌آوری اطلاعات و ارتباطات (ICT)، که با حذف یا کاهش اطلاعات قابل شناسایی شخصی (PII) یا با ممانعت از پردازش غیرضروری و یا نامطلوب PII، بدون از بین رفتن عمل‌کرد سامانه ICT از حریم خصوصی محافظت می‌کند

یادآوری ۱- مثال‌های PETها شامل ابزارهای گمنام سازی و نام مستعارسازی می‌شود که PII را حذف می‌کند، کاهش می‌دهد، پنهان می‌کند یا ناشناس می‌کند یا این‌که از پردازش غیر ضروری، غیر مجاز و یا غیرمطلوب PII جلوگیری می‌کند، اما به این موارد محدود نمی‌شود.

یادآوری ۲-پنهان کردن فرآیند نامشخص کردن عناصر PII است.

۲-۱۶

خط‌مشی حریم خصوصی

هدف و جهت کلی، قوائد و تعهدی که به صورت رسمی‌از سوی کنترل کننده اطلاعات قابل شناسایی شخصی (PII) مرتبط با پردازش PII در یک مجموعه خاص بیان می‌شود

۲-۱۷

اولویت‌های حریم خصوصی

انتخاب‌های خاصی که به وسیله اطلاعات اصلی قابل شناسایی شخصی (PII) در مورد چگونگی این‌که PIIی آنها باید برای یک هدف ویژه پردازش شود، صورت می‌گیرد

۲-۱۸

قواعد کلی حریم خصوصی

مجموعه ای از ارزش‌های به اشتراک گذاشته شده که بر حفاظت حریم خصوصی از اطلاعات قابل شناسایی شخصی (PII) که در سامانه‌های فن‌آوری اطلاعات و ارتباطات پردازش می‌شوند، نظارت دارد

۲-۱۹

مخاطره حریم خصوصی

تاثیر عدم اطمینان بر حریم خصوصی

یادآوری ۱- مخاطره به صورت « تاثیر عدم اطمینان بر اهداف» در راهنمای ISO 73 و ISO 31000 تعریف شده است.

یادآوری ۲- عدم اطمینان، حتی به صورت جزئی، حالتی از نقص اطلاعات مرتبط با درک یا شناخت یک رویداد، نتایج یا احتمال آن است.

1- Privacy Enhancing Technology(PET)

۲۰-۲

ارزیابی مخاطره حریم خصوصی

فرآیند کلی شناسایی مخاطره، تحلیل مخاطره و سنجش مخاطره با توجه به پردازش اطلاعات قابل شناسایی شخصی (PII) می‌باشد.

یادآوری- این فرآیند به عنوان ارزیابی اثر حریم خصوصی نیز شناخته می‌شود.

۲۱-۲

الزامات حفاظت حریم خصوصی

مجموعه ای از الزاماتی که یک سازمان باید هنگام پردازش اطلاعات قابل شناسایی اشخاص (PII) با توجه به حفظ حریم خصوصی PII مورد توجه قرار دهد.

۲۲-۲

ذی‌نفع حریم خصوصی

فرد حقیقی یا حقوقی، مرجع عمومی، آژانس یا گروهی دیگر که می‌تواند تاثیر گذار باشد، تاثیر بپذیرد یا خود را به وسیله یک تصمیم یا فعالیت مرتبط با پردازش اطلاعات قابل شناسایی اشخاص (PII) تاثیر پذیرفته شده درک کنند.

۲۳-۲

پردازش PII

عملیات یا مجموعه ای از عملیات‌هایی که برروی اطلاعات قابل شناسایی اشخاص (PII) صورت می‌گیرد

یادآوری- مثال‌هایی از عملیات‌های پردازش PII شامل، جمع آوری، ذخیره سازی، تغییر، بازیابی، مشاوره، افشاء، گمنام سازی، نام مستعار سازی[1]، انتشار یا درغیر این صورت در دسترس قرار دادن، حذف یا تخریب PII می‌شود، اما به این موارد محدود نمی‌شود.

۲۴-۲

نام مستعار سازی

فرآیند به کار گرفته شده برای اطلاعات قابل شناسایی اشخاص (PII) که اطلاعات شناسایی را با یک نام مستعار جای‌گزین می‌کند

یادآوری ۱- نام مستعار سازی می‌تواند با به وسیله خود اصل PII یا به وسیله کنترل کننده‌های PII اجرا شود. نام مستعار سازی می‌تواند به وسیله اصل PII جهت استفاده مداوم از یک منبع یا خدمت بدون افشاء هویت آنها برای این منبع یا خدمت (یا میان خدمت‌ها) مورد استفاده قرار گیرد، درحالی که همچنان برای آن مصرف، قابل شمارش نگه داشته می‌شود.

یادآوری ۲- نام مستعار سازی احتمال اینکه ممکن است (یک مجموعه محدود) از ذی‌نفع‌های حریم خصوصی به غیر از کنترل کننده PIIی داده نام مستعار سازی شده، موجود باشد که قادر هستند هویت اصلی PII را مبتنی بر نام‌های مستعار و داده مرتبط به آن تعیین کند، نفی نمی‌کند.

1- pseudonymization

۲-۲۵

استفاده ثانویه

پردازش اطلاعات قابل شناسایی اشخاص (PII) در شرایطی که با شرایط اولیه متفاوت است

یادآوری- شرایطی که با شرایط اولیه متفاوت است می‌تواند برای مثال شامل یک هدف جدید برای پردازش PII، یک گیرنده جدید از PII و غیره باشد.

۲-۲۶

PII حساس

دسته ای از اطلاعات قابل شناسایی اشخاص (PII) که یا دارای ماهیت حساس هستند، مانند آنهایی که به بنیادی ترین حوزه اصل PII مرتبط می‌شوند و یا ممکن است دارای یک اثر قابل ملاحظه بر اصل PII باشند

یادآوری- دربرخی از حوزه‌ها یا در زمینه‌های خاص، PII حساس با توجه به ماهیت PII تعریف شده است و می‌تواند متشکل از PII نمایش دهنده منشاء نژادی، عقاید سیاسی یا دینی یا دیگر اعتقادات، داده‌های سلامتی شخصی، زندگی جنسی یا محکومیت‌های جنایی، همچنین PII دیگر که می‌تواند به عنوان حساس تعریف شود باشد.

۲-۲۷

شخص ثالث

ذی‌نفع حریم خصوصی غیر از اطلاعات اصلی قابل شناسایی اشخاص (PII)، کنترل کننده PII و پردازنده PII و افراد حقیقی که به آنها اجازه پردازش داده تحت اختیار مستقیم کنترل کننده PII یا پردازنده PII داده شده است.

۳ نمادها و کوته‌نوشت‌ها

کوته‌نوشت‌های زیر در این استاندارد متداول هستند.

ICT	Information and Communication Technology	فن آوری اطلاعات و ارتباطات
PET	Privacy Enhancing Technology	فن آوری افزایش حریم خصوصی
PII	Personally Identifiable Information	اطلاعات قابل شناسایی اشخاص

۴ عناصر پایه چارچوب کاری حریم خصوصی

۴-۱ مروری بر چارچوب کاری حریم خصوصی

مولفه‌های پیش رو به حریم خصوصی و پردازش PII در سامانه‌های ICT مرتبط است و چارچوب کاری کاری حریم خصوصی شرح داده شده در این استاندارد ملی را تامین می‌کند:

جهت ایجاد این چارچوب کاری حریم خصوصی، مفاهیم، تعاریف و توصیه‌هایی از دیگر منابع رسمی‌مد نظر قرار داده شده است. این منابع می‌تواند در ISO/IEC JTC 1/SC 27 WG5 سند ثابت ۲ (WG 5 SD2) منابع اسناد رسمی‌حریم خصوصی [3] یافت شوند.

۴-۲ عوامل و نقش‌ها

در جهت اهداف این استاندارد، شناسایی عوامل دخیل در پردازش PII از اهمیت برخوردار است. ۴ نوع از این عوامل وجود دارند که می‌توانند در پردازش PII دخیل باشند: PIIاصلی، کنترل کننده‌های PII، پردازنده‌های PII و اشخاص ثالث.

۴-۲-۱اصول PII

اصول PII، PII خود را برای پردازش شدن به کنترل کننده‌های PII و پردازنده‌های PII ارائه می‌دهند، درغیر این صورت زمانی که از سوی قانون قابل اجرا ارائه نشود، موافقت خود را اعلام و اولویت‌های حریم خصوصی خود را برای چگونگی این‌که PII آنها باید پردازش شود تعیین می‌کنند. اصول PII می‌توانند برای مثال شامل کارمندی باشد که در فهرست سامانه منابع انسانی یک شرکت قرار دارد، مصرف کننده ای که در یک گزارش اعتباری ذکر شده است و بیماری که در کارت سلامت الکترونیک قرار داده شده است. همیشه این‌که فرد حقیقی مرتبط مستقیما براساس نام به منظور در نظر گرفته شدن به عنوان یک اصل PII شناسایی شود، ضروری نیست. درصورتی که یک فرد حقیقی که PII به وی مرتبط می‌شود بتواند به صورت غیر مستقیم شناسایی شود (برای مثال، از طریق یک شناسه حساب کاربری، شماره امنیت اجتماعی یا حتی ترکیبی از ویژگی‌های در دسترس)، وی به عنوان اصل PII برای آن مجموعه PII در نظر گرفته می‌شود.

