INSO
19054
1st. Edition
2015

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

استاندارد ملی ایران
۱۹۰۵۴
چاپ اول
۱۳۹۳

فناوری اطلاعات- فنون امنیتی- چارچوب کاری معماری حریم

Information technology — Security techniques — Privacy architecture 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

« فناوری اطلاعات- فنون امنیتی- چارچوب کاری معماری حریم »

رئیس:	**سمت و/یا نمایندگی**
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا دانشگاه تربیت مدرس
دبیر:	
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	مشاور مرکز آپا دانشگاه تربیت مدرس
اعضا: (اسامی به ترتیب حروف الفبا)	
اسدی‌پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
ایزدپناه، سحر سادات (فوق لیسانس مهندسی فناوری اطلاعات)	رییس اداره تدوین استاندارد سازمان فناوری اطلاعات ایران
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
شیرازی، مریم (لیسانس فناوری اطلاعات)	کارشناس پژوهشگاه استاندارد سازمان ملی استاندارد ایران
صادقی، مریم (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس سازمان نظام صنفی رایانه‌ای کشور
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس حقیقی تدوین استاندارد سازمان ملی استاندارد ایران
قندهاری، آزاده (فوق لیسانس هوش مصنوعی)	کارشناس مرکز تحقیقات مخابرات ایران
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر دانشگاه تربیت مدرس
معروف، سینا (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- چارچوب کاری معماری حریم» که پیش‌نویس آن در کمیسیون‌های مربوط توسط مرکز آپا (اگاهی‌رسانی، پشتیبانی و امداد رخدادهای رایانه‌ای) دانشگاه تربیت مدرس تهیه و تدوین شده است و در سیصد و پنجاه و پنجمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۹۳/۱۰/۲۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه 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 تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 29101:2013, Information technology — Security techniques — Privacy architecture framework

فناوری اطلاعات- فنون امنیتی- چارچوب کاری معماری حریم

۱ هدف و دامنه کاربرد

۱-۱ کلیات

هدف از تدوین این استاندارد، تعریف یک چارچوب کاری معماری حریم است که:

- ملاحظاتی برای سامانه‌های فناوری اطلاعات و ارتباطات (ICT)[1] که اطلاعات قابل شناسایی شخصی (PII)[2] را پردازش می‌کند، مشخص می‌کند؛
- مولفه‌هایی برای پیاده‌سازی چنین سامانه‌هایی را فهرست می‌کند؛ و
- دیدگاه های معماری که از این مولفه ها در بافت آن استفاده شده است را ارائه می‌دهد.

این استاندارد ملی در هستارهای درگیر در مشخص کردن، تدارک، معماری، طراحی، آزمون، نگهداری، مدیریت و عملیاتی کردن سامانه‌های ICT که اطلاعات قابل شناسایی شخصی را پردازش می‌کند، کاربردپذیر است.

این استاندارد در درجه اول بر سامانه‌های ICT که برای تعامل با طرف‌های ارتباط[3] PII طراحی شده است، تمرکز دارد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار آن ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نمی‌باشد و در غیر این صورت همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۱۷۶۴۳: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیتی – چارچوب کاری حریم‌خصوصی[4]

2-2 ISO/IEC/IEEE 42010:2011, *Systems and software engineering — Architecture description*

1 - Information and Communication Technology
2 - Personally Identifiable Information
3 -Principals

۴- بر اساس منبع لاتین ISO/IEC 29100:2011.

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف ارائه‌شده در استانداردهای ISO/IEC 29100 و ISO/IEC/IEEE 42010 به کار می‌رود.

۴ نمادها و اصطلاحات کوته‌نوشت

در این استاندارد، کوته‌نوشت‌های زیر به کار می‌رود.

ICT	Information and Communication Technology	فناوری اطلاعات و ارتباطات
PET	Privacy Enhancing Technology	فناوری بهسازی حریم‌خصوصی
PII	Personally Identifiable Information	اطلاعات قابل شناسایی شخصی

۵ مرورکلی چارچوب کاری معماری حریم‌خصوصی

۵-۱ عناصر چارچوب

چارچوب کاری معماری حریم‌خصوصی ارائه‌شده در این استاندارد ملی به عنوان مرجع فنی برای توسعه‌دهندگان سامانه‌های ICT که PII را پردازش می‌کنند، در نظر گرفته می‌شود. این استاندارد الزامات خط‌مشی‌های حریم‌خصوصی را تعیین نمی‌کند؛ فرض می‌شود که خط‌مشی حریم‌خصوصی وجود دارد و الزامات حفاظت امن حریم‌خصوصی، تعریف شده است و حفاظت امن مناسب در سامانه ICT پیاده‌سازی می‌شود.

این چارچوب کاری معماری بر حفاظت از PII تمرکز دارد. از آنجا که این امر تا حدودی یک هدف امنیتی است، سامانه‌های ICT که PII را پردازش می‌کنند باید از خطوط راهنمای مهندسی امنیت اطلاعات نیز پیروی کنند. این چارچوب کاری معماری، برخی مؤلفه‌های امنیت اطلاعات ضروری برای حفاظت امن PII پردازش‌شده در سامانه‌های ICT را فهرست می‌کند. چارچوب کاری معماری ارائه‌شده بر اساس مدل استفاده‌شده در استاندارد ISO/IEC/IEEE 42010 است.

ذینفعان مربوط به این ملاحظات، ذینفعان حریم‌خصوصی تعریف‌شده در ISO/IEC 29100 هستند. جزئیات بیشتر در این مورد در بند ۶ بحث شده است.

ملاحظات برای چارچوب کاری معماری در بند ۷ شرح داده شده است و شامل اصول حریم‌خصوصی استاندارد ISO/IEC 29100 و الزامات حفاظت امن حریم‌خصوصی خاص سامانه ICT است.

چارچوب کاری معماری به شرح زیر ارائه می‌شود:

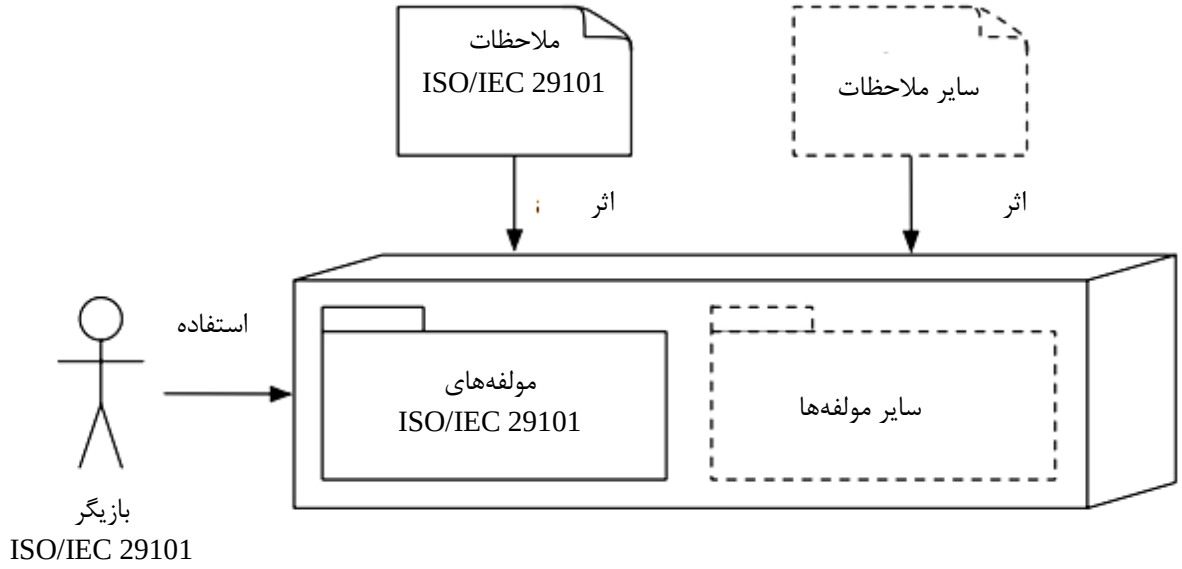
الف. لایه‌های چارچوب کاری معماری فنی بند ۸-۲، معماری را از دیدگاه مولفه نشان می‌دهد. هر لایه، مولفه‌ها را با یک هدف مشترک یا کارکرد مشابه گروه‌بندی می‌کند.

ب. مدل استقرار در بند ۸-۳، چارچوب کاری معماری را از دیدگاه سامانه ICT مستقل[1] نشان می‌دهد. هر دیدگاه گروه‌بندی، مولفه‌ها را بر اساس استقرار آن‌ها در سامانه‌های ICT ذینفعان نشان می‌دهد.

1 - Standalone

پ. دیدگاه‌های بند ۸-۴، چارچوب کاری معماری را از نقطه نظر تعامل نشان می‌دهد. دیـدگاه‌هـا، چگـونگی تعامل بین سامانه‌های ICT ذینفعان مختلف را نمایش می‌دهد.

همچنین چارچوب کاری معماری، قواعد مطابقت بین ملاحظات و نقطه نظرات را از طریق استفاده از جداول نگاشت ارائه می‌دهد.



شکل ۱ – عناصر چارچوب کاری معماری حریم‌خصوصی در زمینه کاری

شکل ۱ رابطه بین عناصر چارچوب کاری معماری حریم‌خصوصی را نشان می‌دهد. عنصـر مرکـزی چـارچوب کاری معماری، سامانه ICT در حال سـاخته شـدن اسـت. بـازیگر[1] اسـتاندارد ISO/IEC 29101 از سـامانه ICTاستفاده می‌کند. طراحی سامانه‌های ICT با ملاحظات این استاندارد و سایر ملاحظات تحـت تـاثیر قـرار می‌گیرد.

مثال‌هایی از سایر ملاحظات شامل الزامات غیر کارکردی است کـه بـر عملکـرد، دسـترس‌پـذیری و طراحـی سامانه ICT تاثیر می‌گذارد و بر پردازش کارکردی PII تاثیر نمی‌گذارد. این ملاحظات خارج از دامنه کـاربرد این استاندارد است.

ممکن است سامانه ICT، مولفه‌های چارچوب کاری معمـاری حـریم‌خصوصـی ایـن اسـتاندارد ملـی و سـایر مولفه‌ها را در برگیرد. این مولفه‌ها، PII را پردازش نمی‌کند، اما به جای آن سـایر کـارکردهـای سـامانه ICT مانند ارائه دسترسی یا پرداز زدن[2] واسطهای کاربری خاص را ساماندهی می‌کند. این مولفه‌ها، خارج از دامنه کاربرد این استاندارد هستند.

۵-۲ ارتباط با سامانه‌های مدیریت

استفاده از سامانه مدیریت، کنترل‌کننده‌ها و پردازشگرهای PII را قادر می‌سازد تا به طـور مـوثرتری الزامـات حفاظت امن حریم‌خصوصـی را بـا اسـتفاده از رویکـرد سـاختاریافته بـرآورده کنـد. همچنـین ایـن رویکـرد

1 - Actor
2- Rendering

ساختاریافته، امکان سنجش نتایج و بهبود مستمر اثربخشی سامانه مدیریت را برای کنترل‌کننده‌ها و پردازشگرهای PII فراهم می‌کند.
یک سامانه مدیریت موثر تا حد ممکن شفاف است، اما همچنان بر افراد، فرآیندها و فناوری اثر می‌گذارد. این سامانه باید بخشی از برنامه کنترل داخلی و راهبرد کاهش مخاطره سازمان باشد و پیاده‌سازی آن به ایجاد انطباق با مقررات حفاظت داده و حفظ حریم‌خصوصی کمک کند.

۶ بازیگران و PII

۶-۱ مرورکلی

بازیگران چارچوب کاری معماری ISO/IEC، ذینفعان حریم‌خصوصی درگیر در پردازش PII هستند که در ISO/IEC 29100 شرح داده شده است. بازیگران عبارتند از:

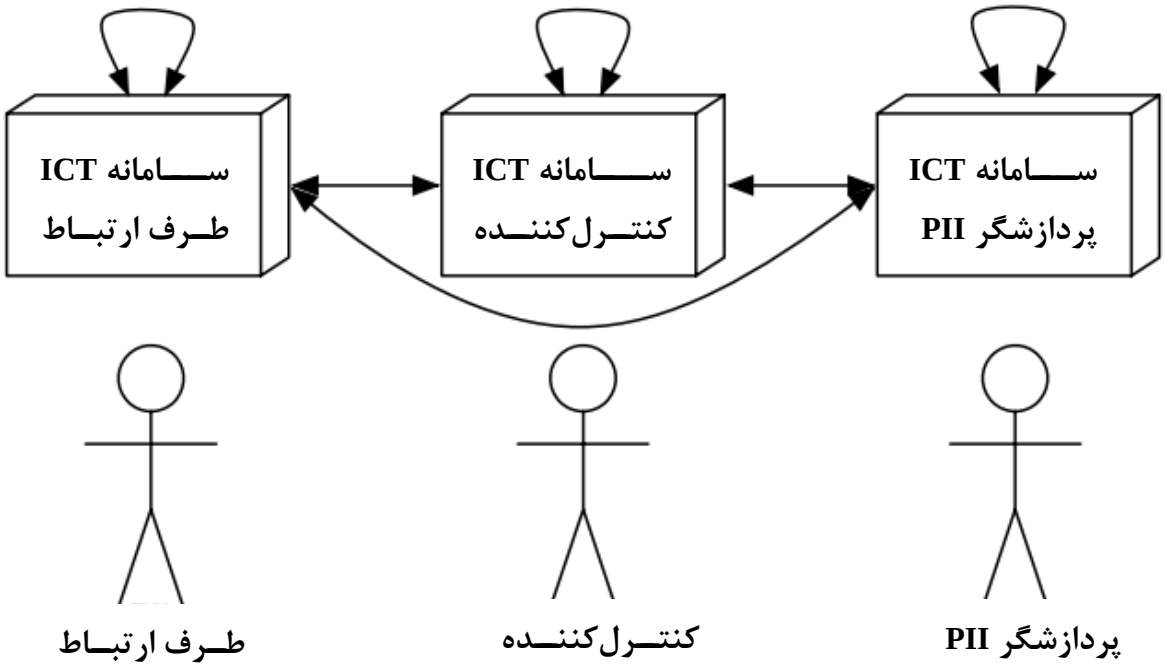
الف. طرف ارتباط PII؛

ب. کنترل‌کننده PII؛ و

پ. پردازشگر PII.

یادآوری- «طرف سوم» که به عنوان یکی از چهار دسته بازیگران در استاندارد ISO/IEC 29100 تعریف شده است، خارج از دامنه کاربرد چارچوب کاری معماری مشخص‌شده در این استاندارد است.

از نقطه نظر استقرار، چارچوب کاری معماری به سه بخش تقسیم می‌شود. هر قسمت به سامانه ICT مستقر از نقطه نظر هر یک از این بازیگران اعمال می‌شود.
شکل ۲، سامانه‌های ICT بازیگران و جریان‌های PII بین این سامانه‌های ICT را نشان می‌دهد. این شکل تقسیم‌بندی منطقی کارکردی برای چارچوب کاری معماری توصیف‌شده در این استاندارد را نمایش می‌دهد. این شکل به منظور ساختار فیزیکی، سازمان یا مالکیت سخت‌افزار سامانه ICT نیست.