۴-۲-۲ کنترل کننده‌های PII

یک کنترل کننده PII تعیین می‌کند که چرا (هدف) و چگونه (ابزار) پردازش PII رخ می‌دهد. کنترل کننده PII باید تبعیت از اصول حریم خصوصی را در این چارچوب کاری طی پردازش PII تحت کنترل آن (برای مثال با به‌کارگیری کنترل‌های لازم برای حریم خصوصی) تضمین کند. ممکن است بیش از یک کنترل کننده PII برای مجموعه PII مشابه یا مجموعه از عملیات‌های انجام شده برروی PII (برای اهداف قانونی مختلف یا مشابه) وجود داشته باشد. در این زمینه کنترل کننده‌های PII متفاوت باید با یکدیگر کارکنند و ترتیب لازم را جهت تضمین این‌که اصول حریم خصوصی طی پردازش PII از آنها پیروی می‌کنند را انجام دهند. یک کنترل کننده PII می‌تواند در مورد این‌که تمام و یا بخشی از عملیات‌های پردازش به وسیله یک ذی‌نفع متفاوت حریم خصوصی به جای آن، صورت گیرد نیز تصمیم گیری کند. کنترل کننده‌های PII باید با دقت ارزیابی کنند که در هر صورت PII حساس را پردازش می‌کنند و کنترل‌های امنیتی و حریم خصوصی مناسب و معقول را مبتنی بر الزاماتی که در حوزه مربوط بیان می‌شود و همچنین هر تاثیر منفی بالقوه برای اصل PII که طی یک ارزیابی خطر حریم خصوصی شناسایی می‌شود اجرا می‌شود.

۴-۲-۳ پردازنده‌های PII

یک پردازنده PII پردازش PII را به جای یک کنترل کننده PII اجرا می‌کند، به جای یا مطابق با ساختارهای کنترل کننده PII عمل می‌کند، الزامات حریم خصوصی تصریح شده را مشاهده می‌کند و کنترل‌های حریم خصوصی مشابه را اجرا می‌کند. در برخی حوزه‌ها، پردازنده PII به وسیله یک قرار داد قانونی محدود می‌شود.

۴-۲-۴ اشخاص ثالث

یک شخص ثالث می‌تواند PII را از یک کنترل کننده PII یا یک پردازنده PII دریافت کند. یک شخص ثالث PII را به جای کنترل کننده PII پردازش نمی‌کند. به صورت کلی، شخص ثالث، با اختیارات خود، زمانی که PII مورد بحث را دریافت کند، یک کنترل کننده PII خواهد شد.

۴-۳ تعاملات

عامل‌های شناسایی شده در بند قبل می‌توانند با یکدیگر به روش‌های متنوعی تعامل داشته باشند. با در نظر گرفتن جریان‌های احتمالی PII میان اصول PII، کنترل کننده PII و پردازنده PII، سناریوهای زیر می‌توانند شناسایی شوند:

الف- اصل PII، PII را به یک کنترل کننده PII ارائه می‌دهد (برای مثال، هنگام ثبت نام برای یک خدمت ارائه شده از سوی کنترل کننده PII)؛

ب- کنترل کننده PII، PII را به یک پردازنده PII ارائه می‌دهد که آن PII را به جای کنترل کننده PII پردازش می‌کند (برای مثال، به عنوان بخشی از یک توافق نامه برای به کار گیری عاملی دیگر جهت انجام خدمات)؛

پ- اصل PII، PII را به یک پردازنده PII ارائه می‌دهد که آن PII را به جای کنترل کننده PII پردازش می‌کند؛

ت- کنترل کننده PII،PII را برای اصل PII فراهم می‌کند که به اصل PII مرتبط است (برای مثال، متعاقب درخواست مطرح شده به وسیله اصل PII)؛

ث- پردازنده PII، PII را به اصل PII ارائه می‌دهد (برای مثال، به صورتی که به وسیله کنترل کننده PII هدایت می‌شود)؛ و

ج- پردازنده PII، PII را به کنترل کننده PII ارائه می‌دهد (برای مثال، پس از اجرای خدمت‌هایی که برای آنها تعیین شده است).

نقش اصل PII، کنترل کننده PII، پردازنده PII و شخص ثالث در این موارد در جدول ۱ نشان داده شده اند.

تمایز میان پردازنده‌های PII و اشخاص ثالث مورد نیاز است چراکه کنترل قانونی PII زمانی که به پردازنده PII فرستاده شود بر عهده کنترل کننده اصل PII باقی خواهد ماند، درحالی که یک شخص ثالث می‌تواند، با اختیارات خود زمانی که PII مورد بحث را دریافت می‌کند، به یک کنترل کننده PII تبدیل شود. برای مثال در جایی که یک شخص ثالث تصمیم به انتقال PII دریافت شده از یک کنترل کننده PII به یک بخش دیگر می‌گیرد، به عنوان کنترل کننده PII، با اختیارات خود عمل خواهد کرد و از این رو دیگر به عنوان شخص ثالث درنظر گرفته نمی‌شود.

با درنظر گرفتن جریان‌های احتمالی میان کنترل کننده‌های PII و پردازنده‌های PII در یک سو و اشخاص ثالث از سوی دیگر، موارد زیر می‌توانند شناسایی شوند:

چ- کنترل کننده PII، PII را به شخص ثالث ارائه می‌دهد (برای مثال در زمینه توافق نامه تجاری)؛ و

ح- پردازنده PII، PII را به شخص ثالث ارائه می‌دهد (برای مثال، به صورتی که توسط کنترل کننده PII هدایت می‌شود).

نقش‌های کنترل کننده PII و شخص ثالث در این موارد نیز در جدول ۱ نشان داده شده اند.

جدول ۱- جریان‌های احتمالی PII میان اصل PII، کنترل کننده PII، پردازنده PII و یک شخص ثالث و نقش‌های آنها

	اصل PII	کنترل کننده PII	پردازنده PII	شخص ثالث
سناریو الف	ارائه دهنده PII	گیرنده PII	-	-
سناریو ب	-	ارائه دهنده PII	گیرنده PII	-
سناریو پ	ارائه دهنده PII	-	گیرنده PII	-
سناریو ت	گیرنده PII	ارائه دهنده PII	-	-
سناریو ث	گیرنده PII	-	ارائه دهنده PII	-
سناریو ج	-	گیرنده PII	ارائه دهنده PII	-
سناریو چ	-	ارائه دهنده PII	-	گیرنده PII
سناریو ح	-	-	ارائه دهنده PII	گیرنده PII

۴-۴ تشخیص PII

برای تعیین این‌که آیا یک فرد حقیقی باید قابل شناسایی درنظر گرفته شود و یا خیر، چندین عامل باید مدنظر قرار گیرد. به طور خاص، حساب کاربری باید دربرگیرنده تمام ابزارهایی که می‌توانند به صورت منطقی به وسیله ذی‌نفع حریم خصوصی که داده را در اختیار دارد، یا به وسیله هر بخش دیگر جهت شناسایی آن شخص حقیقی مورد استفاده قرار گیرد، باشد. سامانه‌های ICT باید از سازوکارهایی که اصل PII را از چنین PIIی آگاه خواهد کرد و کنترل‌های مناسب را در مورد به اشتراک گذاری آن اطلاعات برای شخص حقیقی فراهم می‌کند، پشتیبانی کند. زیربندهای زیر توضیح افزوده ای را در مورد چگونگی تعیین این‌که آیا یک اصل PII باید قابل شناسایی درنظر گرفته شود و یا خیر ارائه می‌دهند.

۴-۴-۱ شناساگرها

در موارد معین، قابلیت شناسایی اصل PII ممکن است بسیار روشن باشد (برای مثال زمانی که اطلاعات دربرگیرنده یک شناساگر است و یا به یک شناساگر وابسته است که جهت عطف و یا ارتباط با اصل PII مورد استفاده قرار می‌گیرد). اطلاعات می‌توانند حداقل در موارد زیر PII در نظر گرفته شوند:

- درصورتی که دربرگیرنده یا وابسته به یک شناساگر باشد که به یک فرد حقیقی اشاره دارد (برای مثال، یک شماره امنیت اجتماعی)؛
- درصورتی که دربرگیرنده و یا وابسته به یک شناساگر باشد که می‌تواند به فرد حقیقی مرتبط باشد (برای مثال، یک شماره گذرنامه، یک شماره حساب)؛
- درصورتی که دربرگیرنده و یا وابسته به یک شناساگر باشد که می‌تواند جهت برقراری ارتباط با یک فرد حقیقی شناسایی شده مورد استفاده قرار گیرد (برای مثال، موقعیت جغرافیایی دقیق، شماره تلفن)؛ یا
- درصورتی که دربرگیرنده یک مرجع باشد که داده را به هر یک از شناساگرهای بالا پیوند می‌دهد.

۴-۴-۲ دیگر مشخصات متمایز

اطلاعات لزوما نباید به منظور این‌که PII درنظر گرفته شوند با یک شناساگر مرتبط باشند. اطلاعات نیز درصورتی که دربرگیرنده یا وابسته به یک مشخصه باشند که یک فرد حقیقی را از دیگر افراد حقیقی متمایز کند، PII درنظر گرفته خواهند شد (برای مثال، داده زیست سنجی).

هر ویژگی که ارزشی را به خود اختصاص می‌دهند که به صورت منحصر به فرد یک اصل PII را شناسایی می‌کند باید به عنوان یک خصیصه متمایز کننده درنظر گرفته شود. توجه به این نکته که آیا یک خصیصه معین، یک فرد حقیقی را از دیگر افراد حقیقی متمایز می‌کند و یا خیر، می‌تواند بسته به زمینه استفاده تغییر کند. برای مثال، درحالی که نام خانوادگی یک فرد حقیقی ممکن است برای شناسایی آن فرد حقیقی در یک مقیاس کلی کافی نباشد، اغلب برای تشخیص آن فرد حقیقی در مقیاس یک شرکت کافی خواهد بود.

به علاوه موقعیت‌هایی نیز می‌تواند وجود داشته باشد که در آنها یک فرد حقیقی، حتی درصورتی که هیچ ویژگی منفردی وجود نداشته باشد که به صورت منحصر به فرد وی را شناسایی کند، قابل شناسایی است. این موردی است که در آن ترکیبی از چندین ویژگی با یکدیگر این فرد حقیقی را از دیگر افراد حقیقی متمایز می‌کند. اگر یک فرد حقیقی بر مبنای ترکیب ویژگی‌ها قابل شناسایی باشد و یا نباشد نیز می‌تواند به دامنه خاص وابسته باشد. برای مثال، ترکیبی از ویژگی‌ها "مونث"، "۴۵" و "وکیل" می‌تواند برای شناسایی یک فرد حقیقی در یک شرکت مشخص کافی باشد، اما برای شناسایی آن فرد حقیقی در خارج از آن شرکت ناکافی خواهد بود.

جدول ۲ مثال‌هایی از ویژگی‌هایی که می‌توانند بسته به دامنه PII باشند را ارائه می‌دهد. این مثال‌ها اطلاعاتی هستند.

جدول ۲- مثال ویژگی‌هایی که می‌توانند جهت شناسایی افراد حقیقی مورد استفاده قرار گیرند

مثال‌ها
سن یا نیازهای خاص افراد عادی آسیب پذیر
ادعاهای مربوط به ارتکاب جرم
هر نوع اطلاعات جمع آوری شده طی خدمات بهداشتی
شماره حساب بانکی یا کارت اعتباری
شناسه زیست سنجی
صورت حساب‌های کارت اعتباری
محکومیت‌های جنایی یا جرایم ارتکابی
گزارش‌های بررسی جرم
شماره مشتری
تاریخ تولد
اطلاعات تشخیصی سلامت
ناتوانی‌ها
صورت حساب‌های پزشک
پرونده‌های منابع انسانی و حقوق کارکنان
مشخصات مالی
جنسیت
وضعیت GPS
خطوط سیر GPS
آدرس منزل
آدرس IP
محل بدست آمده از سامانه‌های مخابراتی
سابقه پزشکی
نام
شناسه‌های ملی (برای مثال شماره گذرنامه)
آدرس ایمیل شخصی
شماره‌های شناسایی شخصی (PIN) یا رمزعبورها
علایق شخصی بدست آمده از پیگیری استفاده از وب سایت‌های اینترنتی
فرم شخصی یا رفتاری
شماره تلفن شخصی
عکس یا تصویر ویدئویی قابل شناسایی برای یک فرد حقیقی
اولویت‌های محصول و خدمت
منشاء نژادی یا قومی
عقاید فلسفی یا دینی
گرایش جنسی
عضویت اتحادیه تجاری
صورت حساب سودمند

۴-۴-۳ اطلاعاتی که به یک اصل PII مرتبط است یا ممکن است مرتبط باشد

درصورتی که اطلاعات مورد بحث، یک اصل PII را شناسایی نکند، باید تعیین کند که آیا اطلاعات به هویت یک فرد حقیقی مرتبط است یا می‌تواند مرتبط باشد.

زمانی که رابطه ای با یک فرد حقیقی قابل شناسایی برقرار شود، باید تصمیم گیری شود که آیا اطلاعات چیزی درمورد این فرد حقیقی می‌گوید و یا خیر، برای مثال درصورتی که به خصوصیات یا رفتار وی اشاره کند. مثال‌ها شامل سوابق پزشکی، فرم‌های مالی یا علایق شخصی بدست آمده از پیگیری استفاده از وب سایت‌های اینترنتی اشاره کرد. همچنین، بیان ویژگی ساده در مورد یک فرد حقیقی مانند سن یا جنسیت یک فرد حقیقی می‌تواند اطلاعات پیوندی را به عنوان PII توصیف کند. صرف نظر از این‌که اگر رابطه با یک فرد حقیقی قابل شناسایی بتواند برقرار شود، چنین اطلاعاتی نیز باید به عنوان PII تلقی شود.

۴-۴-۴ داده دارای نام مستعار

به منظور محدود کردن توانایی کنترل کننده‌ها و پردازنده‌های PII جهت شناسایی اصل PII، نام‌های مستعار می‌توانند جایگزین اطلاعات هویتی شوند. این جایگزینی معمولا به وسیله ارائه دهنده PII پیش از انتقال PII به دریافت کننده PII، به طور خاص در سناریوهای الف، ب، پ،چ و ح جدول ۱ اجرا می‌شود.

فرآیندهای معین تجاری بر پردازنده‌های تعیین شده ای که جایگزینی را اجرا می‌کنند و جدول تخصیص یا عمل‌کرد را کنترل می‌کنند تکیه دارد. این امر اغلب هرجا که داده حساس باید به وسیله ذی‌نفع‌های حریم خصوصی که آنها را جمع آوری نکرده اند پردازش شوند، صدق می‌کند.

تعویض با فرض موارد زیر نام مستعار سازی درنظر گرفته می‌شود:

الف- ویژگی‌های باقی مانده مرتبط با نام‌های مستعار جهت شناسایی اصل PII که به آنها ارتباط دارد کافی نباشند؛ و

ب- تخصیص نام‌های مستعار به صورتی باشد که نتواند با تلاش‌های منطقی ذی‌نفعهای حریم خصوصی به جای آنهایی که عامل آنها هستند نقض شود.

نام مستعار سازی قابلیت پیوند پذیری را حفظ می‌کند. داده متفاوت وابسته به همان نام مستعار می‌تواند پیوند یابد. هر چه مجموعه داده مرتبط با یک نام مستعار معین بزرگتر باشد، خطر تجاوز به دارایی‌ها (الف) افزایش می‌یابد. به علاوه، هر چه گروه افراد حقیقی که مجموعه ای از داده‌های نام مستعار به آنها مرتبط است، کوچکتر باشد، احتمال این‌که اصل PII قابل شناسایی باشد، بیشتر است. ویژگی‌هایی که به صورت مستقیم در اطلاعات مورد بحث قرار می‌گیرند و ویژگی‌هایی که می‌توانند به آسانی به این اطلاعات مرتبط شوند (برای مثال با استفاده از یک موتور جستجو یا ارجاع متقابل به دیگر پایگاه‌های داده) باید هنگام تعیین این‌که آیا اطلاعات به یک فرد حقیقی قابل شناسایی مرتبط است و یا خیر، مد نظر قرار گیرد.

نام مستعار سازی با گمنام سازی مغایرت دارد. فرآیندهای گمنام سازی نیز مشخصات (الف) و (ب) ذکر شده در قسمت بالا را تکمیل می‌کند، اما قابلیت پیوند پذیری را از بین می‌برد. طی گمنام سازی، اطلاعات هویتی به وسیله نام‌های مستعاری که برای جدول یا عمل تخصیص از بین رفته است، یا پاک می‌شود و یا جایگزین می‌شود. از این رو داده گمنام سازی شده دیگر PII نیست.

۴-۴-۵ فراداده

PII می‌تواند در یک سامانه ICT به صورتی ذخیره شود که برای کاربر سامانه به آسانی مشهود نباشد (یعنی برای اصل PII). مثال‌هایی در این زمینه شامل نام اصل PII ذخیره شده به عنوان فراداده در مشخصات یک سند و توضیحات یا تغییرات پیگیری شده ذخیره شده در یک سند پردازش کلمه است. درصورتی که اصل PII از تجربه PII یا پردازش PII برای چنین هدفی آگاه شود، وی ممکن است ترجیح دهد که PII به این روش پردازش نشود یا به صورت عمومی‌به اشتراک گذاشته نشود.

۴-۴-۶ PII ناخواسته

PIIی که از سوی کنترل کننده PII یا پردازنده PII ناخواسته باشد (یعنی به طور غیر عمد بدست آید) نیز ممکن است در سامانه ICT ذخیره شود. برای مثال، یک اصل PII می‌تواند به صورت بالقوه PII را به یک کنترل کننده PII که از سوی کنترل کننده PII درخواست یا طلب نشده است (برای مثال، PII افزوده ارائه شده در متن یک فرم بازخورد ناشناس در یک وب سایت)، ارائه کند. خطر جمع آوری PII ناخواسته می‌تواند با درنظر گرفتن اقدامات حفاظت حریم خصوصی در زمان طراحی سامانه کاهش یابد (همچنین به مفهوم«حریم خصوصی براساس طراحی» اشاره دارد).