شکل ۲ – بازیگران و سامانه‌های ICT آن‌ها مطابق ISO/IEC 29101

بازیگر ممکن است مسئولیت ساخت سامانه‌های ICT مورد استفاده خود را داشته باشد و یا این که مسئول آن نباشد. به عنوان مثال، ممکن است طرف ارتباط PII از سامانه ساخته‌شده استفاده کند و مسئولیت کنترل‌کننده PII یا سامانه ICT طرف ارتباط PII ممکن است بخشی از سامانه ICT کنترل‌کننده PII باشد. علاوه بر این، کارکرد سامانه ICT طرف ارتباط PII ممکن است در سامانه‌های سخت‌افزاری ICT مختلفِ متعلق به طرف ارتباط PII و کنترل‌کننده PII تقسیم شود. به طور مشابه، کنترل‌کننده PII ممکن است سامانه ICT پردازشگر PII را ارائه دهد. فرآیندهای کسب‌وکاری که در سامانه‌های ICT به کار گرفته شده‌اند، از طیف گسترده‌ای از مدل‌های ارتباطی و اعتماد استفاده می‌کنند. چارچوب کاری معماری در این استاندارد ملی بر انتزاع این مدل‌ها ایجاد شده است.

اگر طرف ارتباط PII از یک سامانه ICT متعلق به بخش خصوصی استفاده کند، سایر ذینفعان حریم‌خصوصی ممکن است الزاماتی را به این سامانه ICT تحمیل کنند. به عنوان مثال، سامانه ICT طرف ارتباط PII ممکن است ملزم به برآورده ساختن حداقل خط‌مبنای الزامات امنیتی به منظور اجازه اتصال به سایر سامانه‌های ICT باشد. مثال‌های دیگر شامل استفاده از مولفه‌های امنیتی خاص مانند نشان‌های[1] اصالت سنجی سخت‌افزار، نسخه‌های معین سامانه عامل[2] یا نسخه‌های ویژه مرورگر وب است.

به عنوان مثال، در سامانه‌های ICT که از ارتباطات همتا به همتا[3] (روش ارتباطی، مدل ارتباطی یا فناوری ارتباطی دارای ویژگی ارتباطی بین/ در میان هستارهایی که با یکدیگر و بدون کارساز مرکزی همتا شده‌اند) استفاده می‌کنند، هر برنامه کاربردی ممکن است نقش هر سه بازیگر بیان‌شده را ایفا کند. اطلاعات توسط هر

1 - Token
2 - Operating system
3 -Peer-to-peer

یک از همتایان ارسال و دریافت می‌شود، بنابراین هر همتا می‌تواند برای PII منتقل‌شده توسط طرف دیگر که نقش طرف ارتباط PII را دارد، کنترل‌کننده یا پردازشگر PII باشد.
در برنامه‌های کاربردی شبکه اجتماعی، PII ممکن است توسط هر کسی با دسترسی به رخ‌نماهای افراد دیگر پردازش شود. برنامه‌های کاربردی شبکه اجتماعی مبتنی بر وب به همه کاربران مجاز و ناشناس ممکن خدمت، اجازه می‌دهد PII ارائه‌شده توسط طرف‌های ارتباط PII متصل به شبکه اجتماعی را پردازش کند.

۶-۲ مراحل چرخه عمر پردازش PII

۶-۲-۱ جمع‌آوری

بسیاری از سازمان‌ها اطلاعات را از طرف‌های ارتباط PII جمع‌آوری می‌کند. این اطلاعات می‌تواند شامل PII باشد.
هنگام جمع‌آوری PII، سازمان‌ها همیشه باید اولویت‌های حریم‌خصوصی و حقوق قانونی[1] طرف ارتباط PII و الزامات حفاظت امن حریم‌خصوصی را همان‌گونه که در قانون[2] کاربردپذیر بیان‌شده است در نظر گیرند. عواملی مانند نوع PII، رضایت داده‌شده یا هر اولویت‌های حریم‌خصوصی بیان‌شده نیاز به در نظر گرفتن در تمام مراحل پردازش دارد. PII فقط باید در صورت نیاز برای اهداف اعلام‌شده، جمع‌آوری شود.
مستندات باید همراه با PII باشد. مثال‌ها شامل موارد زیر است اما به این موارد محدود نمی‌شود:
الف. برچسب‌های نرم‌افزاری بیان‌کننده مقاصدی که PII می‌تواند استفاده شود؛
ب. سوابق توصیف‌کننده مقاصدی که PII می‌تواند استفاده کند؛ و
پ. سوابق رضایت داده‌شده و هرگونه حساسیت‌های خاص که باید رعایت شود (به عنوان مثال، برخی دسته‌های معین PII باید پس از یک دوره زمانی معین رمزگذاری یا حذف شود).
کنترل‌های حریم‌خصوصی باید هر جا که داده‌ها به عنوان PII برچسب زده می‌شود یا هر جا که PII با اطلاعات افزوده در خصوص طرف ارتباط PII مشخص می‌شود، پیاده‌سازی شود. همچنین مهم است که برچسب‌های مربوط به پردازش PII در طول استفاده، انتقال، ذخیره‌سازی و مراحل امحا، حفظ شود. اگر PII ذخیره‌شده اصلاح شده باشد، باید دقت و ارزش آن قبل از استفاده، اعتبارسنجی شود.
علاوه بر این، فرآیندهای جمع‌آوری PII باید فقط به منظور جمع‌آوری PII لازم برای تراکنش مرتبط، طراحی شود. سازمان‌ها باید مراحلی را برای کمینه‌کردن جمع‌آوری غیرعمدی/ ناخواسته PII از طریق سامانه‌های ورودی داده (به عنوان مثال، فرم‌های کاربردی وب که اجازه ورود هرگونه اطلاعات را می‌دهد) اتخاذ کنند. ورود PII اختیاری باید از طریق به‌کارگیری نمایش محتوای خاص برای فیلدهای ورودی، با کاهش یا حذف فرم‌های کاربردی وب که اجازه ورود اطلاعات می‌دهند (به عنوان مثال، از بین بردن گزینه‌های انتخاب غیر ضروری و فیلدهای متنی آزاد) به حداقل برسد. علاوه بر این، استفاده از فیلدهای با ورودی‌های از پیش تعریف‌شده (به عنوان مثال، فهرست‌های انتخابی و فهرست‌های کشویی)، شامل گزینه‌های غیر PII، باید در

1 - Legal rights
2 - Law

نظر گرفته شود. وقتی فیلدهای متنی به شکل آزاد لازم است، واسط کاربری (UI)[1] باید موارد زیر را فراهم کند:

الف. هشدارهایی برای اعلام این که طرف ارتباط PII نباید PIIای غیر از آن چه به صراحت خواسته و موافقت شده یا توسط قانون کاربرپذیر مورد نیاز است را وارد کند.

ب. نشانه واضحی از فیلدهایی که در آن PII باید وارد شود و این که چه PIIای باید وارد شود (به عنوان مثال نام، نشانی، اطلاعات سلامت)؛ و

پ. نشانه واضحی از فیلدهایی که نباید PII در آن وارد شود.

۶-۲-۲ انتقال

انتقال، پخش یا انتشار PII به دیگران بدان معنی است که PII دیگر تنها تحت کنترل طرف ارتباط PII نیست. انتقال به طور معمول اصطلاحی برای پخش PII از کنترل‌کننده PII یا پردازشگر PII به سایر کنترل‌کننده‌ها و پردازشگرهای PII است. اگر PII از کنترل‌کننده PII به بازیگر دیگری منتقل شود، انتقال گاهی اوقات، افشا نیز گفته می‌شود.

پاسخگویی و مسئولیت‌پذیری برای PII منتقل‌شده باید توسط هر یک از طرفین درگیر در پردازش PII مورد توافق باشد و نگهداری شود. این توافق‌نامه باید در صورت نیاز توسط قوانین کاربردپذیر نوشته شود. علاوه بر این، چنین توافق‌نامه‌هایی باید با قوانین حفاظت داده در دامنه‌های منبع و مقصد انتقال منطبق شود. هنگامی که انجام این کار مرتبط و مناسب است یا زمانی که از نظر قانونی[2] مورد نیاز است، طرف ارتباط PII باید اطلاع دهد که انتقال در حال وقوع است و باید محتوا و منظور از انتقال را اطلاع دهد. اگر بین طرف ارتباط PII و کنترل‌کننده PII یا پردازشگر PII، اختلاف رخ دهد، سوابق تراکنش‌های انتقال PII مرتبط باید برای کمک به حل هرگونه اختلاف، در دسترس باشد.

از انتقال PII حساس باید اجتناب شود مگر این که برای ارائه خدمتی که طرف ارتباط PII درخواست کرده، ضروری باشد، این امر، یک الزام کسب‌وکار را برای ارائه خدمات درخواست شده، یا در صورتی که توسط قانون[3] مورد نیاز باشد محقق می‌کند. برخی حوزه‌های قضایی، قوانینی[4] که به طور خاص نیاز به توافق‌نامه‌های قراردادی رسمی دارند را پایه‌گذاری کرده‌اند که تمام الزامات حفاظت امن حریم‌خصوصی بین طرف‌های درگیر در زمانی که PII به خارج از حوزه قضایی با سطح حفاظت حریم‌خصوصی تعیین‌شده، منتقل می‌شود را شامل می‌شود. جایی که انتقال برون مرزی استفاده می‌شود، باید به اقدامات حفاظتی برای PII در حال انتقال توجه خاص شود.

سازوکارهای حفاظت مناسب باید در طول انتقال PII وجود داشته باشد. در مورد انتقال دیجیتال (رقمی)، PII باید در یک کانال امن منتقل شود یا اگر انتقال از طریق یک کانال ناامن است، به صورت رمزشده منتقل

1 - User Interface
2 - Legislation
3 - Law
4 - Laws

شود. اگر PII بر روی رسانه‌های فیزیکی منتقل می‌شود، باید رمزگذاری شود. اگر از رمزگذاری استفاده می‌شود، کلید رمزگذاری نباید ذخیره یا همراه با PII رمزگذاری‌شده منتقل شود.

۶-۲-۳ استفاده

استفاده از PII به معنی هر نوع پردازش PII است که «جمع آوری»، «انتقال»، «ذخیره»، «بایگانی» یا «امحا» را شامل نمی‌شود. اصول حریم‌خصوصی شرح داده شده در استاندارد ISO/IEC 29100 (چارچوب حریم‌خصوصی)، و همچنین برخی قوانین حفاظت و حریم‌خصوصی داده، ممکن است در صورتی که آن پردازش با اهداف مشخص‌شده اصلی ناسازگار باشد، پردازش PII را محدود کند. بنابراین، PII فقط باید برای مقاصد اعلام‌شده که برای آن جمع‌آوری شده، پردازش شود.

اگر PII باید برای هر هدف دیگری که با قانون کاربردپذیر، پوشش داده نمی‌شود، پردازش شود، رضایت طرف ارتباط PII یا نماینده وی باید گرفته شود. به طرف ارتباط PII باید در صورت وجود هرگونه سوال در مورد هرگونه فعالیتی که طرف‌های ارتباط PII واضح نیستند، ابزاری را برای تماس با کنترل‌کننده یا پردازشگر PII ارائه دهد.

جایی که چنین پردازشی لازم است، رضایت طرف ارتباط PII باید به دست آید، مگر این که توسط قانون مجاز باشد. به طرف‌های ارتباط PII باید اطلاع واضحی در مورد استفاده خاص از PII ارائه شود.

علاوه بر این، سازوکارهای مناسب حفاظت برای استفاده از PII باید همان طور که ضروری فرض شده با تحلیل مخاطره، به کار گرفته شود. این امر استفاده از فنون گمنامی[1] یا مستعارسازی[2] قبل از پردازش و استفاده از فنون محاسبات امن در طول پردازش را شامل نمی‌شود.

۶-۲-۴ ذخیره‌سازی

هنگامی که ذخیره PII ضروری است، رضایت طرف ارتباط PII باید با توجه به هرگونه اقدامات خاص که ممکن است توسط قانون مورد نیاز باشد به دست آید. در چنین مواردی، PII باید تنها برای مدت زمان لازم برای رسیدن به هدف خاص کسب‌وکار ذخیره شود.

PII باید برای جلوگیری از دسترسی غیرمجاز ، اصلاح، تخریب، حذف یا سایر استفاده‌های غیرمجاز، با کنترل‌ها و سازوکارهای مناسب ذخیره شود. این کنترل‌ها شامل رمزگذاری، اشتراک‌گذاری مخفی، مستعارسازی و گمنامی است، اما به این موارد محدود نمی‌شود.

PII بایگانی‌شده نیاز به توجه دقیق دارد. اصول حریم‌خصوصی بیان می‌کند که PII باید تنها تا زمانی که برای انجام اهداف بیان‌شده لازم است، حفظ شود و پس از آن به صورت امن نابود یا گمنام شود. با این حال، اگر کنترل‌کننده PII یا پردازشگر PII توسط قانون کاربردپذیر نیاز به حفظ PII پس از انقضای سایر اهداف داشته باشد، PII باید قفل شود (به عنوان مثال، برای جلوگیری از استفاده بیشتر با سازوکارهای کنترل دسترسی بایگانی و محافظت شود). ملاحظات اولیه در بایگانی PII باید اطمینان حاصل کند که سازوکارهای

1 - Anonymization
2 - Pseudonymization

مناسب حفاظت داده وجود دارد، از جمله راه‌حل‌های مدیریت دسترسی که دسترسی به PII بایگانی‌شده را تنها به کاربران مجاز ارائه می‌دهد.
کنترل‌کننده PII باید کنترل‌هایی را در سامانه‌های ذخیره‌سازی پیاده‌سازی کند تا PII را در زمان انقضا یا زمانی که هدف ذخیره‌سازی یا پردازش PII معتبر نیست، امحا کند.

۶-۲-۵ امحا

در مرحله پایانی چرخه عمر پردازش PII، PII حذف، گمنام، نابود، بازگردانده یا با برخی روش‌های دیگر امحا می‌شود. PII خاص در سوابق PII ممکن است از استفاده غیرمجاز با نشانه‌گذاری آن برای امحا، قفل شود. لازم به ذکر است که حذف PII لزوما به این معنی نیست که PII در نهایت امحا شده است، زیرا PII حذف‌شده در سامانه‌های ICT اغلب می‌تواند بازیابی شود. اگر چه ممکن است این کار در ساماندهی PII بسیار واضح به نظر برسد، اما گاهی اوقات روال‌های مربوط به امحای PII با الزامات حفاظت امن حریم‌خصوصی منطبق نیست. ویژگی‌های ارائه‌شده توسط طرف ارتباط PII (به عنوان مثال، هدف استفاده) یا الزامات مشخص‌شده توسط قانون (به عنوان مثال، تاریخ انقضا برای PII خاص) باید قبل از امحای PII در نظر گرفته شود.

۷ ملاحظات

۷-۱ مرورکلی

ملاحظه طبق تعریف ISO/IEC/IEEE 42010، نفع از یک سامانه مربوط به یک یا چند ذینفع است. چارچوب کاری معماری حریم‌خصوصی در این استاندارد بر ملاحظات ذینفعان حریم‌خصوصی مربوط به پردازش PII متمرکز می‌شود. ملاحظات ISO/IEC 29100، شامل اصول حریم‌خصوصی ISO/IEC 29100 و هرگونه الزامات حفاظت امن حریم‌خصوصی برگرفته‌شده و منطبق با این اصول است.
الزامات حفاظت امن حریم‌خصوصی باید با پیروی از فرایند مدیریت مخاطرات حریم‌خصوصی منطبق با فرآیند شرح‌داده‌شده در بند ۴-۵ ISO/IEC 29100. تعیین شود. هر فرد یا سازمانی که طراح سامانه ICT که PII را پردازش می‌کند، است باید از این فرایند پیروی کند. تمامی الزامات حفاظت امن حریم‌خصوصی شناسایی‌شده باید با قانون حریم‌خصوصی کاربردپذیر مطابقت داشته باشد.

۷-۲ اصول حریم‌خصوصی ISO/IEC 29100

کنترل‌کننده PII مسئول حفاظت از PII و ساماندهی عادلانه و قانونی[1] آن در همه زمان‌ها در سازمان و به علاوه پردازش PII برون‌سپاری‌شده به پردازشگرهای PII است.
در نهایت کنترل‌کننده PII مسئول پیاده‌سازی کنترل‌های حریم‌خصوصی در سامانه ICT است. کنترل‌های حریم‌خصوصی برای اطمینان از پرداختن و انجام سازگار الزامات حفاظت امن حریم‌خصوصی تعیین‌شده برای طرف ارتباط PII خاص، تراکنش یا سناریو (فرانامه)[2] در نظر گرفته می‌شود. شواهد پیاده‌سازی باید توسط

1 - Lawful
2 - Scenario

مستندسازی مناسب کنترل‌های حریم‌خصوصی که به کار گرفته شده و ارائه مستندات ممیزی که وجود کنترل‌ها و پیاده‌سازی درست و کارکرد مناسب را تصدیق می‌کند، ارائه شود. در نهایت، کنترل‌کننده PII باید اصول حریم‌خصوصی شرح‌داده‌شده در ISO/IEC 29100 را بپذیرد و به آن پایبند باشد.

الف- رضایت و انتخاب؛

ب- قانونی بودن[1] و ویژگی هدف؛

پ- محدودیت مجموعه؛

ت- کمینه کردن داده‌ها؛

ث- محدودیت استفاده، ابقا و افشا؛

ج- دقت و کیفیت؛

چ- باز بودن، شفافیت و اطلاع؛

ح- مشارکت فردی و دسترسی؛

خ- پاسخگویی؛

د- امنیت اطلاعات؛ و

ذ- انطباق حریم‌خصوصی.

۷-۳ الزامات حفاظت امن حریم‌خصوصی

سامانه‌های ICT باید کنترل‌های حریم‌خصوصی را به عنوان یک عنصر اصلی در هر مرحله از چرخه عمر پردازش PII پیاده‌سازی کنند. الزامات حفاظت امن حریم‌خصوصی، طراح سامانه ICT را برای عملیاتی کردن پیوند بین اصول حریم‌خصوصی و مولفه‌های معماری بند ۸ قادر می‌سازد.

به منظور پیاده‌سازی کنترل‌های حریم‌خصوصی موثر در سامانه ICT، جریان‌های پردازش PII توصیف‌کننده پردازش PII باید ایجاد شود. نمودارهای جریان پردازش PII، نمایشی گرافیکی (نگاشتاری)[2] از «جریان» PII از طریق سامانه ICT و بین بازیگران مختلف است. برای مثال، اگر یک بازیگر، PII را به بازیگر دیگری انتقال دهد (به عنوان مثال، پردازشگرهای PII) نمودار جریان پردازش PII باید آن انتقال‌های PII را شامل شود.

همچنین نمودار جریان پردازش PII ممکن است به عنوان جدول جریان PII ارائه شود. این نمودار یا جدول از جمع‌آوری، انتقال، استفاده، ذخیره‌سازی یا امحای PII پیروی می‌کند و اطلاعاتی مانند نوع PIIای که PII را جمع‌آوری کرده، هدف پردازش، جایی که PII به آن منتقل می‌شود، دریافت رضایت طرف ارتباط PII، دوره ابقا و محل ذخیره‌سازی و سطح مخاطره حریم‌خصوصی نتیجه‌شده را شامل می‌شود. اطلاعات جریان پردازش PII، یک ورودی به فرآیند مدیریت مخاطرات حریم‌خصوصی خواهد بود که خروجی آن الزامات حفاظت امن حریم‌خصوصی است.

پس از تکمیل تحلیل الزامات سامانه ICT، توسعه‌دهندگان باید الزامات حفاظت امن حریم‌خصوصی سامانه ICT را با فهرستی از ملاحظات این استاندارد ارجاع متقابل دهند. پس از آن الزامات حفاظت امن

1 - Legitimacy
2 - Graphic

حریم‌خصوصی باید برای انتخاب آن دسته از مولفه‌های معماری که الزامات گفته‌شده را برآورده می‌کنند، استفاده شود.
پیوست الف این استاندارد ملی شامل فهرست نمونه ملاحظات است و چگونگی پیوند ملاحظات اصول حریم‌خصوصی ISO/IEC 29100 و مولفه‌های معماری ISO/IEC 29101 را نشان می‌دهد.

۸ دیدگاه‌های معماری

۸-۱ مقدمه

دیدگاه‌های معماری در این بند به سه دیدگاه ساختار یافته است. اول، دیدگاه مولفه که مولفه‌های سامانه ICT را با جزئیات توصیف می‌کند و آن‌ها را به لایه‌های مبتنی بر کارکردهای آنها جدا می‌کند. هر لایه، مولفه‌هایی که به مشارکت پردازش مناسب PII کمک می‌کند را گروه‌بندی می‌کند. راهنمای پیاده‌سازی محدودی برای هر مولفه ارائه می‌شود. راهنمای بازیگر خاص در صورت کاربردپذیری ارائه می‌شود. این دیدگاه برای درک بلوک‌های سازنده در چارچوب کاری معماری حریم‌خصوصی مفید است.
جداول، مثال‌هایی از روابط معمول بین اصول حریم‌خصوصی ISO/IEC 29100 را نشان می‌دهد و مولفه‌های معماری در دیدگاه مولفه ارائه شده است. این جداول نگاشت، برای درک چگونگی پایبند بودن سامانه ICT به اصول حریم‌خصوصی ISO/IEC 29100 کمک می‌کند. جداول مشابه می‌تواند به عنوان مثال استفاده شود و در طول طراحی سامانه برای چگونگی پایبندبودن سامانه ICT خاص به اصول حریم‌خصوصی ISO/IEC 29100 به روز شود.
دیدگاه بازیگر به مولفه‌های توصیف‌شده در دیدگاه مولفه، از منظر سامانه ICT یک بازیگر فردی نگاه می‌کند. این دیدگاه در طراحی معماری سامانه ICT خاص مفید است. دیدگاه تعاملی به مولفه‌ها از منظر استقرار نگاه می‌کند. این دیدگاه برای درک چگونگی تعامل مولفه‌های سامانه‌های ICT بازیگران مختلف با یکدیگر مفید است.

۸-۲ دیدگاه مولفه

دیدگاه مولفه به منظور توصیف مولفه‌های سامانه ICT است که در پردازش PII درگیر هستند.
انتخاب مولفه‌ها باید با الزامات حفاظت امن حریم‌خصوصی مناسب، هدایت شود. توسعه‌دهندگان سامانه ICT برای بازیگر(های) خاص (به شکل ۲ مراجعه شود) باید از دیدگاه مولفه استفاده کنند تا مولفه‌هایی که نیاز به شامل شدن در معماری سامانه‌ای که در حال توسعه آن هستند، تعیین شود. این معماری باید مبتنی بر الزامات حفاظت امن حریم‌خصوصی مستقرشده با استفاده از راهنمایی ارائه‌شده در بند ۷ باشد. توجه شود که تمام مولفه‌های توصیف‌شده در این استاندارد ملی لزوما در یک سامانه ICT خاص مناسب نخواهد بود.
دیدگاه مولفه در سه لایه ارائه می‌شود. هر لایه یک گروه منطقی از مولفه‌هایی است که در یک هدف خاص در پردازش PII شرکت می‌کند. مولفه‌ها در لایه تنظیمات حریم‌خصوصی در میان سایرین، مدیریت فراداده در مورد پردازش PII را ساماندهی می‌کنند، از جمله تبادل اطلاعات در مورد هدف پردازش، رضایت و اولویت‌های طرف ارتباط PII. مولفه‌ها در لایه هویت و مدیریت دسترسی، مسئولیت اطمینان از استفاده از

اطلاعات هویت مناسب در پردازش PII و کنترل دسترسی به PII با توجه به الزامات حفاظت امن حریم‌خصوصی را دارد. در نهایت، مولفه‌های لایه PII وظایف مختلف پردازش PII را انجام می‌دهد.
چارچوب کاری معماری با این فرض که تمامی مولفه‌ها با چندین مولفه دیگر در تعامل هستند، طراحی می‌شود. با این حال، به منظور حفظ کلیت و خوانایی، تعامل‌های ممکن بین مولفه‌ها از بازنمایی، حذف شده است.
برخی مولفه‌ها در چارچوب کاری معماری، فناوری‌های بهسازی حریم‌خصوصی (PETs) هستند. این انتخاب فناوری‌های بهسازی حریم‌خصوصی جامع نیست. فناوری‌های بهسازی حریم‌خصوصی دیگری وجود دارد که در این استاندارد شرح داده نشده است و توسعه‌دهنده سامانه ICT مسئول انتخاب فناوری‌های بهسازی حریم‌خصوصی مناسب و تطابق آن با این چارچوب کاری معماری است.
پیوست ب این استاندارد ملی، مثالی از معماری سامانه ICT ارائه می‌دهد که فناوری‌های بهسازی حریم‌خصوصی را برای پردازش امن PII اعمال می‌کند. پیوست پ این استاندارد ملی، مثالی از نحوه استفاده از اعتبارهای مبتنی بر صفت را برای ساخت سامانه ICT که هویت مستعار و مدیریت کنترل دسترسی فراهم می‌کنند، ارائه می‌کند.
بخش‌های زیر، لایه‌ها، مولفه‌های درون آن‌ها و بازیگرانی که در تعامل با مولفه‌ها هستند را شرح می‌دهد. توصیف کلی هر مولفه داده شده است و دستورالعمل‌های بازیگر خاص نیز به دنبال آن آمده است. برای برخی مولفه‌ها، هیچ راهنمای خاصی در سامانه ICT بازیگر خاص به دلیل مشابهت رفتار مولفه در سامانه‌های ICT تمامی بازیگران، ارائه نشده است.

۸-۲-۱ لایه تنظیمات حریم‌خصوصی

لایه تنظیمات حریم‌خصوصی شامل مولفه‌هایی است که خط‌مشی حریم‌خصوصی سامانه را به بازیگران مرتبط اطلاع‌رسانی و الزامات حفاظت امن حریم‌خصوصی سامانه را پیاده‌سازی می‌کند.
علاوه بر این، مولفه‌ها در این لایه باید هرگونه اولویت‌های حریم‌خصوصی و اطلاعات اعلام رضایت جمع‌آوری‌شده از طرف ارتباط PII را به کنترل‌کننده PII و پردازشگر PII انتقال دهند.

۸-۲-۱-۱ ارتباط خط‌مشی و هدف

کلیات. این مولفه مسئول بازپخش اطلاعات، از جمله روزآمدها[1]، در مورد خط‌مشی حریم‌خصوصی کنترل‌کننده PII و هدف جمع‌آوری PII در سامانه‌های ICT ذینفعان حریم‌خصوصی است.
اطلاعات اطلاع‌رسانی‌شده باید دست کم شامل موارد زیر باشد:
الف- هویت‌های کنترل‌کننده‌های PII و هر پردازشگرهای PII مرتبط؛
ب- خط‌مشی‌ها در مورد انتقال PII به پردازشگر PII؛
پ- استفاده از فناوری‌های بهسازی حریم‌خصوصی (مانند گمنامی) با اهداف مرتبط.
ت- اهداف جمع‌آوری PII.
ث- شناسایی PIIای که باید جمع‌آوری شود؛ و

1 - Updates

ج- حقوق قانونی طرف ارتباط PII برای دسترسی به PII خود بـه منظـور تعیـین میـزان PII ذخیـره‌شـده و وارسی و تصحیح اشتباه‌ها و روال‌های انجام این کار.

طرف ارتباط PII. مولفه ارتباط خط‌مشی و هدف سامانه ICT طرف ارتباط PII باید:

الف- خط‌مشی‌ها و اطلاعات هدف را از مولفه مرتبط در سامانه ICT کنترل‌کننده PII دریافت کند.

ب- اطلاعات دریافت‌شده را تفسیر کند و نمایش دهد یا در غیر این صورت به طرف ارتباط PII بـه شـیوه‌ای قابل فهم، برساند.

پ- به طرف ارتباط PII، فرصت ذخیره محلی اطلاعات دریافت‌شده را پیشنهاد دهد؛ و

ت- به کنترل‌کننده PII تایید دهد که خط‌مشی و اطلاعات هدف توسط طرف ارتباط PII دریافت شده است.

کنترل‌کننده PII. مولفه ارتباط خط‌مشی و هدف سامانه ICT تحت کنترل کنترل‌کننده PII باید:

الف- خط‌مشی و اطلاعات هدف که به طرف ارتباط PII رسانده شده است را ذخیره کند؛

ب- واقعه‌نگاری[1] اقدامات رساندن خط‌مشی و اطلاعات هدف به طرف‌های ارتباط PII به‌گونه‌ای که بتواند این که کدام اطلاعات موجود بوده و در چه زمانی به طرف‌های ارتباط PII منتقل شده اسـت را همـراه بـا تاییـد دریافت این اطلاعات، ایجاد کند؛

پ- رساندن خط‌مشی کنونی و اطلاعات هدف به مولفه مرتبط سامانه ICT طرف ارتباط PII به شیوه‌ای کـه بتواند به طور مستقیم توسط این سامانه استفاده شود تا به طرف ارتباط PII بـه صـورت کامـل و قابـل فهـم اطلاع داده شود، یا بتواند با مولفه گفته‌شده مانند شکل برخی نگاشت‌های از پیش تعریف‌شده، نگاشت شود.

ت- انتقال مرجع به خط‌مشی نمایش داده‌شده و اطلاعات هدف به آن دسته از مولفه‌هایی که به ذخیره‌سازی اطلاعات رضایت و ذخیره‌سازی خود PII ساماندهی می‌کنند؛ و

ث- رساندن روزآمدها در مورد تغییرات خط‌مشی و اطلاعات هدف به مولفـه‌هـای مـرتبط سـامانه‌هـای ICT متعلق به آن دسته از طرف‌های ارتباط PII که دریافت این اطلاعات را قبول کرده‌اند.

پردازشگر PII. سامانه ICT پردازشگر PII به طور معمول باید رونوشت‌های رقمی خط‌مشی حریم‌خصوصی و هدف پردازش را از سامانه ICT کنترل‌کننده PII دریافت کند. سامانه ICT پردازشـگر PII بایـد مسـتندات خط‌مشی حریم‌خصوصی و هدف پردازش دریافت‌شده از کنترل‌کننده PII را به شکل واضح قابـل فهـم بـرای تمامی افراد دارای دسترسی به PII تحت نظارت خط‌مشی ارائه دهد.

کنترل‌کننده PII ممکن است پردازش PII توسط پردازشگرهای PII مختلف را ترتیب دهـد. مولفـه ارتبـاطی هدف در سامانه ICT کنترل‌کننده PII باید هدف مربوط به PII ارائه‌شده را به تمام پردازشگرهای PII مرتبط انتقال دهد. هر پردازشگر PII باید از هدف (های) پردازش PII اطلاع داشته باشد.