۴-۴-۷ PII حساس

حساسیت در تمام PIIهایی که PII حساس می‌تواند از آن استنتاج شود گسترده می‌شود. برای مثال نسخه‌های پزشکی می‌توانند اطلاعات با جزئیات را در مورد سلامت اصل PII بیان کنند. حتی درصورتی که PII حاوی اطلاعات مستقیمی‌در مورد گرایش جنسی یا سلامتی اصل PII نباشد، درصورتی که بتواند برای استنباط چنین اطلاعاتی مورد استفاده قرار گیرد، PII می‌تواند حساس باشد. در جهت اهداف این استاندارد، PII باید به عنوان PII حساسی که چنین استنتاج و آگاهی از هویت اصل PII به طور معقولی محتمل است درنظر گرفته شود.

در برخی از حوزه‌ها، آنچه PII حساس را شکل می‌دهد نیز به طور روشن در قانون تعریف شده است. مثال‌هایی در این زمینه شامل نمایش نژاد، منشاء قومی، عقاید فلسفی یا دینی، نظرات سیاسی، عضویت اتحادیه تجاری، سبک زندگی یا گرایش جنسی و سلامت جسمیو روانی اصل PII می‌شود. در حوزه‌های دیگر PII حساس ممکن است شامل اطلاعاتی باشد که می‌تواند سرقت هویت را تسهیل کند و یا درغیر این صورت به زیان مالی قابل توجه به شخص حقیقی منجر شود (برای مثال، شماره‌های کارت اعتباری، اطلاعات حساب بانکی یا شناسه‌هایی که از سوی دولت منتشر می‌شوند مانند شماره‌های گذرنامه، شماره امنیت اجتماعی یا شماره‌های گواهی نامه‌های رانندگی) و اطلاعاتی که می‌توانند برای تعیین موقعیت حال حاضر اصل PII مورد استفاده قرار گیرند.

پردازش PII حساس مستلزم اقدامات احتیاطی ویژه است. در برخی حوزه‌ها، پردازش PII حساس ممکن است از سوی قانون قابل اجرا حتی با ترجیح موافقت اصل PII ممنوع باشد. برخی حوزه‌ها ممکن است مستلزم اجرای کنترل‌های ویژه در جایی که انواع خاصی از PII حساس پردازش می‌شوند باشد (برای مثال، الزامی‌برای رمزگذاری PII درمانی هنگام انتقال آن در یک شبکه عمومی).

۴-۵ الزامات حفاظت حریم خصوصی

سازمان‌ها برای محافظت PII به دلایل گوناگون دارای انگیزه هستند: برای محافظت از حریم خصوصی اصل PII جهت برآورده کردن الزامات قانونی و تنظیمی، جهت اجرای مسئولیت مشترک، جهت افزایش اطمینان مصرف

کننده و غیره. هدف این بند ارائه مروری بر عوامل مختلفی است که می‌توانند الزامات حفاظت حریم خصوصی را که به یک سازمان خاص یا PII پردازش کننده ذی‌نفع حریم خصوصی مرتبط است، تحت تاثیر قرار دهد.

الزامات حفاظت حریم خصوصی می‌تواند به بسیاری از جنبه‌های مختلف پردازش PII مرتبط باشد، برای مثال مجموعه و حافظه PII، انتقال PII به اشخاص ثالث، روابط قراردادی میان کنترل کننده‌های PII و پردازنده‌های PII، انتقال ملی PII و غیره. الزامات حفاظت حریم خصوصی همچنین می‌توانند از نظر ویژگی متنوع باشند. آنها می‌توانند از نظر ماهیت بسیار کلی باشند، برای مثال شامل برشمارش اصول سطح بالای حریم خصوصی که از یک سازمان انتظار می‌رود تا هنگام پردازش PII آنها را مد نظر قرار دهد. اگرچه، الزامات حفاظت حریم خصوصی می‌تواند شامل محدودهای خاص بسیاری در پردازش انواع مشخص PII باشد، یا اجرای کنترل‌های خاص حریم خصوصی را دستور دهد.

طراحی هر سامانه ICT که شامل پردازش PII می‌شود باید پیش از شناسایی الزامات حفاظت حریم خصوصی مرتبط باشد. مفاهیم حریم خصوصی سامانه‌های ICT به صورت اساسی تغییر داده شده که شامل پردازش PII است باید پیش از آنکه آن سامانه‌های ICT اجرا شوند، مقرر شوند. سازمان‌ها به صورت معمول فعالیت‌های مدیریت ریسک وسیعی را اجرا می‌کنند و نمایه‌های خطر مرتبط با سامانه‌های ICT خود را توسعه می‌دهند.

مدیریت خطر به صورت «فعالیت‌های هماهنگ جهت هدایت و کنترل یک سازمان با توجه به خطر»تعریف می‌شود (راهنمای ISO ۷۳:۲۰۰۹). فرآیند مدیریت خطر حریم خصوصی دربرگیرنده فرآیندهای زیر است:

- برقراری یک مفهوم به وسیله درک سازمان (برای مثال، پردازش PII، مسئولیت‌ها)، محیط فنی و عوامل تاثیرگذار بر مدیریت خطر حریم خصوصی (یعنی عوامل قانونی و تنظیمی، عوامل قراردادی، عوامل تجاری و عوامل دیگر)؛
- ارزیابی خطر با شناسایی، تحلیل و سنجیدن خطر برای PIIاصلی (خطراتی که آنها به شدت می‌توانند تحت تاثیر آن قرار گیرند)
- تدبیر در مورد خطر با تعریف الزامات حفاظت حریم خصوصی، شناسایی و اجرای کنترل‌های حریم خصوصی جهت اجتناب یا کاهش خطرات برای PIIاصلی؛
- ارتباط و مشاوره با بدست آوردن اطلاعات از بخش‌های ذی‌نفع، احراز توافق در مورد هر فرآیند مدیریت خطر و مطلع کردن PIIاصلی و ارتباط درمورد خطرات و کنترل‌ها؛ و
- نظارت و بررسی با پیگیری خطرات و کنترل‌ها و بهبود دادن فرآیند.

یک مورد قابل ارائه می‌تواند ارزیابی اثر حریم خصوصی باشد که مولفه ای از مدیریت خطر است که بر تضمین مطابقت با الزامات حریم خصوصی و قانون حفاظت داده و ارزیابی مفاهیم حریم خصوصی برنامه‌ها یا فعالیت‌های جدید یا اساسا اصلاح شده متمرکز است. ارزیابی‌های اثر حریم خصوصی باید در چارچوب کاری وسیع تر مدیریت خطر یک سازمان ساخته شود.

شکل ۱- عوامل تاثیر گذار بر مدیریت خطر حریم خصوصی

الزامات حفاظت حریم خصوصی به عنوان بخشی از فرآیند مدیریت خطر حریم خصوصی کلی شناسایی شده است که تحت تاثیر عوامل زیر قرار داد (همانطور که در شکل ۱ نشان داده و در زیر شرح داده شده است):

- عوامل قانونی و تنظیمی‌برای حفاظت حریم خصوصی فرد حقیقی و حفاظت PII آنها؛
- عامل قراردادی مانند رهنمودهای صنعت، استانداردهای حرفه ای، خط‌مشی‌های شرکت؛
- عوامل تجاری از پیش تعیین شده به وسیله برنامه کاربردی تجاری خاص یا در یک زمینه استفاده خاص؛ و

عوامل دیگری که می‌توانند طراحی سامانه‌های ICT و الزامات حفاظت حریم خصوصی مرتبط را تحت تاثیر قرار دهند.

۴-۵-۱ عوامل قانونی و تنظیمی

الزامات حفاظت حریم خصوصی اغلب در (۱) قوانین بین المللی، ملی و محلی ، (۲) مقررات، (۳) تصمیمات قضایی یا (۴) توافق نامه‌های انجام شده با انجمن‌های کاری یا دیگر سازمان‌های کاری منعکس شده اند. برخی از مثال‌های قانون‌گذاری ملی و محلی شامل قوانین حفاظت داده، قوانین حفاظت مشتری، قوانین هشدار نفوذ، قوانین نگهداری داده و قوانین استخدامی‌هستند. قانون بین المللی مرتبط ممکن است شامل قوانین تاثیر گذار بر انتقال مرزی PII باشد. کنترل کننده‌های PII باید از تمام الزامات حفاظت حریم خصوصی به وجود آمده از عوامل قانونی یا تنظیمی‌آگاهی داشته باشند. برای دست یابی به این هدف، می‌توانند از نزدیک با متخصصان قانون هماهنگ شوند. درحالی که در بسیاری از حوزه‌ها کنترل کننده PII خواهد بود که در نهایت مسئول تضمین پیروی هستند، تمام فعالان دخیل در پردازش PII باید رویکردی کنش‌گرایانه را در شناسایی الزامات حفاظت حریم خصوصی ایجاد شده به وسیله عوامل قانونی و دیگر عوامل اتخاذ کنند.

۴-۵-۲ عوامل قراردادی

تعهدات قراردادی نیز می‌توانند الزامات حفاظت حریم خصوصی را تحت تاثیر قرار دهند. این تعهدات می‌توانند از توافق نامه‌های میان و در بین چندین فعال مختلف، مانند پردازنده‌های PII، کنترل کننده‌های PII و اشخاص

ثالث ناشی شود. برای مثال، یک ذی‌نفع حریم خصوصی ممکن است مستلزم استفاده اشخاص ثالث از کنترل‌های خاص حریم خصوصی و موافقت با الزامات ازبین بردن PII پیش از آنکه PII به آنها انتقال یابد، باشد. الزامات حفاظت حریم خصوصی می‌تواند نتیجه خط‌مشی شرکت و پیوند قوانین مشترک باشد که ذی‌نفع حریم خصوصی برای خود تنظیم کرده است، برای مثال جهت حفاظت از عنوان تجاری خود دربرابر تبلیغات منفی در بروز نقض حریم خصوصی.