۸-۲-۱-۲ دسته‌بندی PII

کلیات. سامانه ICT باید از دسته‌های PII ای که پردازش می‌کند، آگاه باشد، در نتیجه می‌توانـد بـین انـواع مختلف داده‌ها (به عنوان مثال، PII حساس، PII و غیر PII) تمایز قائل شود این امر بـرای خـدمات پـردازش PII به طور متفاوت وابسـته بـه دسـته لازم اسـت. عـلاوه بـر ایـن، سـامانه ICT بایـد از مقـادیر PII شـامل

1 - Log

شناسانه‌های مستقیم، مانند نام‌ها و شماره‌های امنیت اجتماعی آگاه باشد. این مولفه باید کارکردهایی که چنین دسته‌بندی در سامانه ICT را ارائه می‌دهد پیاده‌سازی کند.
در مقابله با غیر PII، مخاطره ترکیب غیر PII برای استنباط یا اشتقاق هویت یا مشخصات منحصر به فرد کاربر یا دست کم زیرمجموعه به اندازه کافی کوچک کاربران باید درک و ارزیابی شود.
تمام PII ها باید به ترتیبی که پردازش می‌شوند و توسط سامانه ICT با توجه به حساسیت مشخص‌شده ذخیره می‌شوند، به درستی دسته‌بندی شود. اگر PII ندانسته جمع‌آوری شود، به عنوان مثال به عنوان نتیجه‌ی ورودی ناخواسته، انجام این کار ممکن نیست و از این رو اقدامات برای کمینه کردن احتمال جمع‌آوری PII ناخواسته باید انجام شود.
در حالی که سامانه ICT باید از مقادیر PII ای که شامل شناسه‌های مستقیم مانند نام‌ها و شماره‌های امنیت اجتماعی است، آگاه باشد، انجام این کار در صورتی که PII ناخواسته جمع‌آوری شده باشد، ممکن نیست.
طرف ارتباط PII. سامانه ICT طرف ارتباط PII باید قادر به شناسایی دسته‌بندی علامت‌گذاری مرتبط با PII باشد و باید PII را با توجه به دسته‌بندی آن پردازش کند. همچنین دسته‌بندی می‌تواند برای شناسایی PIIای که باید با استفاده از فناوری‌های بهسازی حریم‌خصوصی (به عنوان مثال PII حساس) محافظت شود، استفاده شود. همچنین مولفه دسته‌بندی PII، دسته‌بندی بیشتر PII به زیردسته‌هایی که این زیردسته‌ها نیازمندی یک دامنه کاربرد خاص هستند را فراهم می‌کند.
کنترل‌کننده PII. سامانه ICT کنترل‌کننده PII باید شامل دسته‌بندی جامعی از PII استفاده‌شده در سامانه‌های ICTای که PII دسته‌بندی‌شده را پردازش می‌کند، باشد. این اطلاعات باید به پردازشگرهای PII منتقل شود. همچنین، این دسته‌بندی می‌تواند با واقعه‌نگاری ممیزی، PII مستعار، افشای PII و بایگانی PII و ابقای مولفه‌هایی که می‌تواند مشخص کند کدام بخش از داده‌ها شامل PII است، استفاده شود.
پردازشگر PII. سامانه ICT پردازشگر PII باید قادر به پردازش دسته‌بندی PII مرتبط با PII دریافت‌شده باشد. اطلاعات باید در ممیزی PII و پردازش امن PII استفاده شود.

۸-۲-۱-۳ مدیریت رضایت

کلیات. رضایت طرف ارتباط PII پیش‌شرط مهم پردازش PII است، مگر این که چنین پردازشی توسط قانون مجاز شده باشد.
این مولفه وظایف مدیریت رضایت از جمله موارد زیر را ساماندهی می‌کند، اما به این موارد محدود نمی‌شود:
الف- دریافت رضایت آگاهانه از طرف ارتباط PII؛
ب- ذخیره‌سازی اطلاعات رضایت در سامانه‌های ICT ذینفعان حریم‌خصوصی؛
پ- مرتبط ساختن اطلاعات رضایت ذخیره‌شده به نسخه‌ای از خط‌مشی و اطلاعات هدف برای مواردی که رضایت داده شده است؛
ت- وارسی رضایت قبل از پردازش PII؛ و
ث- نگهداری وضعیت اطلاعات رضایت.
ممکن است قانون منتج به لغو یا محدودیت رضایت بیان‌شده توسط طرف ارتباط PII شود.

طرف ارتباط PII. کنترل‌کننده PII باید رضایت آگاهانه طرف ارتباط PII را با کمک مولفه مدیریت رضایت در سامانه ICT طرف ارتباط PII به دست آورد. در شرایط خاص، ممکن است طرف ارتباط PII رضایت را اصلاح یا از آن صرف نظر کند و این اطلاعات باید به سامانه ICT کنترل‌کننده PII بازپخش شود.

کنترل‌کننده PII. در سامانه ICT کنترل‌کننده PII، این مولفه باید اطلاعات به روز در مورد وضعیت رضایت را نگهداری کند. سامانه ICT کنترل‌کننده PII باید قادر به بازیابی، ذخیره‌سازی، مدیریت و نگهداری اطلاعات رضایت باشد.

سامانه ICT کنترل‌کننده PII باید اطلاعات رضایت را به طرف‌های دیگر در سامانه که به آن نیاز دارند، منتقل کند. علاوه بر این، این مولفه باید روزآمدهای وضعیت رضایت (به عنوان مثال، اصلاح یا صرف نظر کردن از رضایت) طرف‌های ارتباط PII را بپذیرد. سامانه ICT کنترل‌کننده PII باید این اطلاعات را در صورت لزوم ارائه و منتشر کند.

پردازشگر PII. سامانه ICT پردازشگر PII باید وجود رضایت از تمام طرف‌های ارتباط PII مرتبط را با PII ارائه‌شده به آن وارسی کند. این اطلاعات باید از سامانه ICT کنترل‌کننده PII به دست آید. قبل از هر گونه پردازش، سامانه ICT پردازشگر PII باید مطمئن شود که اطلاعات رضایت فعلی درباره طرف‌های ارتباط PII مرتبط را دارد. سامانه ICT پردازشگر PII باید آماده پذیرش تغییرات وضعیت رضایت، زمانی که این تغییرات توسط کنترل‌کننده PII اعلام می‌شود، باشد.

۸-۲-۱-۴ مدیریت اولویت حریم‌خصوصی

کلیات. در برخی شرایط، طرف ارتباط PII ممکن است قادر به بیان اولیت‌های خود برای چگونگی پردازش PII خود با کنترل‌کننده یا پردازشگر PII باشد. در این موارد، سامانه‌های ICT مرتبط بازیگران باید قادر به ثبت مناسب آن اولویت‌ها و شناختن آنها به کنترل‌کننده و پردازشگر PII باشد. کنترل‌کننده و پردازشگر PII باید قادر به درک اولویت‌ها باشد و باید به آن اولویت‌ها در هنگام پردازش PII تا بیشترین حد ممکن احترام بگذارد.

طرف ارتباط PII. اگر پردازش PII بر اساس تنظیمات اولویت حریم‌خصوصی باشد، پس باید واسطی به طرف ارتباط PII، برای انتخاب مناسب‌ترین تنظیمات برای هدف خود ارائه شود. به عنوان مثال، این واسط ممکن است شامل تنظیمات تعیین چگونگی استفاده، انتقال یا افشا PII سامانه ICT باشد.

کنترل‌کننده PII. اگر طرف ارتباط PII هرگونه اولویت حریم‌خصوصی را مشخص کرده باشد، سامانه ICT کنترل‌کننده PII باید این انتخاب‌ها را به کنترل‌کننده PII ارائه کند.

سامانه ICT کنترل‌کننده PII باید اولویت‌های حریم‌خصوصی مرتبطی که ممکن است طرف‌های ارتباط PII از گزینه‌های در دسترس آن اشاره کرده باشند را در صورت وجود جمع‌آوری کند. کنترل‌کننده نیز باید این اطلاعات را به طرف‌هایی که PII مرتبط با این اولویت‌ها را پردازش می‌کنند، منتشر کند.

پردازشگر PII. اگر به وظایف تخصیص‌یافته پردازشگر PII مربوط باشد، سامانه ICT پردازشگر PII باید آگاه باشد و پیرو محدودیت‌های تنظیم‌شده در پردازشگر PII توسط اولویت‌های حریم‌خصوصی منتخب طرف

ارتباط PII عمل کند. این اطلاعات و روزآمدهای ممکن باید از کنترل‌کننده PII یا به طور مستقیم از طرف ارتباط PII از طریق سامانه‌های ICT مرتبط به دست آید.

۸-۲-۱-۵ ارتباط بین اصول حریم‌خصوصی و مولفه‌های لایه تنظیمات حریم‌خصوصی

جدول ۱ مثالی از نگاشت اصول حریم‌خصوصی ISO/IEC 29100 به مولفه‌های لایه تنظیمات حریم‌خصوصی را نشان می‌دهد. 'X' در جدول نشان‌دهنده ارتباط بین مولفه لایه و یک اصل است. اگرچه این ارتباط فقط به عنوان یک مثال نشان داده شده است.

جدول ۱ – مثال رابطه بین اصول حریم‌خصوصی و مولفه‌های لایه تنظیمات حریم‌خصوصی

اصول / مولفه‌ها	رضایت و انتخاب	قانونی بودن هدف و ویژگی	محدودیت جمع‌آوری	کمینه‌سازی داده	استفاده، ابقا و محدودیت افشا	دقت و کیفیت	بازبودن، شفافیت و اطلاع	مشارکت و دسترسی انفرادی	پاسخگویی	کنترل‌های امنیت اطلاعات	انطباق
ارتباط خط‌مشی و هدف	X	X	X	X			X		X		X
دسته‌بندی PII			X	X	X						
مدیریت رضایت	X	X	X					X			
مدیریت اولویت حریم‌خصوصی	X	X	X		X		X				

۸-۲-۲ لایه مدیریت هویت و مدیریت دسترسی

مولفه‌ها در لایه مدیریت دسترسی و هویت به شناسایی بازیگران ISO/IEC 29101 و سامانه‌های ICT آنها و مدیریت اطلاعات هویت مرتبط کمک می‌کند. به‌علاوه، مولفه‌های موجود در این لایه کنترل می‌کنند که چگونه بازیگران ISO/IEC 29101 به PII دسترسی دارند. مولفه‌ها، قابلیت کارکردی زیر را پیاده‌سازی می‌کنند:

الف) مدیریت هویت‌های ذینفعان حریم‌خصوصی؛

ب) مدیریت هویت‌های بازیگرانی که از سامانه‌های ICT استفاده می‌کنند؛

پ) فراهم کردن اطلاعات برای سایر مولفه‌های سامانه‌های ICT؛ و

ت) مدیریت نگاشت بین هویت‌های طرف ارتباط PII و اسامی مستعار برای مستعارسازی PII.

هویت و لایه مدیریت دسترسی، اطلاعات هویتی را برای مولفه‌ها در لایه‌های دیگر که به آن نیاز دارند فراهم می‌کند. یادآوری می‌شود که این استاندارد فنون مدیریت هویتی که باید استفاده شود را مشخص نمی‌کند.

۸-۲-۲-۱ سامانه مدیریت هویت

کلیات. این مولفه می‌تواند چندین هدف داشته باشد، که هریک می‌تواند توسط یک سامانه مدیریت هویت مجزا پیاده‌سازی شود.

ابتدا، مولفه می‌تواند هویت‌های طرف‌های ارتباط PII را که PII آنها در سامانه ICT پردازش می‌شود، مدیریت کند. دوم، مولفه می‌تواند هویت‌های کاربران سامانه‌های ICT که PII را پردازش می‌کنند، مدیریت کند. سوم، مولفه می‌تواند هویت‌های سامانه‌های ICT ذینفعان حریم‌خصوصی را مدیریت کند. این کار به سامانه‌های ICT ذینفعان حریم‌خصوصی مختلف این امکان را می‌دهد که یکدیگر را در حین انتقال PII متقابلاً اصالت‌سنجی کنند. این فهرست از مثال‌ها جامع نیست.

سازوکارهای نشان دادن ماهیت و دقت اطلاعات هویت اساسی، توسط این استاندارد تعریف نمی‌شود. قابلیت کارکردی مولفه مدیریت هویت برای تمامی بازیگران مشابه است.

۸-۲-۲-۲ طرح مستعارسازی

کلیات. اگر مستعارسازی در پردازش PII استفاده شود، سامانه‌های ICT درگیر باید کارکردهایی برای مدیریت نمونه‌های کارکرد مستعارسازی انفرادی مورد استفاده داشته باشد.

مولفه طرح مستعارسازی در لایه مدیریت هویت و دسترسی شامل اطلاعاتی در مورد طرح مستعارسازی پیاده‌سازی‌شده و پارامترهای آن است. برای مثال، در صورتی که طرح رمزگذاری استفاده شود، این مولفه کلید استفاده‌شده را ذخیره می‌کند.

مولفه مستعارسازی PII مرتبط در لایه PII برای انجام تبدیل‌های واقعی در PII استفاده قرار می‌شود.

طرف ارتباط PII. اگر مستعارسازی در سامانه ICT طرف ارتباط PII استفاده شود، سامانه باید توضیحی از طرح مستعارسازی پیاده‌سازی‌شده داشته باشد. مولفه مستعارسازی در لایه PII سامانه ICT طرف ارتباط PII باید این طرح مستعارسازی را در PII به کار برد.

کنترل‌کننده PII. طرح‌های مستعارسازی ممکن است توسط سامانه ICT کنترل‌کننده PII مدیریت شود. در این مورد، سامانه ICT کنترل‌کننده PII، اطلاعات درباره طرح‌های مستعارسازی که توسط سامانه‌های ICT طرف‌های ارتباط PII و پردازشگرهای PII استفاده می‌شود را انتقال می‌دهد. این کار ممکن است برای اطمینان از این که PII مستعارشده از سامانه ICT طرف ارتباط PII بتواند در سامانه‌های ICT کنترل‌کننده PII و پردازشگر PII پردازش شود، مورد نیاز باشد. همچنین یادآوری می‌شود که ممکن است نمونه‌های چندگانه از یک طرح مستعارسازی لازم باشد، برای مثال، برای مستعارسازی PII به طور متفاوت در پردازشگرهای مختلف.

پردازشگر PII. اگر پردازشگر PII نیاز به انجام مستعارسازی مطابق با دستورالعمل‌های کنترل‌کننده PII داشته باشد، به پیاده‌سازی این مولفه برای مدیریت طرح‌ها نیز نیاز دارد.

۸-۲-۲-۳ کنترل دسترسی

کلیات. سازوکارهای کنترل دسترسی باید اطمینان حاصل کنند که دسترسی به ویژگی‌های موجود در سامانه ICT ساماندهی- PII تنها در محدوده‌های الزامات حفاظت امن حریم‌خصوصی داده می‌شود. برای مثال، در صورتی که جمع‌آوری PII از طرف ارتباط PII با استفاده از یک فرم وب انجام شود و این اتفاق بعد از یک مدت زمان مشخص روی دهد، دسترسی به فرم وب باید تنها در طول همان زمان فراهم شود. در این مثال، سامانه ICT کنترل‌کننده PII باید دسترسی طرف‌های ارتباط PII به فرم جمع‌آوری PII را محدود کند.

قابلیت کارکردی مولفه کنترل دسترسی برای همه بازیگران مشابه است. قواعد و روش‌ها برای کنترل دسترسی در هر سامانه ICT از الزامات حفاظت امن حریم‌خصوصی مشتق می‌شود.

۸-۲-۲-۴ اصالت‌سنجی

کلیات. اصالت‌سنجی، مولفه امنیتی مهم سامانه ICTای که PII را پردازش می‌کند است. این مولفه می‌تواند محرمانگی و یکپارچگی PII را که توسط سامانه جمع‌آوری، ذخیره و پردازش می‌شود، تضمین کند.

مولفه اصالت‌سنجی می‌تواند چندین هدف داشته باشد. اول، می‌تواند اصالت‌سنجی کاربرانی که با سامانه ICT کار می‌کنند را ساماندهی کند. دوم، می‌تواند اصالت‌سنجی متقابل سامانه‌های ICT یا مولفه‌های آن را به عنوان بخشی از دسترسی و انتقال امن PII مدیریت کند. این فهرست از مثال ها جامع نیست.

قواعد و روش‌های استفاده‌شده در هر استقرار سامانه ICT باید به طور جداگانه مورد توجه قرار گیرد و اهداف امنیتی بازیگری که از سامانه ICT استفاده می‌کند در نظر گرفته شود.

به عنوان مثال، سامانه ICT طرف ارتباط PII باید طرف‌های ارتباط PIIای که از سامانه استفاده می‌کنند را اصالت‌سنجی کند. به طور مشابه، سامانه ICT طرف ارتباط PII باید کنترل‌کننده PII را قبل از انتقال PII به سامانه ICT کنترل‌کننده PII اصالت‌سنجی کند.

قابلیت کارکردی مولفه اصالت‌سنجی در سامانه‌های ICT همه بازیگران مشابه است.

۸-۲-۲-۵ مجازشناسی[1]

کلیات. در سامانه‌های ICTای که دسترسی هر بازیگر محدود شده است، سامانه مجازشناسی باید مستقر شود. تنها کاربران مجاز سامانه ICT باید به PII دسترسی داشته باشند. برای مثال، طرف‌های ارتباط PII که هدف پردازش PII هستند می‌توانند به PII مرتبط خود دسترسی داشته باشند.

قابلیت کارکردی مولفه مجازشناسی برای همه بازیگران مشابه است. قواعد و روش‌ها برای اصالت‌سنجی در هر سامانه ICT از الزامات حفاظت امن حریم‌خصوصی مشتق خواهد شد.

1 - Authorization

۸-۲-۲-۶ ارتباط بین اصول حریم‌خصوصی و مولفه‌های لایه مدیریت دسترسی و هویت

جدول ۲ مثالی از نگاشت اصول حریم‌خصوصی ISO/IEC 29100 به مولفه‌های لایه مدیریت دسترسی و هویت را نشان می‌دهد. 'X' در جدول نشان‌دهنده ارتباط بین مولفه لایه و یک اصل است. اگرچه این ارتباط، تنها به عنوان یک مثال نشان داده شده است.

۸-۲-۳ لایه PII

مولفه‌های لایه PII باید قابلیت‌های کارکردی زیر را پیاده‌سازی کنند.

الف- جمع‌آوری و انتقال PII؛

ب- پردازش PII، شامل پردازش امن و ارائه؛

پ- ذخیره و بایگانی PII؛ و

ت- ممیزی PII و تراکنش‌های واقعه‌نگاری انجام‌شده در آن.

جدول ۲ – مثال ارتباط بین اصول حریم‌خصوصی و مولفه‌های لایه مدیریت دسترسی و هویت

اصول / مولفه‌ها	رضایت و انتخاب	قانونی بودن هدف و ویژگی	محدودیت جمع‌آوری	کمینه‌سازی داده	استفاده، ابقا و محدودیت افشا	دقت و کیفیت	بازبودن، شفافیت و اطلاع	مشارکت و دسترسی انفرادی	پاسخگویی	کنترل‌های امنیت اطلاعات	انطباق
سامانه مدیریت هویت					X		X			X	
طرح مستعارسازی				X	X				X	X	
کنترل دسترسی					X	X		X	X	X	
اصالت‌سنجی					X	X		X	X	X	
مجازشناسی					X	X		X	X	X	

این استاندارد تنها الزامات مدیریت PII عمومی را با حذف مشخصات موردنظر طراح برنامه کاربردی پیشنهاد می‌کند. حفاظت‌های امن حریم‌خصوصی مرتبط (یا کنترل‌ها) باید برای کاهش مخاطره نقض‌های حریم‌خصوصی در حین پردازش PII استفاده شود.

لایه PII از اطلاعاتی از لایه تنظیمات حریم‌خصوصی برای تقویت سنجش‌ها در الزامات حفاظت امن حریم‌خصوصی استفاده می‌کند که مرتبط با پردازش PII است.

۸-۲-۳-۱ مدیریت PII

کلیات. هر سامانه ICT که PII را پردازش می‌کند باید ویژگی‌های پایه معینی برای مدیریت PII در سامانه ICT داشته باشد. این موارد شامل ورود، دسترسی، روزآمد و حذف PII است. در هنگام نیاز، سامانه ICT باید قادر به پشتیبانی از فرایند مستمری باشد که جمع‌آوری و پردازش PII را در طول عمر سامانه فراهم می‌آورد.

طرف ارتباط PII. مولفه مدیریت PII سامانه ICT طرف ارتباط PII بر جمع‌آوری و پردازش محلی PII جمع‌آوری‌شده از طرف ارتباط PII تمرکز دارد.

کنترل‌کننده PII. مولفه مدیریت PII سامانه ICT کنترل‌کننده PII باید دارای قابلیت تبادل PII با سامانه‌های ICT طرف‌های ارتباط PII (جمع‌آوری PII) و پردازشگرهای PII (برای سپردن پردازش) باشد. با توجه به خط‌مشی حریم‌خصوصی، استفاده از فناوری‌های بهسازی حریم خصوصی مختلف و سایر عوامل ممکن است ابزارهای مدیریت PII موجود در سامانه ICT کنترل‌کننده PII را محدود کند. برای مثال، سامانه ICT کنترل‌کننده PII ممکن است از افزودن یا پیوند دادن PII با سایر اطلاعات ممنوع شده باشد.

پردازشگر PII. مولفه مدیریت PII سامانه ICT پردازشگر PII، PII دریافت‌شده از کنترل‌کننده PII را مدیریت می‌کند.

۸-۲-۳-۲ انتقال PII

کلیات. مولفه انتقال PII مسئول تبادل PII با سامانه‌های ICT از ذینفعان حریم‌خصوصی مختلف است. انتقال PII باید شامل اصالت‌سنجی متقابل و رمزگذاری بین نقاط منبع و مقصد برای حفظ انتقال PII و اطمینان از محرمانگی آن باشد. در این مورد، مولفه انتقال PII باید از اصالت‌سنجی و مولفه‌های رمزگذاری PII استفاده کند.

۸-۲-۳-۳ اعتبارسنجی PII

کلیات. PIIای که در حال پردازش است، باید از نظر دقت داده و درستی قالب، اعتبارسنجی شود. این مولفه باید اطلاعات کافی درباره مدل داده و گستره مقادیر مجاز برای اطلاع‌رسانی به ذینفعان حریم‌خصوصی با استفاده از سامانه ICT درباره خطاهای ممکن در ورود PII را داشته باشد.

طرف ارتباط PII. سامانه ICT طرف ارتباط PII، اعتبارسنجی را بر روی داده جمع‌آوری‌شده از طرف ارتباط PII یا طرف‌های ارتباطی PII که از سامانه ICT استفاده می‌کنند، انجام دهد.

کنترل‌کننده PII. حتی زمانی که سامانه ICT طرف ارتباط PII برای انجام اعتبارسنجی طراحی شده است، سامانه ICT کنترل‌کننده PII باید همان کار را انجام دهد و احتمالا وارسی‌های بیشتری برای اطمینان از دقت داده و درستی قالب PII داشته باشد. سامانه ICT کنترل‌کننده PII ممکن است همچنین وارسی‌های جامعی را برای برون‌نهادها[1] و انحرافات آماری انجام دهد.

پردازشگر PII. سامانه ICT پردازشگر PII باید وظایفی مشابه سامانه ICT کنترل‌کننده PII انجام دهد.

1 - Outliers

۸-۲-۳-۴ مستعارسازی PII

کلیات. مولفه مستعارسازی در لایه PII از طرح مستعارسازی همان طور که در لایه مدیریت دسترسی و هویت توصیف شده استفاده می‌کند تا شناسانه‌هایی را جایگزین کند که هویت درست طرف‌های ارتباط PII را با نام‌های مستعاری که هویت‌های درست را پنهان می‌کند، آشکار کند.

راه دیگر برای دستیابی به اهداف مستعارسازی می‌تواند اغلب از طریق ارائه اطلاعاتی که تاحدودی گمنام هستند، به دست آید.

مثال‌هایی از زمانی که مستعارسازی می‌تواند استفاده شود شامل موارد زیر است:

الف) هویت طرف ارتباط PII برای دستیابی به اهداف پردازش PII موردنیاز نیست؛ و

ب) شناسانه مستعارسازی برای پردازش PII موردنیاز است (به طور مثال، پیوند به چندین پایگاه‌داده یا شناسایی مجدد منفرد).

طرف ارتباط PII. سامانه ICT طرف ارتباط PII، مستعارسازی را در PII ای انجام می‌دهد که قبل از ارسال به سامانه ICT کنترل‌کننده PII جمع‌آوری شده است.

کنترل‌کننده PII. مولفه مستعارسازی در سامانه ICT کنترل‌کننده PII می‌تواند برای پردازش هویت‌های مستعارشده در PII ای که از سامانه ICT طرف ارتباط PII دریافت شده، استفاده شود. در صورتی که طرح مستعارسازی بر پایه کارکرد دو طرفه‌ای باشد که توسط طرف ارتباط PII و کنترل‌کننده PII به اشتراک گذاشته شده است، مورد آخر می‌تواند همچنین در زمان نیاز PII را شناسایی مجدد کند. سامانه ICT کنترل‌کننده PII می‌تواند همچنین از مستعارسازی در PII ای استفاده کند که به سامانه ICT پردازشگر PII ارسال می‌شود. کارکردهای مستعارسازی پارامترشده متفاوت باید زمانی که PII برای بازیگران مختلف آشکار می‌شود استفاده شود.

برای مثال، اگر PII به سامانه‌های ICT چندین پردازشگر PII منتقل می‌شود، کارکردهای مستعارسازی مختلفی باید بر PII داده‌شده به هر پردازشگر جهت کاهش مخاطره تبانی میان پردازشگرها استفاده شود. کنترل‌کننده PII، ثبت پردازشگرهای PII و کلیدهای مستعارسازی مرتبط آنها را نگهداری می‌کند. به‌علاوه، هر رویدادی از افشای PII باید توسط هر دو طرف تراکنش افشا - سامانه‌های ICT کنترل‌کننده PII و پردازشگر PII ثبت شود.

پردازشگر PII. سامانه ICT پردازشگر PII می‌تواند مستعارسازی را در صورتی انجام دهد که توسط کنترل‌کننده PII برای انجام آن ساختار یافته باشد.

۸-۲-۳-۵ مستعارسازی PII

کلیات. فرایند مستعارسازی، PII را دریافت می‌کند و تمامی شناسانه‌های شخصی را حذف می‌کند یا در غیر این صورت به صورت غیرتکراری از طریقی هشدار می‌دهد که طرف ارتباط PII دیگر نمی‌تواند به صورت مستقیم یا غیر مستقیم به تنهایی توسط کنترل‌کننده PII یا با همکاری طرف دیگر شناسایی شود.

مثال‌هایی از فنون مستعارسازی شامل موارد زیر است:

الف- تعمیم PII، کاهش دقت اطلاعات، به طور مثال گروه‌بندی مقادیر پیوسته یا جایگزینی مقادیر قطعی با عبارات طولانی‌تر.
ب- توقیف PII – حذف کل یک سابقه یا بخش‌های معینی از سوابقی که قابل شناسایی ارائه می‌شوند.
پ- ایجاد اختلال در PII – اضافه کردن مقادیر کوچک مختلف به فیلدهای اطلاعاتی منتخب به طور مثال وزن، ارتفاع یا سن؛
ت- معاوضه PII – تبادل فیلدهای معین PII از یک سابقه با همان فیلد PII از سابقه مشابه (به طور مثال معاوضه کدهای پستی از دو سابقه)؛ و
ث) جایگزینی PII با مقدار میانگین – جایگزینی هر مقدار PII با سوابق شاخه‌ای با مقدار میانگین برای کل گروه PII.
فنونی وجود دارد که احتمال شناسایی مجدد طرف ارتباط PII مربوط به داده را محتمل می‌سازد. چنین فنونی برای برنامه کاربردی در این مولفه مناسب نیستند. به‌علاوه، فنون مستعارسازی وجود دارد که ممکن است به طور تصادفی PII را طوری تغییر دهد که طرف ارتباط PII دیگری را شناسایی کند. کیفیت فن مستعارسازی استفاده‌شده باید قبل از شامل شدن در طراحی سامانه ICT، ارزیابی شود.
PII می‌تواند توسط سامانه ICT هر ذینفع حریم‌خصوصی قبل از انتقال به سامانه‌های ICT دیگر ذینفعان حریم‌خصوصی گمنام شود.

۸-۲-۳-۶ اشتراک‌گذاری مخفی

کلیات. اشتراک‌گذاری مخفی فنی برای توزیع مقادیر PII به صورت مشترک است طوری که هیچ اطلاعاتی درباره مقدار اصلی به صورت منفرد آشکار نشود. اشتراک‌گذاری مخفی می‌تواند برای جمع‌آوری PII جهت کاهش مخاطره نقض حریم‌خصوصی استفاده شود. اشتراک‌گذاری مخفی، حریم‌خصوصی بهتری را در زمان انجام در سامانه ICT طرف ارتباط PII فراهم می‌آورد و همراه با محاسبات چند طرفه امن استفاده می‌شود.
اشتراک‌گذاری مخفی می‌تواند برای کاهش مخاطره حملات داخلی، زمانی که یک طرف با دسترسی اشتراک‌گذاری مقدار PII نتواند مقدار اصلی را از آن فرا بگیرد، استفاده شود. این کار حملات داخلی را به طور چشمگیری پیچیده‌تر می‌کند. برای نتایج بهینه، اشتراک‌گذاری مخفی نیاز دارد که بیش از یک نمونه از هر بازیگر در سامانه وجود داشته باشد. هر نمونه باید تعداد محدودی از اشتراک‌ها را ذخیره و پردازش کند.
طرف ارتباط PII. سامانه ICT طرف ارتباط PII می‌تواند اشتراک‌گذاری مخفی را در PII جمع‌آوری شده از طرف‌های ارتباطی PII انجام دهد. سپس اشتراک‌های منتج شده به کنترل‌کننده‌های PII منتقل می‌شوند.
کنترل‌کننده PII. سامانه ICT کنترل‌کننده PII می‌تواند از اشتراک‌گذاری مخفی برای پردازش PII مشترک محرمانه که از سامانه ICT طرف ارتباط PII دریافت شده است استفاده کند یا اشتراک‌گذاری مخفی را در PII آشکار قبل از این که به سامانه ICT پردازشگر PII انتقال یابد، انجام دهد.
پردازشگر PII. سامانه ICT پردازشگر PII می‌تواند از اشتراک‌گذاری مخفی برای یک یا دو هدف استفاده کند اولین هدف ذخیره یا بارگذاری PII مشترک محرمانه قبل از پردازش است. در این مورد، PII در فرم مشترک محرمانه ذخیره می‌شود، اما قبل از پردازش نوسازی می‌شود. دومین هدف استفاده از آن همراه با

محاسبه چندطرفه امن است. در این مورد، احتمال انجام محاسبات به طور مستقیم در PII مشترک محرمانه وجود دارد.