اصولا، هر بخش که به PII دسترسی دارد باید از تعهدات خود به وسیله کنترل کننده‌های PII مربوطه به روشی رسمی، برای مثال، با عقد توافق نامه‌هایی با شخص ثالث آگاهی یابد. چنین توافق نامه‌هایی احتمالا دربرگیرنده تعدادی از الزامات حفاظت حریم خصوصی است که شخص ثالث (پذیرنده PII) باید مد نظر خود قرار دهد. در حوزه‌های معینی، مراجع ملی و محلی ممکن است ابزارهای قراردادی و قانونی را که انتقال PII، به شخص ثالث امکان پذیر می‌کند را برقرار کنند.

۴-۵-۳ عوامل تجاری

الزامات حفاظت حریم خصوصی می‌تواند تحت تاثیر عوامل تجاری نیز قرار گیرد که شامل خصوصیات ویژه یک برنامه کاربردی در نظر گرفته شده یا زمینه استفاده از آن می‌شود. عوامل تجاری می‌تواند بسته به نوع ذی‌نفع حریم خصوصی و نوع تجارت بسیار متنوع باشد. برای مثال، می‌توانند به ناحیه ای مرتبط باشد که یک سازمان در آن فعال است (برای مثال، رهنمودهای صنعتی، ضوابط اجرا، تجربیات موفق، استانداردها) یا ماهیت مدل تجاری آن (برای مثال خدمت‌های برخط ۲۴/۷، خدمت اشتراک گذاری اطلاعات، برنامه‌های کاربردی بانکداری).

همین‌طور بسیاری از عوامل تجاری دارای اثر مستقیم بر الزامات حفاظت حریم خصوصی نیستند. استفاده در نظر گرفته شده از PII احتمالا می‌تواند بر به‌کارگیری خط‌مشی‌های حریم خصوصی سازمان و همچنین انتخاب کنترل‌های حریم خصوصی اثر گذار باشد، اما نباید بر اصول حریم خصوصی که سازمان به آنها متعهد است اثر گذارد. برای مثال، ارائه یک خدمت معین ممکن است مستلزم این باشد که یک ارائه دهنده خدمت PII افزوده را جمع آوری کند یا برای بیشتر کارکنان خود اجازه دسترسی به انواع معینی از PII را فراهم کند. اگرچه این امر به معنای آن نیست که یک کنترل کننده PII که به اصول قرارگرفته در این چارچوب کاری متعهد است نباید دیگر با دقت ارزیابی کند که کدام نوع از PII به شدت نیازمند ارائه خدمت است (اصول محدودیت جمع آوری) و دسترسی کارمندانش به PII مورد بحث را به آنهایی که به منظور انجام وظایف خود نیازمند دسترسی به آنها هستند را محدود کند.(اصول امنیت اطلاعات)

۴-۵-۴ عوامل دیگر

مهمترین عاملی که سازمان‌های باید هنگام شناسایی الزامات حفاظت حریم خصوصی مورد توجه قرار دهند به اولویت‌های اصول PII مربوط می‌شود. استقرار شخصی یک فرد حقیقی در برابر حریم خصوصی و آنچه ملاحظات یک فرد حقیقی را به خطر می‌اندازد می‌تواند به تعدادی از عوامل شامل درک فرد حقیقی از فن‌آوری مورد استفاده، پیش زمینه آنها، اطلاعات ارائه شده، هدف از تراکنش، تجربه پیشین فرد حقیقی و عوامل اجتماعی-روانی بستگی داشته باشد.

طراحان سامانه ICT باید برای درک نگرانی‌های احتمالی حریم خصوصی یک اصل PII و درک انواع PII که باید از طریق سامانه‌های آنها پردازش شوند تلاش کنند. همانند یک توسعه دهنده سامانه یا یک ارائه دهنده خدمت

یا برنامه کاربردی که گروه‌های مشتری هدف را برای انتظارات استفاده و خواسته‌ها و نیازهای آنها مورد مطالعه قرار می‌دهد، با توجه به حریم خصوصی آزمودن و درک انتظارات و اولویت‌های افراد حقیقی از اهمیت برخوردار است.هر چند، این امکان همیشه برای طراحان سیستم‌های ICT وجود ندارد که اصل PII را با ویژگی‌هایی که با مزیت‌های امنیتی آنها منطبق باشد، فراهم کنند. این در واقع یک نکته مهم طراحی است.

مثال‌هایی از اولویت‌های حریم خصوصی می‌تواند شامل اولویتی برای گمنامی‌یا نام مستعار داشتن ، توانایی محدود کردن این‌که چه کسی می‌تواند به PII معینی دسترسی داشته باشد، یا توانایی محدود کردن هدف این‌که کدام PII پردازش خواهد شد، می‌شود. تا حد امکان، اصل PII باید گزینه اولویت‌های پردازش داده وی، برای مثال این‌که آیا PII برای اهداف ثانویه مانند بازاریابی مورد استفاده قرار می‌گیرد، را در اختیار قرار دهد. توانایی بیان اولویت‌های سازگار با حریم خصوصی[1] می‌تواند با استفاده از واسط کاربری گرافیکی سامانه ICT اجرا شود. این امر می‌تواند به اصل PII با نمایش مجموعه ای از گزینه‌های از پیش تعیین شده برای اولویت‌های متداول حریم خصوصی با استفاده از زبان به آسانی قابل فهم کمک کند. اجرای واسط کاربری می‌تواند مبتنی بر عناصری مانند جعبه‌های انتخاب[2] یا فهرست‌های بالا به پایین[3] باشد.

علاوه بر فاکتورهای فهرست شده در بندهای پیش، هم‌چنان عوامل دیگری وجود دارند که می‌توانند طراحی سامانه‌های ICT و الزامات حفاظت حریم خصوصی مربوطه را تحت تاثیر قرار دهد. برای مثال، الزامات حفاظت حریم خصوصی می‌تواند تحت تاثیر سامانه‌های کنترل داخلی یا استانداردهای فنی که یک سازمان اتخاذ کرده است قرار گیرد (برای مثال، یک استاندارد اختیاری، مانند استاندارد ISO).

۶-۴ خطمشی‌های حریم خصوصی

راس مدیریت یک سازمان که در پردازش PII دخیل است باید یک خطمشی حریم خصوصی را برقرار کند. خطمشی حریم خصوصی باید:

- مناسب هدف سازمان باشد؛
- چارچوب کاریی را برای ایجاد اهداف ارائه کند؛
- تعهدی را نسبت به برآورده کردن الزامات حفاظت حریم خصوصی قابل اجراء دربرگیرد؛
- تعهدی را نسبت به بهبود مدام دربرگیرد؛
- با سازمان مرتبط باشد؛
- برای طرف‌های ذی‌نفع به طور مناسب قابل دسترس باشد.

سازمان باید خطمشی حریم خصوصی خود را به صورت نوشته مستند کند. درجایی که سازمان پردازش کننده PII، پردازنده PII باشد، این خطمشی‌ها می‌تواند در مقیاس وسیعی به وسیله کنترل کننده PII تعیین شود. خطمشی حریم خصوصی باید با قواعد و تعهدات با جزئیات بیشتر ذی‌نفعهای حریم خصوصی مختلف دخیل در پردازش PII (برای مثال، رویه‌هایی برای حوزه‌ها یا کارمندان خاص) تکمیل شوند. به علاوه، کنترل‌هایی که

1 - privacy-friendly

2- checkboxes

3- dropdown

جهت اجرای خط‌مشی حریم خصوصی در یک مجموعه ویژه (برای مثال، کنترل دسترسی، مقررات اعلام، بازبینی‌ها و غیره) باید به روشنی مستند شود.

اصطلاح «خط‌مشی حریم خصوصی» اغلب برای اشاره به خط‌مشی‌های حریم خصوصی، هم داخلی و هم خارجی مورد استفاده قرار می‌گیرد. خط‌مشی حریم خصوصی داخلی، قواعد، تعهدات، محدودیت‌ها و یا کنترل‌هایی که یک سازمان جهت برآورده کردن الزامات حفاظت حریم خصوصی که به پردازش PII آن مرتبط می‌شود را به‌کار می‌گیرند، مستند می‌کند. خط‌مشی حریم خصوصی خارجی اعلام اقدامات حریم خصوصی سازمان و همچنین دیگر اطلاعات مرتبط مانند هویت و آدرس رسمی‌کنترل کننده PII، نقاط تماسی که اصلیهای PII ممکن است از آن نقاط اطلاعات افزوده را بدست آورد و موارد دیگر را در اختیار بیگانه‌ها قرار می‌دهد. در زمینه استفاده از این چارچوب کاری، اصطلاح «خط‌مشی حریم خصوصی» برای اشاره به خط‌مشی حریم خصوصی داخلی یک سازمان مورد استفاده قرار می‌گیرد. به خط‌مشی‌های حریم خصوصی خارجی به عنوان اعلانات اشاره می‌شود.

۴-۷ کنترل‌های حریم خصوصی

سازمان‌ها باید کنترل‌های حریم خصوصی را جهت برآورده کردن الزامات حفاظت حریم خصوصی به وسیله ارزیابی خطر برای حریم خصوصی و فرآیند مقابله، شناسایی و اجرا کنند. به علاوه، کنترل‌های حریم خصوصی شناسایی و اجرا شده باید به عنوان بخشی از ارزیابی خطر برای حریم خصوصی سازمان مستند شوند. انواع معینی از پردازش PII می‌توانند تضمین کنند، کنترل‌های خاص را برای مواردی که نیاز تنها زمانی مشهود خواهد شد که یک عملیات درنظر گرفته شده با دقت تحلیل شده باشد. ارزیابی خطر برای حریم خصوصی می‌تواند در شناسایی خطرات خاص نقض حریم خصوصی که در یک عملیات درنظر گرفته شده وجود دارد، به سازمان‌ها کمک کند.

از سوی سازمان‌ها تلاش‌هایی باید جهت توسعه کنترل‌های حریم خصوصی آنها به عنوان بخشی از یک رویکرد «حریم خصوصی براساس طراحی»صورت گیرد، یعنی پیروی در مرحله طراحی سامانه‌های پردازش PII، به جای حمایت کردن در مرحله بعدی مدنظر قرار می‌گیرد.

تا آنجا که کنترل‌های امنیت اطلاعات مورد توجه است، توجه به این نکته که تمام پردازش PII مستلزم همان سطح یا نوع حفاظت نیست از اهمیت برخوردار است. سازمان‌ها باید میان عملیات‌های پردازش براساس خطرات مشخصی که معرفی می‌کنند تمایز قائل شوند تا تعیین کنند که کدام کنترل امنیت اطلاعات در کدام مورد مناسب است. مدیریت خطر در این فرآیند یک روش مرکزی است و شناسایی کنترل‌های حریم خصوصی نیز باید بخشی یک‌پارچه از چارچوب کاری کاری مدیریت امنیت اطلاعات سازمان باشد.

۵ اصول حریم خصوصی ISO/IEC 29100

۵-۱ مرور کلی بر اصول حریم خصوصی

اصول حریم خصوصی شرح داده شده در این استاندارد از اصول موجود توسعه یافته توسط تعدادی از ایالات، کشورها و سازمان‌های بین المللی استنتاج شده است. این چارچوب کاری بر اجرای اصول حریم خصوصی در سامانه‌های ICT و توسعه سامانه‌های مدیریت حریم خصوصی جهت اجرا در سامانه‌های ICT سازمان متمرکز است. این اصول حریم خصوصی باید جهت هدایت طراحی، توسعه و اجرای اصول حریم خصوصی و کنترل‌های

حریم خصوصی مورد استفاده قرار گیرد. به علاوه این اصول می‌توانند به عنوان خط مبنایی در جنبه‌های نظارت

۱- موافقت و انتخاب
۲- درستی و مشخصات هدف
۳- محدودیت جمع آوری (مجموعه)
۴- کمینه سازی داده
۵- بازداری استفاده و محدودیت افشاء
۶- دقت و کیفیت

و سنجش عمل‌کرد، محک زنی و بازبینی برنامه‌های مدیریت حریم خصوصی در یک سازمان مورد استفاده قرار گیرد.

برخلاف تفاوت‌های موجود در عوامل اجتماعی، فرهنگی، قانونی و اقتصادی که می‌تواند به‌کارگیری این اصول را در برخی زمینه‌ها محدود کند، به‌کارگیری تمام اصول تعریف شده در این استاندارد ملی توصیه می‌شود. استثناءها برای این اصول باید محدود شوند.

اصول حریم خصوصی زیر مبنای این استاندارد ملی را شکل می‌دهد.

جدول ۳- اصول حریم خصوصی ISO/IEC 29100

۷- آشکاری، شفافیت و اعلام

۸- دسترسی و مشارکت فردی

۹- قابلیت شمارش

۱۰- امنیت اطلاعات

۱۱- قابلیت پیروی از حریم خصوصی

۵-۲ موافقت و انتخاب

رعایت اصل موافقت یعنی:

- ارائه حق انتخاب به اصل PII در مورد این‌که آیا PII آنها پردازش شود و یا خیر، به غیر از زمانی که اصل PII نتواند آزادانه از موافقت امتناع کند یا درجایی که قانون کاربست‌پذیر به طور خاص امکان پردازش PII را بدون موافقت فرد حقیقی فراهم کند. انتخاب اصل PII باید آزادانه، خاص و برمبنای آگاهی اعلام شود؛
- احراز موافقت ترجیح داده شده اصل PII جهت جمع آوری یا درغیر این صورت پردازش PII حساس به غیر از جایی که قانون کاربست‌پذیر پردازش PII حساس را بدون موافقت فرد حقیقی امکان پذیر کند؛
- آگاه کردن اصل PII، پیش از احراز موافقت، درمورد حقوق آنها تحت مشارکت فرد و اصل دسترسی؛
- فراهم نمودن اصل PII، قبل از کسب موافقت، همراه با اطلاعاتی که با آزادی، شفافیت و توجه اصلی نمایش داده می‌شود، و
- تعریف مفاهیم واگذاری یا ممانعت موافقت برای PIIهای اصلی.

مقرراتی باید برای ارائه فرصت انتخاب این‌که چگونه PII آنها به‌کار برده شود و امکان پذیر کردن صرف نظر کردن از موافقت به آسانی و بدون هزینه برای PII، اصلی ایجاد شود. در مورد این درخواست باید مطابق با خط‌مشی حریم خصوصی اقدام شود. حتی اگر از موافقت صرف نظر شود، کنترل کننده PII ممکن است به حفظ PII معین برای یک دوره زمانی به منظور برآورده شدن تعهدات قانونی و قراردادی (برای مثال، حفظ داده، جوابگویی) نیاز داشته باشد. درجایی که پردازش PII مبتنی بر موافقت نیست و درعوض مبتنی بر مبنای قانونی دیگری است، اصل PII باید هر زمان که امکان پذیر است مطلع شود. در جایی که اصل PII دارای توانایی صرف نظر از موافقت باشد و انجام این کار را انتخاب کرده باشد، این PII باید از پردازش برای هر هدفی که قانونی فرمان داده نشده است، صرف نظر شود.

برای یک کنترل کننده PII، رعایت اصل انتخاب یعنی:

- ارائه اصول PII سازوکاری روشن، مهم، به آسانی قابل فهم، قابل دسترس و امکان پذیر جهت انتخاب و اعلام موافقت در ارتباط با پردازش PII آنها در زمان جمع آوری، اولین مرتبه استفاده یا به محض آنکه عملی شود به اصل PII؛ و
- اجرای اولویت‌های اصل PII، همانطور که در موافقت آنها اعلام شده است.

به علاوه، مقررات افزوده می‌توانند برای PII درحال پردازش، متفاوت از موافقت تعریف شوند (برای مثال،عمل‌کرد یک قرارداد، بهره حیاتی اصل PII، یا مطابقت با قانون). قانون کاربست‌پذیر در برخی از نمونه‌ها نشان می‌دهد که اصل PII یک مبنای قانونی کافی را جهت پردازش PII تشکیل نمی‌دهد (برای مثال، موافقت یک فرد نابالغ که بدون رضایت والدین یا قیم اعلام می‌شود). به علاوه، الزامات افزوده برای انتقال PII به صورت بین المللی باید مدنظر قرار گیرد. مطابقت با این مقررات افزوده پیش از پردازش یا انتقال داده وظیفه کنترل کننده PII است.

۵-۳ درستی و مشخصات هدف

رعایت اصل درستی و مشخصات هدف یعنی:

- تضمین مطابقت اهداف با قانون کاربست‌پذیر و تکیه بر یک مبنای قانونی مجاز؛
- ارتباط با اصل PII پیش از زمانی که اطلاعات جمع آوری می‌شود یا برای اولین بار برای یک هدف جدید مورد استفاده قرار می‌گیرد؛
- استفاده از زبان برای این مشخصات که هم روشن و هم به صورت مناسب با شرایط منطبق است؛ و
- درصورت امکان، ارائه تعاریف کافی برای نیاز به پردازش PII حساس.

با توجه به PII حساس، قواعد شدیدتری می‌تواند درمورد هدف پردازش اعمال شود. هدف می‌تواند مستلزم یک مبنای قانونی یا تصویب به وسیله مرجع حفاظت داده یا یک مرجع دولتی باشد. درصورتی که اهداف پردازش PII از قانون کاربست‌پذیر تبعیت نکند، پردازش نباید رخ دهد.

۵-۴ محدودیت جمع آوری

رعایت اصل محدودیت جمع آوری یعنی:

- محدود کردن جمع آوری PII به اندازه ای که میان مرزهای قانون کاربست‌پذیر قرار گیرد و به شدت برای اهداف مشخص شده ضروری باشد.

سازمان‌ها نباید PII را بطور غیر مشخص جمع آوری کنند. هم میزان و هم نوع PII جمع آوری شده باید به اندازه ای محدود شود که جهت برآورده کردن (قانونی کردن) هدف مشخص شده به وسیله کنترل کننده PII ضروری است. سازمان‌ها باید با دقت درنظر داشته باشند که کدام PII جهت تحقق یک هدف مشخص پیش از پرداختن به جمع آوری PII مورد نیاز خواهد بود. سازمان‌ها باید نوع PII جمع آوری شده، همچنین توجیه آنها برای انجام آن به عنوان بخشی از خط‌مشی‌های اداره اطلاعات آنها و اقدامات، را مستند کنند.