۸-۲-۳-۷ رمزگذاری PII

کلیات. مولفه‌های رمزگذاری PII باید سازوکارهایی را برای رمزگذاری PII قبل از ذخیره‌سازی فراهم کند. طراحی سامانه ICT باید شامل تعریف این که کدام PII ذخیره‌شده نیاز به رمزگذاری دارد باشد. بسته به الزامات حفاظت امن حریم‌خصوصی، کلیدهای رمزگذاری می‌توانند بین سامانه‌های ICT به اشتراک گذاشته شوند در نتیجه هر یک از آنها می‌توانند PII را رمزگشایی کرده و به طور مناسب به آن دسترسی داشته باشد. اگر فن محاسباتی امن که مناسب پردازش PII رمزگذاری‌شده است استفاده شود، الزامی به رمزگشایی اطلاعات برای پردازش نیست.

خدمات مولفه شامل مدیریت کلید، رمزگذاری PII با پایگاه‌های داده و رمزگذاری PII ذخیره‌شده همچون پرونده‌های پشتیبان و بایگانی‌ها است.

رمزگذاری PII می‌تواند برای حفظ PII ذخیره‌شده استفاده شود. این کار می‌تواند برای دو هدف انجام شود. اول، می‌توان PII رمزگذاری‌شده را برای جلوگیری از دسترسی غیرمجاز به آن ذخیره کرد. در صورتی که به پردازش نیاز داشته باشد، با کلید رمزگشایی مرتبط رمزگشایی می‌شود. رمزگذاری PII، مخاطره امنیت نقض داده از پشتیبان‌ها را کاهش می‌دهد. این کلیدها که برای رمزگذاری استفاده می‌شوند باید جد از PII رمزگذاری‌شده ذخیره شوند.

به‌علاوه، PII می‌تواند برای آماده‌سازی جهت پردازش در شکل رمزگذاری با استفاده از فنون محاسباتی امن به طور مثال رمزگذاری هم‌ریختی (هوموومورفیک)[1] رمزگذاری شود.

در همه موارد، طول‌های کلید مناسب باید طوری تعریف شود که منابع محاسباتی جاری و در آینده نزدیک نتوانند آن کلید را بشکنند.

۸-۲-۳-۸ استفاده PII

کلیات. برای استفاده از PII در محاسبات یا تحلیل‌ها، سامانه ICT بازیگر باید مولفه استفاده PII را پیاده‌سازی کند. این مولفه، منطق کسب‌وکار پردازش PII را پیاده‌سازی می‌کند. یادآوری می‌شود که برخی فرانامه‌های استفاده PII می‌توانند با استفاده از محاسبات امن برای کاهش مخاطره نشت PII پیاده‌سازی شوند.

۸-۲-۳-۹ محاسبات امن

کنترل‌کننده PII و پردازشگر PII، محاسبات امن می‌توانند برای ایجاد امکان پردازش به کنترل‌کننده‌های PII و پردازشگرهای PII بدون داشتن دسترسی به مقادیر ورودی خام استفاده شود. در عوض، فنون محاسبات امن، محاسباتی در PII انجام می‌دهد که توسط فناوری‌های بهسازی حریم خصوصی به طور مثال رمزگذاری یا اشتراک‌گذاری مخفی انتقال داده شده است.

1 - Homomorphic

زیرمجموعه‌ای از فنون محاسبات امن که به عنوان محاسبه چندطرفه امن شناخته می‌شود فنی است که به موجب آن طرف‌های چندگانه می‌توانند به صورت مشترک برخی مقادیر مبتنی بر اطلاعات منفرد نگه‌داشته‌شده طرف‌های محرمانه اطلاعات را محاسبه کند بدون این که موارد محرمانه در حین پردازش برای دیگری آشکار شود. برای حفظ بهینه در مقابل نقض‌های حریم‌خصوصی، محاسبه چندطرفه امن باید چندین کنترل‌کننده PII یا پردازشگر PII و سامانه ICT را با اطلاعات امن مرتبط در بر گیرد.

تا زمانی که PII جهت پردازش طرف به شکلی شفاف فراهم نشده است، محاسبه امن می‌تواند مخاطره نشت‌های PII را از سامانه ICT بازیگر کاهش دهد.

۸-۲-۳-۱۰ مدیریت پرسمان[1]

کلیات. مولفه مدیریت پرسمان سامانه ICT کنترل‌کننده PII و/یا پردازشگر PII برای پالایش پرسمان‌های ورودی مستقر می‌شود. برای مثال، خدمت می‌تواند از پاسخ به یک پرسمان آماری در صورتی که ورودی‌های کافی برای آن پرسمان وجود نداشته باشد، امتناع کند. درحالی که امتناع از پاسخ به پرسمان همچنان برخی اطلاعات را برای ذینفع حریم‌خصوصی که پرسمان را می‌سازد، فراهم می‌کند، این فن باید همچنان در فرانامه‌های معین مورد توجه قرار گیرد.

مدیریت پرسمان فنی ویژه است که در برنامه‌های کاربردی داده کاوی برای کمینه کردن پردازش PII استفاده می‌شود. این فن، ارائه خدمات تحلیل PII را تسهیل می‌کند درحالی که خطر سوء استفاده از PII و به خطر انداختن دقت الگوریتم‌های داده کاوی را به همراه ندارد. فرایند مدیریت پرسمان باید برای اطمینان از پردازش فقط یک PII کافی در پردازش‌های درگیر، استفاده شود.

روش‌های مدیریت پرسمان شامل محدود کردن اندازه نتایج پرسمان، کنترل هم‌پوشانی در میان پرسمان‌های پی در پی، حفظ دنباله‌های ممیزی از تمامی پرسمان‌های پاسخ داده شده و وارسی ثابت برای خطرهای احتمالی، توقیف سلول‌های PII هستارهای اندازه‌های کوچک و خوشه‌ای به جمعیت‌های هسته‌ای انحصاری متقابل است.

۸-۲-۳-۱۱ سیاهه PII[2]

کلیات. مولفه سیاهه PII مروری بر PII ذخیره‌شده در سامانه ICT فراهم می آورد. اطلاعات از سامانه دسته‌بندی PII باید برای دسته‌بندی مقادیر PII ذخیره‌شده در سامانه استفاده شود. سامانه مدیریت هویت باید برای تعیین طرف ارتباط PII مربوط به یک قلم خاص PII استفاده شود. مولفه سیاهه PII باید قادر به ارائه ذینفع حریم‌خصوصی با استفاده از سامانه ICT با دست کم متریک‌های زیر باشد:

الف- مقدار PII در سامانه (تعداد سوابق، فراداده در مورد سوابق)؛ و

ب- تعداد طرف‌های ارتباط PII که اطلاعات را فراهم آورده اند.

بسته به الزامات حفاظت امن حریم‌خصوصی، این مولفه می‌تواند اطلاعات بیشتری را همچون فهرست طرف‌های ارتباط PII فراهم کند.

---

1 - Query

2 - Inventory

مولفه سیاهه PII، کارکرد مشابهی در همه بازیگران دارد – برای فراهم کردن مروری بر این که PII به چه میزان به صورت محلی حفظ می‌شود و طرف‌های ارتباط PII مرتبط کدام هستند. سامانه ICT کنترل‌کننده PII باید این قابلیت کارکردی را با حفظ سوابق پردازش PII تحت سامانه‌های ICT پردازشگرهای PII گسترش دهد. این کار باید با همکاری مولفه‌های مدیریت PII و بایگانی مرتبط در سامانه ICT پردازشگر PII انجام شود.

۸-۲-۳-۱۲ افشای PII

کنترل‌کننده PII. مولفه افشای PII مسئول مدیریت هر افشای PII توسط کنترل‌کننده PII است. این مولفه ممکن است شامل آماده‌سازی PII قبل از ترک سامانه ICT کنترل‌کننده PII باشد. برای مثال، کنترل‌کننده PII می‌تواند PII را با استفاده از مولفه مرتبط قبل از ارسال آن به یک پردازشگر PII، مستعار یا گمنام کند. افشای PII اغلب نیازمند استفاده از مولفه انتقال PII است.

در صورتی که مستعارسازی در حین افشای PII استفاده شود، ثبت آن باید همچنین شامل توضیحی از کارکرد مستعارسازی استفاده‌شده برای افشای PII باشد. در این مورد، کارکردهای مستعارسازی متفاوتی باید در حین افشا استفاده شود تا امکان پیوند پایگاه‌های داده افشاشده با یکدیگر را کاهش دهد و شناسانه مشابه به نام مستعار مشابه نگاشت نشود.

پردازشگر PII. PII می‌تواند توسط سامانه ICT پردازشگر PII به روشی مشابه در سامانه ICT کنترل‌کننده PII افشا شود. هر افشا باید مطابق با جهت‌های کنترل‌کننده PII انجام شود.

۸-۲-۳-۱۳ بایگانی و ابقای PII

کلیات. زمانی که PII در استفاده فعال قرار ندارد و طبق زمانبندی باید بایگانی شود، PII باید برای بایگانی آماده شود. مولفه بایگانی و ابقا باید اطمینان حاصل کند که بایگانی به اندازه کافی حفاظت شده است و از روال‌های بایگانی و ابقا پیروی می‌شود. رمزگذاری، اشتراک‌گذاری مخفی و مستعارسازی می‌تواند برای حفظ PII بایگانی‌شده از پردازش غیرمجاز استفاده شود. مهم است که بدانیم کدام کلید رمزگذاری، طرح اشتراک‌گذاری مخفی یا طرح مستعارسازی در حین پردازش برای بازیابی بعدی PII مورد استفاده قرار گرفته است.

در صورتی که مدت زمان ابقای PII گذشته باشد، این مولفه باید مستعارسازی یا حذف امن PII را از سامانه زمانبندی کند.

۸-۲-۳-۱۴ واقعه‌نگاری ممیزی[1]

مولفه واقعه‌نگاری ممیزی باید هر تراکنش انجام‌شده در PII را ثبت کند. این مولفه باید با هر مولفه دیگر یکپارچه باشد تا بتواند همه فعالیت‌های مرتبط را ثبت کند.

هویت بازیگر یا بازیگرانی که به PII دسترسی دارند، تراکنش‌های PII را راه‌اندازی می‌کند یا نتایج PII را از تراکنش‌های PII دریافت می‌کند باید در واقعه‌نگاری تراکنش ثبت شود. این کار مستلزم یکپارچگی

1 - Audit logging

واقعه‌نگاری ممیزی با پودمان‌های[1] اصالت‌سنجی، مجازشناسی و لایه PII است. برای جلوگیری از مداخله با ورودی‌های ثبت باید از فنون واقعه‌نگاری امن استفاده شود.

ارتباط بین اصول حریم‌خصوصی و مولفه‌ها در لایه PII

جدول ۳ مثالی از نگاشت اصول حریم‌خصوصی ISO/IEC 29100 به مولفه‌های لایه PII را نشان می‌دهد. ’X‘ در جدول نشان‌دهنده ارتباط بین مولفه لایه و یک اصل است. اگرچه این ارتباط، تنها به عنوان یک مثال نشان داده شده است.

1 - modules

جدول ۳ – مثال ارتباط بین اصول حریم‌خصوصی و مولفه‌ها در لایه PII

اصول / مولفه‌ها	رضایت و انتخاب	قانونی بودن هدف و ویژگی	محدودیت جمع‌آوری	کمینه‌سازی داده	استفاده، ابقا و محدودیت افشا	دقت و کیفیت	بازبودن، شفافیت و اطلاع	مشارکت و دسترسی انفرادی	پاسخگویی	کنترل‌های امنیت اطلاعات	انطباق
مدیریت PII	X	X	X	X	X		X	X			
انتقال PII	X	X		X	X		X	X			
اعتبارسنجی PII						X					
مستعارسازی PII				X						X	
گمنام‌سازی PII				X						X	
اشتراک‌گذاری مخفی				X						X	
رمزگذاری PII				X						X	
استفاده PII	X	X		X	X	X	X				
محاسبه امن				X						X	
مدیریت پرسمان				X	X					X	
سیاهه PII				X	X		X		X		
افشای PII	X	X		X	X		X				
بایگانی و ابقای PII	X	X		X	X		X				
واقعه‌نگاری ممیزی									X	X	

۳-۸ دیدگاه بازیگر

دیدگاه بازیگر نشان می‌دهد که چگونه مولفه‌های چارچوب کاری معماری ISO/IEC 29101 در سامانه‌های ICT ذینفع حریم‌خصوصی خاص مستقر هستند. برای هر بازیگر، این دیدگاه زیرمجموعه‌ای از مولفه‌هایی را ارائه می‌دهد که مناسب استقرار در سامانه ICT همان بازیگر است. توسعه‌دهنده از این دیدگاه برای تصمیم‌گیری این که کدام مولفه‌ها باید در معماری سامانه ICT ذینفع حریم‌خصوصی شامل شود، استفاده می‌کند.

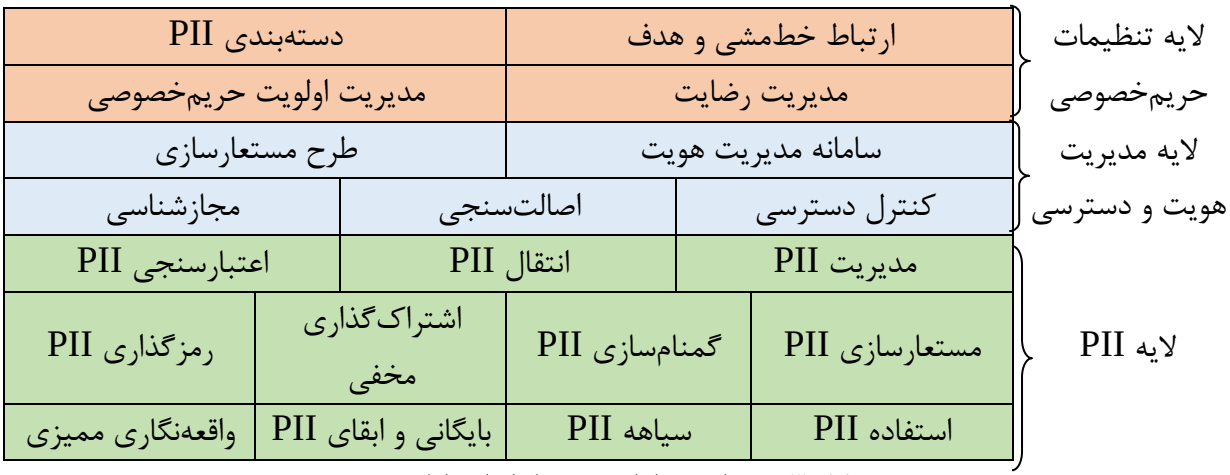
این دیدگاه، هیچ مولفه‌ای را در سامانه ICT ذینفع دیدگاه خاص اجباری نمی‌کند.

۸-۳-۱ سامانه ICT طرف ارتباط PII

سامانه ICT طرف ارتباط PII بر ارتباط خط‌مشی حریم‌خصوصی با ساماندهی مدیریت رضایت و جمع‌آوری PII تمرکز دارد اما به آن محدود نمی‌شود.