یک کنترل کننده PII ممکن است بخواهد PII افزوده را برای اهدافی غیر از شرط یک خدمت معین که به وسیله اصل PII (برای مثال، برای اهداف بازاریابی مستقیم) درخواست شده است، جمع آوری کند. بسته به حوزه، چنین اطلاعات افزوده ای ممکن است تنها با موافقت اصل PII جمع آوری شود. همچنین ممکن است جمع آوری اطلاعات مشخص به وسیله قانون لازمم الاجرا فرمان داده شود. در زمان که امکان پذیر باشد، به اصل PII باید توانایی انتخاب این‌که آیا چنین اطلاعاتی را ارائه کند و یا خیر داده شود. اصل PII باید همچنین به روشنی از این واقعیت که واکنش آنها به چنین درخواست‌هایی برای اطلاعات افزوده می‌تواند اختیاری باشد، مطلع شود.

۵ـ۵ کمینه سازی داده

کمینه سازی داده با اصل «محدودیت جمع آوری»پیوند نزدیکی دارد اما از آن فراتر می‌رود. نظر به این‌که «محدودیت جمع آوری»به داده محدود جمع آوری شده در ارتباط با اهداف تعیین شده اشاره دارد، «کمینه سازی داده» به شدت، پردازش PII را به حداقل می‌رساند.

رعایت اصل کمینه سازی داده یعنی طراحی و اجرای رویه‌های پردازش داده و سامانه‌های ICT به چنان روشی که:

- PII ایی را که پردازش می‌شود و تعداد ذی‌نفعهای حریم خصوصی و افرادی را که PII برای آنها فاش می‌شود یا به آن دسترسی دارند، کمینه می‌کند؛
- اتخاذ اصل «نیاز به دانستن» را تضمین می‌کند، یعنی باید به فرد امکان دسترسی برای PII که برای اجرای وظایف رسمی خود در چارچوب کاری کاری هدف قانونی PIIی درحال پردازش ضروری است داده شود؛
- استفاده یا ارائه به عنوان گزینه‌های پیش فرض، هرزمان که امکان پذیر باشد، تعاملات و تبادلاتی که در شناسایی PIIهای اصلی نقشی ندارند، مشاهده پذیری رفتار آنها را کاهش می‌دهد و پیوند پذیری PII جمع آوری شده را محدود می‌کند؛ و
- حذف و از بین بردن PII هرزمان که هدف پردازش PII منقضی شود، هیچ الزام قانونی جهت نگه داری PI یا هر زمان که انجام این کار عملی باشد وجود ندارد.

۶ـ۵ محدودیت استفاده، نگهداری و افشاء

رعایت اصل محدودیت استفاده، نگهداری و افشاء یعنی:

- محدود کردن استفاده، نگهداری و افشاء (شامل انتقال) PII به اندازه ای که جهت برآورده کردن اهداف خاص، روشن و قانونی ضروری است؛
- محدود کردن استفاده از PII برای اهدافی مشخص شده به وسیله کنترل کننده PII پیش از جمع آوری، مگر این‌که هدفی متفاوت به صراحت به وسیله قانون قابل اجرا لازم دانسته شود؛
- نگه داری PII تنها به اندازه ای که جهت برآورده کردن اهداف بیان شده ضروری باشد و پس از آن از بین بردن و یا گمنام سازی آن به صورت ایمن؛ و
- قفل کردن (یعنی بایگانی، حفظ و مستثنی کردن PII در برابر پردازش بیشتر) هر PII هنگامی‌که و به مدتی که اهداف بیان شده منقضی شوند، اما در جایی که نگهداری از سوی قوانین قابل اجرا لازم دانسته شود.

زمانی که PII به صورت بین المللی انتقال می‌یابد، کنترل کننده PII باید از هر الزام محلی و ملی افزوده که به انتقال‌های مرزی اختصاص دارد اگاه باشد.

۷ـ۵ دقت و کیفیت

رعایت اصل دقت و کیفیت یعنی:

- تضمین این‌که PII پردازش شده دقیق، کامل، به روز (مگر این‌که مبنایی قانونی برای قدیمی نگه‌داشتن[1] داده وجود داشته باشد)، مناسب و مرتبط برای اهداف استفاده باشد؛
- تضمین قابل اطمینان بودن PII جمع آوری شده از منبعی غیر از اصل PII پیش از آنکه پردازش شده باشد؛
- بازبینی اعتبار و صحت ادعاهای مطرح شده از سوی اصل PII پیش از ایجاد هرنوع تغییر در PII (به منظور تضمین این‌که تغییرات به طور صحیح مجاز شمرده شده اند)، از طریق ابزارهای مناسب، درجایی که انجام آن مناسب باشد؛
- برقراری رویه‌های جمع آوری PII برای کمک به تضمین دقت و کیفیت؛ و
- برقراری سازوکارهای کنترل جهت بررسی دوره ای دقت و کیفیت PII جمع آوری و ذخیره شده.

این اصل به صورت خاص در مواردی که داده می‌تواند جهت موافقت یا رد یک مزیت قابل توجه برای فرد حقیقی یا در مواردی که داده نادرست می‌تواند در غیراین صورت باعث صدمه غیر قابل توجه به فرد حقیقی شود، مهم است

۸-۵ آشکاری، شفافیت و اعلام

رعایت اصل آشکاری، شفافیت و اعلام یعنی:

- ارائه اصول اطلاعات روشن و به آسانی قابل دسترس درمورد خط‌مشی‌ها، رویه‌ها و عمل‌کردهای کنترل کننده PII با توجه به پردازش PII به اصل PII؛
- بیان این واقعیت که PII درحال پردازش شدن است، هدفی که برای آن این امر انجام شده است، انواع ذی‌نفعهای حریم خصوصی برای کسانی که PII ممکن است افشاء شود و هویت کنترل کننده PII شامل اطلاعات درمورد چگونگی تماس با کنترل کننده PII در اعلام‌ها؛
- افشاء انتخاب‌ها و ابزارهای ارائه شده به وسیله کنترل کننده PII برای اصلیهای PII برای اهداف محدود کردن پردازش و برای ارزیابی، اصلاح و حذف اطلاعات آنها؛ و
- اعلام به اصل PII چه زمانی تغییرات مهم در رویه‌های اداره PII رخ می‌دهد.

شفافیت، شامل اطلاعات کلی درمورد منطق اساسی پردازش PII می‌تواند مورد نیاز باشد، به ویژه در صورتی که پردازش شامل تصمیمی‌باشد که بر اصل PII اثر گذار باشد. ذی‌نفعهای حریم خصوصی که PII را پردازش می‌کنند باید اطلاعات مشخصی را درمورد خط‌مشی‌ها و عمل‌کردهای خود که به مدیریت PII که به آسانی در دسترس عموم قرار دارد، ایجاد کنند. تمام تعهدات قراردادی که بر پردازش PII اثر گذار هستند باید به طور مقتضی به صورت داخلی مستند و ابلاغ شود. این PII همچنین باید به صورت خارجی نیز به اندازه ای که آن تعهدات محرمانه نباشند ابلاغ شوند.

به علاوه، هدف از پردازش شدن PII باید به اندازه کافی با جزئیات بیان شود تا برای اصل PII امکان درک موارد زیر را فراهم کند:

- PII مشخص شده مورد نیاز برای اهداف مشخص شده؛

1- outdated

- هدف مشخص شده برای جمع آوری PII؛
- پردازش مشخص شده (شامل سازوکارهای جمع آوری، ارتباط و ذخیره سازی)؛
- انواع افراد حقیقی مجاز که به PII دسترسی خواهند داشت و PII می‌تواند به آنها انتقال یابد؛ و
- الزامات از بین بردن و نگه داری داده PII مشخص شده.

۵-۹ دسترسی و مشارکت فردی

رعایت اصل دسترسی و مشارکت فردی یعنی:

- ایجاد توان دسترسی و بررسی PII آنها برای PIIهای اصلی، با فرض این‌که هویت آنها ابتدا با یک سطح مناسب تضمین تصدیق شده است و این چنین دسترسی به وسیله قانون قابل اجرا ممنوع نشده است؛
- فراهم کردن امکان اعتراض به دقت و تمامیت PII به PIIهای اصلی و خواست تغییر، اصلاح و حذف شدن به طور مناسب و امکان پذیر در زمینه مشخص؛
- فراهم کردن هرنوع تغییر، اصلاح یا حذف برای پردازنده‌های PII و اشخاص ثالث که داده شخصی برای آنها درجایی که آنها شناخته شده هستند افشاء شده است؛ و
- برقراری رویه‌هایی جهت توانا ساختن PIIهای اصلی جهت اعمال این حقوق به روشی ساده، سریع و کارامد که مستلزم تاخیر و هزینه زیادی نیست.

کنترل کننده PII باید کنترل‌های مناسبی را جهت تضمین این‌که PIIهای اصلی به طور دقیق به PII خود دسترسی دارند نه به دیگر PIIهای اصلی، اعمال کنند، مگر این‌که دسترسی فرد حقیقی تحت نظارت مرجعی به جای اصل PII که قادر به اجرای حقوق دسترسی خود نیست انجام شود. قانون قابل اجرا می‌تواند حق دسترسی، بررسی و اعتراض به پردازش PII را تحت شرایط معینی، در اختیار فرد حقیقی قرار داد. زمانی که یک چالش در جهت رضایت یک فرد حقیقی حل نشده باشد، مفاد چالش حل نشده باید به وسیله سازمان ثبت شود. در زمان مقتضی، وجود چالش حل نشده باید به پردازنده‌های PII و دیگر اشخاص ثالث که به اطلاعات مورد بحث دسترسی دارند انتقال یابد.

۵-۱۰ قابلیت شمارش

پردازش PII وظیفه مراقبت و اتخاذ اقدامات مستحکم و عملی را برای حفاظت آن را در برمی‌گیرد. رعایت اصل قابلیت شمارش یعنی:

مستند سازی و ابلاغ که برای تمام خط‌مشی‌ها، رویه‌ها و تجربه‌های مرتبط با حریم خصوصی مناسب است؛

- واگذاری وظیفه اجرای خط‌مشی‌ها، رویه‌ها و عمل‌کردهای مرتبط با حریم خصوصی به یک فرد خاص در سازمان (که ممکن است به طور مقتضی به نوبت به دیگران در سازمان محول شود)؛
- هنگام انتقال PII به اشخاص ثالث، تضمین این‌که پذیرنده شخص ثالث موظف به ارائه سطحی مشابه از حفاظت حریم خصوصی از طریق ابزارهای قراردادی یا دیگر ابزارها مانند خط‌مشی‌های داخلی الزامی(قانون قابل اجرا می‌تواند دربرگیرنده الزامات افزوده درخصوص انتقال‌های داده بین المللی باشد) خواهد بود؛
- ارائه آموزش مناسب برای کارکنان کنترل کننده PII که به PII دسترسی خواهند داشت؛

- تنظیم رسیدگی به شکایت داخلی کارآمد و رویه‌های جبران خسارت برای استفاده شدن توسط PIIهای اصلی؛
- آگاهی دادن به PIIهای اصلی در مورد نقض‌های حریم خصوصی که می‌تواند موجب خسارت اساسی به آنها (مگر آنکه ممنوع شده باشد، برای مثال هنگام کار براساس اقدام قانونی) و همچنین اقدامات درنظر گرفته شده برای تحلیل، شود؛
- مطلع کردن تمام ذی‌نفعهای حریم خصوصی درمورد نقض‌های حریم خصوصی که در برخی از حوزه‌ها مورد نیاز است (برای مثال مراجع حفاظت داده) و به سطح خطر بستگی دارد؛
- امکان پذیر کردن دسترسی برای اصل PII زیان دیده به مجوزها و یا راه حل‌های مناسب و موثر مانند تصحیح، از بین بردن یا جبران درصورت وقوع نقض حریم خصوصی؛ و
- درنظر گرفتن رویه‌هایی برای جبران موقعیت‌هایی که در آن برگرداندن وضعیت حریم خصوصی فرد حقیقی به موقعیتی که هیچ اتفاقی رخ نداده است، دشوار یا غیر ممکن خواهد بود.

اقدامات برای از بین بردن یک نقض حریم خصوصی باید متناسب با خطرات مرتبط با نقض باشد اما باید تا حد امکان با سرعت اجرا شود (مگر این‌که ممنوع شده باشد، برای مثال تداخل با یک تحقیق قانونی).

برقراری رویه‌های جبران خسارت بخش مهمی‌از برقراری قابلیت شمارش است. جبران خسارت ابزارهایی را برای اصل PII جهت بدست گرفتن کنترل کننده PII که مسئول سوءاستفاده از PII است را فراهم می‌آورد. استرداد یکی از اشکال جبران خسارت است که شامل ارائه غرامت به اصل PII زیان دیده می‌شود. این امر نه تنها در موقعیت سرقت هویت، آسیب به شهرت یا سوءاستفاده از PII از اهمیت برخوردار است، بلکه درجایی که اشتباهات درمورد اصلاح یا تغییر PII مربوطه رخ می‌دهد نیز مهم است.

درجایی که فرآیندهای جبران خسارت درحال انجام است، PIIهای اصلی ممکن است احساس اطمینان بیشتری در ورود به یک تراکنش داشته باشند، چراکه خطر مشاهده شده برای فرد حقیقی با توجه به خروجی به طور موثری کاهش یافته است. برای برخی خدمت‌ها، رسیدن به جبران خسارت آسان تر (برای مثال، خسارت مالی) از خدمت‌های دیگر (برای مثال، یک هویت سرقت شده، آسیب به یک تصویر یا شهرت فرد حقیقی)، است که توانایی بیان کمیت و جبران زیان می‌تواند تاحدی سخت تر باشد. جبران خسارت زمانی که مبتنی بر شفافیت و صداقت باشد بهترین عمل‌کرد را دارد. انواع مورد نیاز اقدامات جبران خسارت می‌تواند براساس قانون نظارت شود.

۵-۱۱ امنیت اطلاعات

رعایت اصل امنیت اطلاعات یعنی:

- حفاظت از PII تحت نظارت خود با کنترل‌های مناسب در سطح عملیاتی، عمل‌کردی و استراتژیک جهت تضمین یک‌پارچگی، قابلیت اطمینان و دسترس پذیری PII، و محافظت از آن در مقابل خطراتی مانند دسترسی، تخریب، استفاده، اصلاح، افشاء یا زیان غیرمجار در تمام چرخه حیات آن؛
- انتخاب پردازنده‌های PII که حداقل ضمانت نامه‌های کافی را با توجه به کنترل‌های سازمانی، فیزیکی و فنی برای پردازش PII و تضمین مطابقت با این کنترل‌ها، ارائه می‌دهند؛
- قرار دادن این کنترل‌ها بر مبنای الزامات قانونی قابل اجرا، استانداردهای امنیتی، نتایج ارزیابی‌های منظم خطر امنیتی که در ISO 31000 شرح داده شده است و نتایج تحلیل هزینه/سود؛

- به‌کارگیری کنترل‌های متناسب با احتمال و شدت عواقب بالقوه، حساسیت PII، تعداد PIIهای اصلی که ممکن است تحت تاثیر قرار گیرد و زمینه ای که در آن قرار می‌گیرد؛
- محدود کردن دسترسی به PII برای افرادی که به این چنین دسترسی برای اجرای وظایف خود نیاز دارند و محدود کردن دسترسی که در اختیار آن افراد قرار دارد به PII که به منظور اجرای وظایف خود به دسترسی به آن نیاز دارند؛
- رفع خطرات و آسیب پذیری‌هایی که از طریق ارزیابی‌های خطر حریم خصوصی و فرآیندهای بازبینی کشف شده اند؛ و
- قراردادن کنترل‌ها در معرض مرور و ارزیابی دوره ای در یک فرآیند مدیریت خطر امنیت درحال جریان.

۱۲-۵ پیروی از حریم خصوصی

رعایت اصل پیروی از حریم خصوصی یعنی:

- تایید و نشان دادن این‌که پردازش حفاظت از داده و الزامات حفاظت از حریم خصوصی را برآورده می‌کند با استفاده از بررسی‌هایی که به صورت دوره ای اجرا می‌شوند با استفاده از بازرس‌های داخلی یا بازرس‌های شخص ثالث مورد اطمینان؛
- ایجاد کنترل‌های داخلی مناسب و سازوکارهای نظارتی مستقل در جایی که پیروی از قانون حریم خصوصی مربوطه را با امنیت، حفاظت داده و خط‌مشی‌های حریم خصوصی و رویه‌های آنها را تضمین می‌کند؛ و
- توسعه و حفظ ارزیابی‌های خطر حریم خصوصی به منظور سنجیدن این‌که آیا ابتکارات انتقال برنامه و خدمت شامل پردازش PII با حفاظت داده و الزامات حریم خصوصی مطابقت می‌کند و یا خیر.

قانون قابل اجرا می‌تواند مقرر کند که یک یا چند مرجع نظارتی مسئول نظارت بر پیروی از قانون حفاظت داده قابل اجرا هستند. در این موارد، رعایت اصل پیروی از حریم خصوصی نیز به معنای هماهنگی با این مراجع نظارتی و رعایت رهنمودها و درخواست‌های آنها است.

پیوست الف

(اطلاعاتی)
تشابه میان مفاهیم ISO/IEC 29100 و مفاهیم ISO/IEC 27000

به منظور تسهیل استفاده از خانواده ISO/IEC 27000 استانداردهای بین المللی در زمینه خاص حریم خصوصی و مفاهیم یک‌پارچه حریم خصوصی در متن ISO/IEC 27000، جدول زیر ارتباط میان مفاهیم اصلی آنها را نشان می‌دهد:

جدول الف-۱- مطابقت مفاهیم ISO/IEC 29100 با مفاهیم ISO/IEC 27000

مفاهیم ISO/IEC 29100	مطابقت با مفاهیم ISO/IEC 27000
ذی‌نفع حریم خصوصی	ذی‌نفع
PII	دارایی اطلاعات
نقض حریم خصوصی	رویداد امنیت اطلاعات
کنترل حریم خصوصی	کنترل
خطر حریم خصوصی	خطر
مدیریت خطر حریم خصوصی	مدیریت خطر
الزامات حفاظت حریم خصوصی	اهداف کنترل