از آنجایی که طرف ارتباط PII طرفی است که PII را به سامانه جامع ارائه می‌کند، سامانه ICT که توسط طرف ارتباط PII استفاده می‌شود باید شامل مولفه‌هایی برای امن کردن PII در حین جمع‌آوری باشد. این فنون ممکن است شامل مستعارسازی، گمنام‌سازی، رمزگذاری و اشتراک‌گذاری مخفی باشد اما به آنها محدود نمی‌شود.

معماری سامانه ICT طرف ارتباط PII در شکل ۳ ارائه شده است.



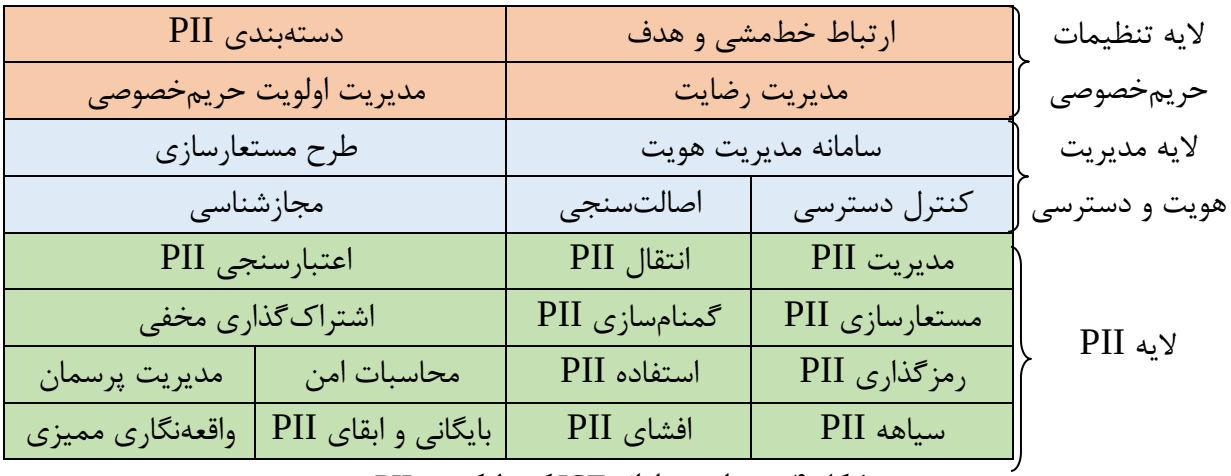
شکل ۳- معماری سامانه ICT طرف ارتباط PII

۸-۳-۲ سامانه ICT کنترل‌کننده PII

سامانه ICT کنترل‌کننده PII باید با خط‌مشی حریم‌خصوصی دیگر شرکا ارتباط داشته باشد. به‌علاوه، کنترل‌کننده PII باید جمع‌آوری و پردازش کل PII را مدیریت کند. سامانه ICT کنترل‌کننده PII باید PII را مبتنی بر آخرین خط‌مشی، الزامات حفاظت امن حریم‌خصوصی و هر اولویت حریم‌خصوصی که از طرف ارتباط PII جمع‌آوری شده است، پردازش کند. کنترل‌کننده PII باید اطمینان حاصل کند که مولفه‌های تنظیمات حریم‌خصوصی به طور دائم شامل اطلاعات به‌روز در مورد خط‌مشی و اهداف است.

به‌علاوه، کنترل‌کننده PII پردازش PII توسط پردازشگرهای PII را مدیریت می‌کند. این کار شامل نظارت و مسئولیت اجرای خط‌مشی‌های حریم‌خصوصی مناسب و هر محدودیت رضایت و اولویت‌های حریم‌خصوصی است که از طرف ارتباط PII جمع‌آوری شده است. این کار نیاز دارد تا کنترل‌کننده PII این اطلاعات را به پردازشگرهای PII ابلاغ کند، رفتار آنها را پایش کند و در صورتی که محدودیت‌ها و اولویت‌ها با یکدیگر هماهنگ نیستند، اقدام جبرانی انجام دهد.

به‌علاوه، کنترل‌کننده ممکن است فناوری های ارتقا حریم‌خصوصی را همچون مستعارسازی، گمنام‌سازی یا اشتراک‌گذاری مخفی را به کار برد تا احتمال این که سامانه ICT پردازشگر PII بتواند طرف ارتباط PII مرتبط با PII را شناسایی کند را کاهش دهد. شکل ۴ مولفه‌هایی از سامانه ICT کنترل‌کننده PII را نشان می‌دهد.

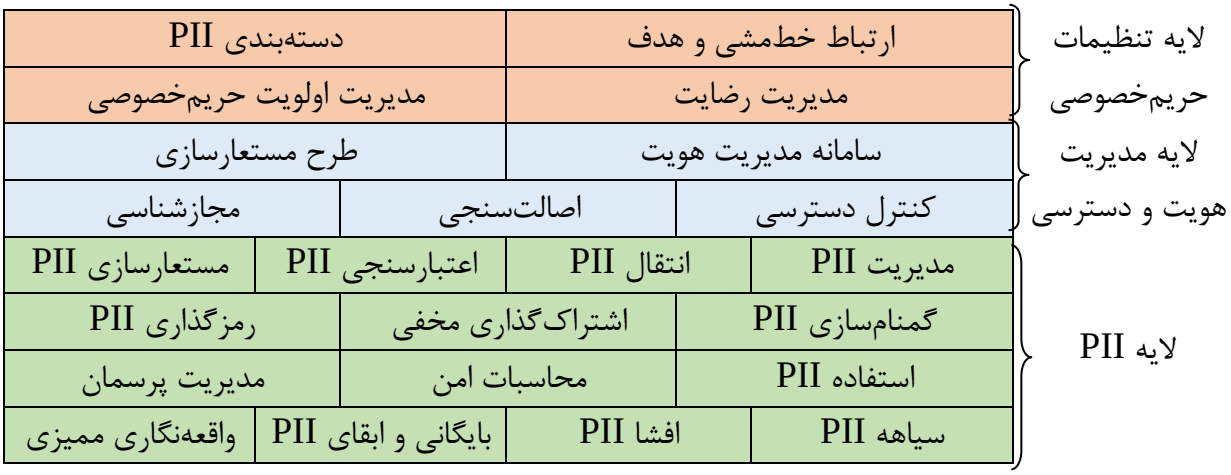


شکل ۴- معماری سامانه ICT کنترل‌کننده PII

۸-۳-۳ سامانه ICT پردازشگر PII

پردازشگر PII از سامانه ICT خود برای پردازش PII مطابق توافق‌نامه با کنترل‌کننده PII استفاده می‌کند. سامانه ICT کنترل‌کننده PII، اطلاعات مرتبط با PII و ضروری برای پردازش آن را تحت خط‌مشی و اولویت‌های حریم‌خصوصی ارسال می‌کند. به‌علاوه، سامانه ICT پردازشگر PII باید قادر به پشتیبانی PII که توسط فناوری‌های ارتقا افزایش حریم‌خصوصی تبدیل شده است، باشد.

اگر یک فناوری بهسازی حریم خصوصی که بازنمایی PII را تغییر نمی‌دهد (برای مثال، مستعارسازی یا گمنام‌سازی) برای حفظ PII استفاده شود، سامانه ICT پردازشگر PII الزامی به داشتن فناوری‌های پردازش خاص ندارد. گرچه، اگر فنون رمزنگاری به طور مثال اشتراک‌گذاری مخفی یا رمزگذاری PII استفاده شود، سامانه ICT پردازشگر PII نیاز دارد تا محاسبه چندطرفه امن یا رمزگشایی PII را مستقر سازد تا قادر به کار با PII باشد. محاسبه چندطرفه امن ممکن است مخاطره کاهش‌یافته یا نقض‌های حریم‌خصوصی را در حین پردازش ارائه کند. برای معماری سامانه ICT پردازشگر PII به شکل ۵ مراجعه کنید.



شکل ۵- معماری سامانه ICT پردازشگر PII

۸-۴ دیدگاه تعاملی

دیدگاه تعاملی توصیف می‌کند که چگونه مولفه‌های مستقر در سامانه‌های ICT از ذینفعان حریم‌خصوصی متفاوت با یکدیگر تعامل می‌کنند. اکثریت مولفه‌هایی که در این چارچوب کاری معماری توصیف شده اند نیاز به اشتراک‌گذاری اطلاعات یا ارتباط میان بازیگران دارند. این بند توصیف می‌کند که کدام مولفه‌ها ممکن است از اشتراک‌گذاری PII یا فراداده میان بازیگران بهره ببرند. توسعه دهنده سامانه ICT می‌تواند از این دیدگاه برای طراحی تعاملات بین سامانه‌های ICT بازیگران منفرد استفاده کند.

یک شکل برای هر لایه مولفه‌های معماری ارائه شده است. این شکل پوشش مولفه‌های میان بازیگران را نشان می‌دهد. در صورتی که مولفه منفرد، بازیگران چندگانه را پوشش دهد، کد داده یا برنامه این مولفه باید میان بازیگران مرتبط به اشتراک گذاشته شود. یادآوری می‌شود که این کار به معنی این نیست که کل PII باید به اشتراک گذاشته شود. اطلاعات باید تنها بر اساس اصول با حداقل اختیار ویژه توزیع شود – در صورتی که بازیگر نیازی به اطلاعات قطعی برای انجام وظایفش نداشته باشد، نباید به این اطلاعات دسترسی داشته باشد.

برای مثال، حتی اگر سامانه ICT پردازشگر PII نیازمند دسترسی به اولویت‌های حریم‌خصوصی طرف ارتباط PII برای درنظرگرفتن آنها باشد، باید تنها به اولویت‌هایی برای آن طرف‌های ارتباطی که PII را ارائه کرده اند دسترسی داشته باشد. کنترل‌کننده PII ممکن است PII را از طرف‌های ارتباط PII چندگانه داشته باشد، اما در صورتی که کنترل‌کننده پردازش را از طرف یک طرف ارتباط PII خاص به یک پردازشگر PII واگذار نکرده است، الزامی برای اشتراک‌گذاری اولویت‌های حریم‌خصوصی مرتبط ندارد. از سوی دیگر، در صورتی که PII از کنترل‌کننده به پردازشگر انتقال داده شود، اولویت‌های حریم‌خصوصی طرف‌های ارتباط PII مرتبط باید برای سامانه ICT پردازشگر PII در دسترس باشند.

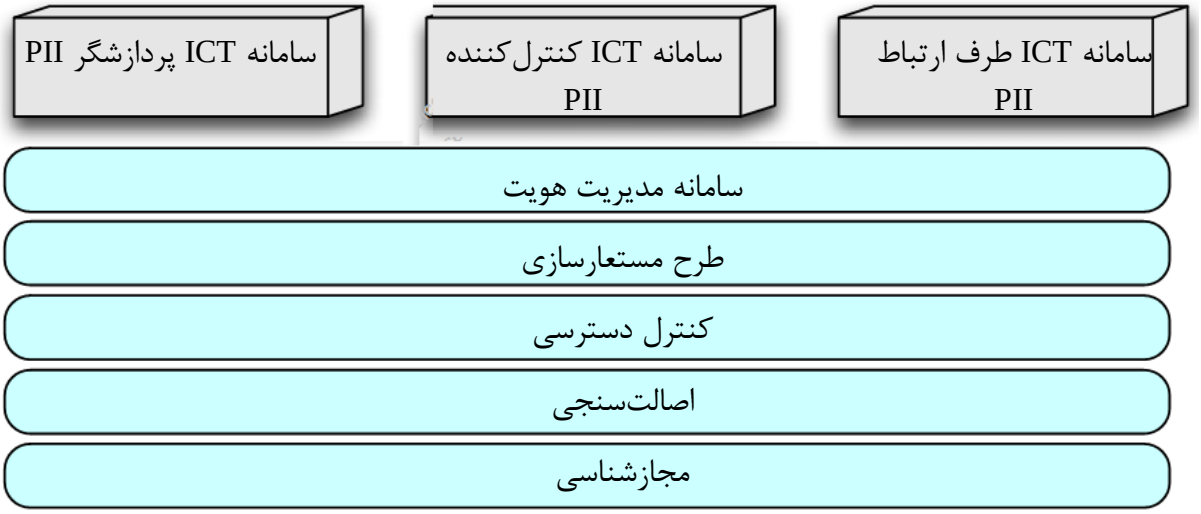
۸-۴-۱ لایه تنظیمات حریم‌خصوصی

لایه تنظیمات حریم‌خصوصی، خدمات و اطلاعات نظارتی همه جوانب پردازش PII را پوشش می‌دهد. بنابراین، باید در سراسر پردازش PII حاضر باشد. شکل ۶ پوشش مولفه‌های تنظیمات حریم‌خصوصی را در بازیگران نشان می‌دهد.

شکل ۶ – استقرار مولفه‌ها در لایه تنظیمات حریم خصوصی

۸-۴-۲ لایه مدیریت هویت و دسترسی

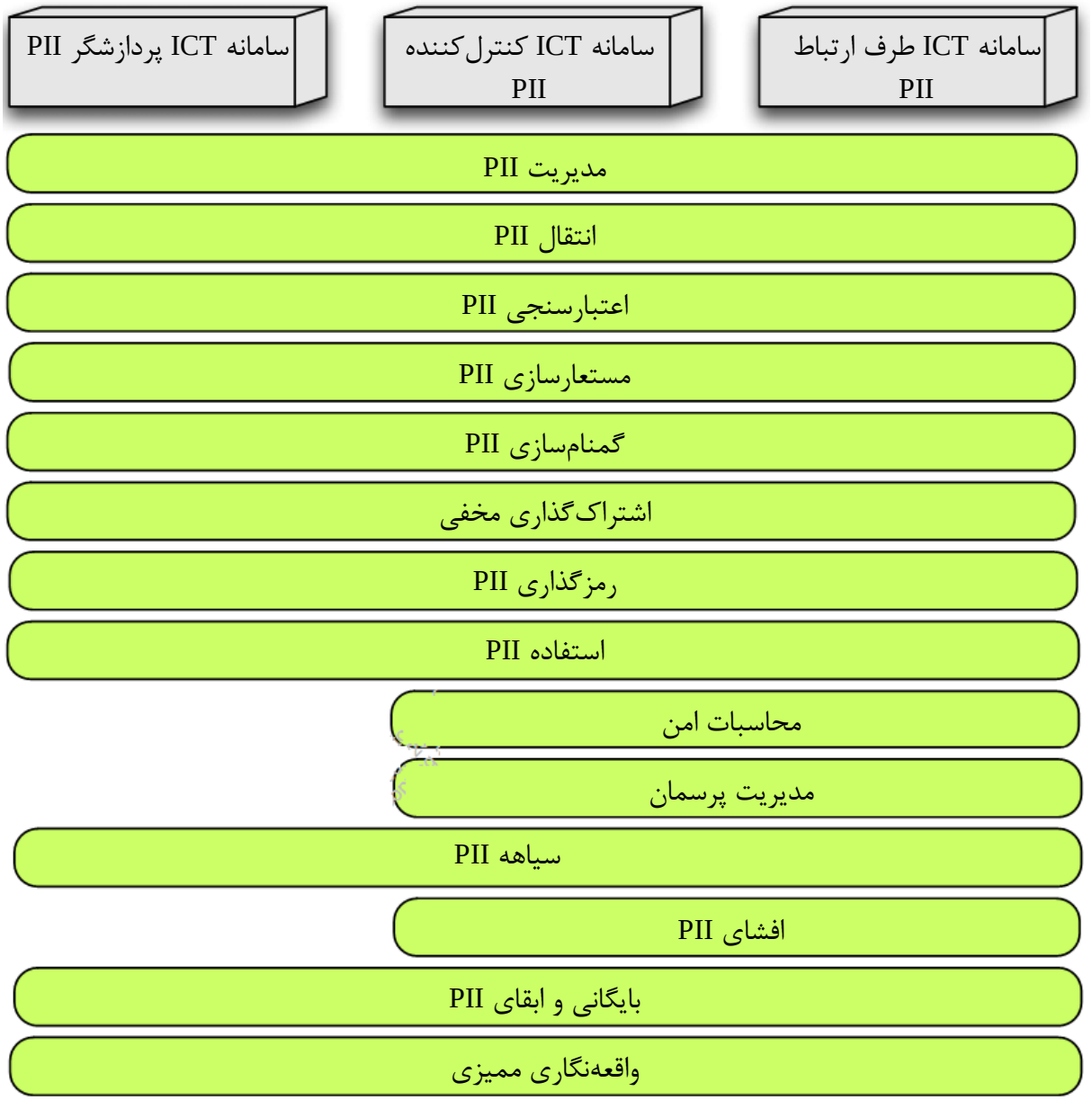
برخی خدمات مدیریت هویت عمومی است و توسط همه بازیگران استفاده می‌شود. با این حال، این به آن معنی نیست که همه بازیگران باید تمام اطلاعات هویت را به اشتراک بگذارند. اصل حداقل اختیار ویژه باید پیروی شود و هر سامانه‌های ICT تنها باید به اطلاعات هویتی که نیاز دارد دسترسی داشته باشد. شکل ۷ استقرار خدمات مدیریت هویت را نشان می‌دهد.



شکل ۷ - استقرار مولفه‌ها در لایه مدیریت هویت و دسترسی

۸-۴-۳ لایه PII

لایه PII همچنین شامل خدمات کلی استفاده‌شده مانند مدیریت PII عمومی و سیاهه PII است. با این حال، باید توجه داشت که خدماتی در این لایه وجود دارد که می تواند برای هر بازیگر مستقر شود، اما بسته به طراحی سامانه، ممکن است به نفع باشد که تنها برای برخی از بازیگران مستقر شود. به عنوان مثال، اشتراک گذاری مخفی، زمانی که به طور مستقیم در سامانه ICT طرف ارتباط PII مستقر شده است، بیشترین تاثیر را دارد. اما، همچنین می تواند توسط سامانه ICT کنترل‌کننده PII قبل از عبور PII به سامانه ICT پردازشگر PII انجام شود. شکل ۸ نشان می‌دهد که چگونه مولفه‌های PII مرتبط، می‌توانند مستقر شوند.



شکل ۸- استقرار مولفه‌ها در لایه PII

پیوست الف

(اطلاعاتی)

مثال‌های ملاحظات PII مرتبط سامانه ICT

الف – ۱ مقدمه

موارد زیر مثال‌های ملاحظات PII مرتبط معماری سامانه ICT است. این ملاحظات به مولفه‌های معماری با هر مولفه که به یک یا چند ملاحظه نگاشت شده باشد، پیوند خورده است. توسعه‌دهندگان باید ملاحظات ویژه‌ای را برای برنامه‌های کاربردی شناسایی کنند و اطمینان حاصل کنند که طراحی معماری سامانه ICT شامل مولفه‌هایی است که ملاحظات را نشان می‌دهد.

در مثال زیر، ملاحظات سطح بالا به تعدادی ملاحظه فرعی تقسیم شده است. ملاحظات فرعی یکه در اینجا توصیف شده اند به عنوان یک تصویر ارائه شده است و لزوما کامل نیستند. توسعه‌دهندگان باید ملاحظات و ملاحظات فرعی مناسب را برای برنامه کاربردی از طریق فرایند تحلیلی تعیین کنند.

الف – ۲ به دست آوردن و ابلاغ رضایت

رضایت توسط طرف ارتباط PII برای پردازش PII آن، جنبه مهمی از مدیریت آن PII است. متعاقباً، معماری سامانه ICT باید شامل عناصری باشد که مدیریت آن رضایت را فعال می‌کند، علاوه بر آنهایی که اطمینان دارند محدودیت‌هایی به طور مثال رضایت باید در نظر گرفته شود.

رضایت به اهداف اعلام‌شده از استفاده اختصاص دارد و باید به صورت داوطلبانه از طرف ارتباط PII بر پایه اطلاعات فراهم‌شده توسط کنترل‌کننده PII در مورد آن اهداف و تمامی هستارهایی (کنترل‌کننده و پردازشگر (های) PII) که آن را پردازش می‌کنند به دست آید، که شامل حوزه قضایی قانونی[1] که به آنها اعمال می‌شود است.

در برخی موارد، قانون قابل کاربرد ممکن است، استثنائاتی را در جایی تعریف کند که پردازش PII بدون رضایت طرف ارتباط PII ممکن است مجاز باشد (به طور مثال در ارتباط با بررسی قانونی). قوانین مرتبط باید برای شناسایی تمامی چنین استثنائات و مفاد مربوط به رضایت بررسی شوند.

در صورتی که طرف ارتباط PII به طور قانونی شایسته نباشد (به طور مثال، طرف ارتباط PII یک کودک باشد)، رضایت ممکن است همچنین توسط یک نماینده مجاز قانونی فراهم شود (به طور مثال پدر و مادر، ولی، وکیل). نماینده، PII طرف ارتباط PII را به جای خود طرف ارتباط PII، ارائه می‌کند و اطلاعات و محدودیت‌های رضایت مرتبط در استفاده را تعیین و ارائه می‌کند و PII را به دیگر طرف‌ها از سوی طرف ارتباط PII انتقال می‌دهد. PII و اطلاعات استفاده و رضایت مرتبط باید توسط نماینده به صورت محرمانه نگهداری شود.

1 - Legal

نمایندگان باید اشخاص قابل اعتمادی باشند که جهت رساندن بهترین سود به کارخواهان عمل می‌کننـد. در رویداد نقض اعتماد مشاهده‌شده توسط نماینده، سوگندهای قانونی ممکن است کاملا به طور خـاص محـدود به نمایندگانی باشد که رابطه نزدیکی با طرف ارتباط PII دارند (به طور مثال پدر و مادر یا ولی). در مـواردی که نمایندگان حرفه ای هستند (به طور مثال وکلا) که برای اقدام از سوی طـرف‌هـای ارتبـاط PII منصـوب شده‌اند ممکن است برای مقابله با نمایندگانی که موفق به حمایت از وظیفه خود در اعتمادسازی نشده‌اند بـه تحریم‌های قانونی و حرفه‌ای متوسل شوند.

برخی ملاحظات مرتبط به شرح زیر است:

الف- به دست آوردن رضایت از طرف ارتباط PII یا نماینده؛

ب- انتقال امن و ثبت اطلاعات رضایت؛

پ- اجازه بازگشت یا تغییر رضایت؛

ت- اطلاعات مرتبط با رضایت با PII؛

ث- ثبت برنامه کاربردی رضایت؛ و

ج- واکنش به صرف نظر کردن و اصلاح رضایت داده‌شده قبلی.

در مواردی که طرف ارتباط PII رضایتی را برای PII جهت جمع‌آوری و پردازش ندارد، ممکن است لازم باشد چیدمان‌های جایگزینی که درگیر PII نیست انجام شود. در جایی کـه چیـدمان‌هـای جـایگزین در دسـترس نیست ممکن است لازم باشد طرف ارتباط PII از استفاده خدمت، منع شود.

الف – ۳ ابلاغ هدف جمع‌آوری PII

کنترل‌کنندگان PII، PII را برای هدف خاصی جمع‌آوری می‌کند. اطلاعات در مورد این اهداف باید به طـرف ارتباط PII در حین تعاملات در زمان نیازمندی به رضایت ارائه شود.

اطلاعات در مورد هدف پردازش باید با کنترل‌کننده PII یا پردازشگرهای PII در زمـانی کـه PII انتقـال داده می‌شود در ارتباط باشد (به طور مثال برچسب زدن PII بـا اهـداف آن قبـل از انتقـال). بـا ایـن روش، همـه کنترل‌کنندگان PII و پردازشگرهای PII، هدف و محدودیت‌های پردازش مجاز را می دانند.

حفظ پردازش با محدودیت‌های هدف اصلی می‌تواند با ابزارهای سـازمانی کسـب شـود. بـه طـور جـایگزین، فناوری‌های بهسازی حریم خصوصی همچون مدیریت پرسمان می‌توانند برای اجرای محدودیت‌ها در پردازش PII استفاده شوند.

برخی ملاحظات مرتبط برای نگهداری و ابلاغ اطلاعات سامانه ICT در مورد هدف جمـع‌آوری PII بـه شـرح زیر است:

الف- وارد کردن و روزآمد اطلاعاتی که هدف (های) جمع‌آوری، استفاده و انتقال PII را توصیف می‌کند؛

ب- انتقال و ارائه اطلاعاتی که هدف (های) جمع‌آوری PII را در محدوده سامانه ICT توصیف می‌کند؛

پ- اطلاعات مربوط به هدف (های) جمع‌آوری با PII مرتبط؛ و

ت- اطمینان از این که تمامی پردازش‌های بیشتر در محدوده هدف ارائه‌شده، وجود دارد.

الف – ۴ پردازش PII امن

توسعه‌دهندگان سامانه ICT باید ماهیت و گستره دسترسی مجاز به PII با ملاحظات را داشته باشند. هرچه بیشتر PII مورد دسترسی قرار می‌گیرد و افراد بیشتری حقوق دسترسی به PII را داشته باشند، احتمال نقض‌های حریم‌خصوصی بیشتری وجود دارد.

عامل دیگری که با در نظر گرفته شود، سطح کنترل مستقیم کنترل‌کننده PII یا پردازشگر PII در PII در حال پردازش است. برای مثال، در صورتی که PII در سامانه ICT کنترل‌کننده PII یا پردازشگر PII راه دور در دسترس است، آن بازیگر باید سطح مخاطره بالاتری را به PII تخصیص دهد.

ملاحظات برای انتقال PII و فرایندهای ذخیره‌سازی باید حداقل دسته‌های زیر را پوشش دهد:

الف- جمع‌آوری و اصلاح PII؛

ب- مجازشناسی انتقال‌های PII؛

پ- انتقال اصالت‌سنجی‌شده و محرمانه PII؛

ت- ذخیره‌سازی PII؛

ث- اطمینان از دقت PII؛ و

ج- استقرار کنترل‌های حریم‌خصوصی بیشتر و فناوری‌های بهسازی حریم خصوصی که توسط الزامات حفاظت امن حریم‌خصوصی پیشنهاد می‌شوند.

الف – ۵ طبقه‌بندی و کنترل PII

مدل‌های جریان پردازش PII باید به عنوان مولفه کاملی از ارزیابی مخاطره حریم‌خصوصی توسعه داده شود. نمودار جریان پردازش PII نباید تنها نواحی را نشان دهد که PII جمع‌آوری، منتقل، استفاده، ذخیره یا نشان داده شده است اما باید نواحی را نشان دهد که در آنها PII حساس پردازش می‌شود و به عنوان یک پیشامد، نیازمند پیاده‌سازی سنجه‌های حفاظت امن قوی‌تر است.

طبقه‌بندی داده در PII و غیر PII در جایی که PII حساس پردازش می‌شود (به طور مثال داده‌های شخصی در حوزه سلامت، قومیت و غیره) کمینه الزامات است. چنین داده‌هایی باید با سنجه‌های محافظانه‌تر مطابق با قوانین مرتبط باشد.

طبقه‌بندی و کنترل ملاحظات در محدوده سامانه ICT باید شامل موارد زیر باشد:

الف- تعیین این که کدام داده PII است و طبقه‌بندی PII؛

ب- تعیین تعداد بازیگران PII؛

پ- تعیین مقدار و حساسیت PII؛ و

ت- کنترل انتقال‌ها و رونوشت‌های داخلی PII؛

الف-۶ محاسبه و ممیزی عملیات PII

تراکنش‌های در ارتباط با PII باید در یک پایگاه‌داده تراکنش PII محاسبه شود. محاسبه باید شامل ثبت پردازش PII و هر خطایی باشد که روی می‌دهد و می‌تواند سبب به خطر افتادن محرمانگی یا یکپارچگی PII

باشد. سوابق محاسباتی باید ممیزی‌های مستقل دوره‌ای برای وارسی نقض‌های بالقوه محرمانگی، یکپارچگی یا هر دسترسی غیرمجاز یا رفتار غیرمجاز را شامل شود.

ملاحظات مربوط به قابلیت ممیزی در عملیات PII شامل موارد زیر است:

الف- واقعه‌نگاری امتیاز، اصلاح و لغو رضایت؛

ب- واقعه‌نگاری ذخیره‌سازی و انتقال PII؛

پ- واقعه‌نگاری پردازش PII حساس؛ و

ت- واقعه‌نگاری انتقال‌های PII.

الف–۷ بایگانی و امحای PII

زمانی که PII دیگر مورد نیاز نباشد، باید امحا شود. روال‌های امحا باید اطمینان حاصل کنند که احتمال بازیابی PII از رسانه استفاده‌شده برای ذخیره‌سازی آن وجود ندارد.

ملاحظات مربوط به بایگانی و امحای صحیح PII شامل موارد زیر است:

الف- پشتیبان‌گیری امن PII؛ و

ب- فنون امحای PII امن.

جدول الف-۱، جدول الف-۲ و جدول الف-۳ نگاشت تطبیقی بین ملاحظات مثال و مولفه‌های لایه‌های معماری ISO/IEC 20101 را نشان می‌دهد. 'X' در جدول نشان‌دهنده ارتباط بین مولفه لایه و یک اصل است. گرچه این ارتباط، تنها به عنوان یک مثال نشان داده شده است.

جدول الف-۱ مثال ارتباط بین ملاحظات و مولفه‌ها در لایه تنظیمات حریم خصوصی

ملاحظات / مولفه‌ها	به دست آوردن و ساماندهی رضایت	نگهداری اطلاعات هدف	ذخیره‌سازی و انتقال PII امن	پردازش PII امن	طبقه‌بندی و کنترل PII	دسترس پذیری عملیات PII	بایگانی و امحای PII
ارتباط خط‌مشی و هدف	X	X	X	X		X	
دسته‌بندی PII			X	X	X	X	X
مدیریت رضایت	X				X	X	
مدیریت اولویت حریم‌خصوصی	X	X	X	X		X	X

جدول الف-۲ مثال ارتباط بین ملاحظات و مولفه‌ها در لایه مدیریت هویت و دسترسی

اصول / مولفه‌ها	به دست آوردن و ساماندهی رضایت	نگهداری اطلاعات هدف	ذخیره‌سازی و انتقال PII امن	پردازش PII امن	طبقه‌بندی و کنترل PII	دسترس پذیری عملیات PII	بایگانی و امحای PII
سامانه مدیریت هویت	X		X		X	X	X
طرح مستعارسازی			X				
کنترل دسترسی			X	X		X	
اصالت‌سنجی			X	X		X	
مجازشناسی			x	X		X	

جدول الف-۳ مثال ارتباط بین ملاحظات و مولفه‌ها در لایه PII

اصول / مولفه‌ها	به دست آوردن و ساماندهی رضایت	نگهداری اطلاعات هدف	ذخیره‌سازی و انتقال PII امن	پردازش PII امن	طبقه‌بندی و کنترل PII	دسترس پذیری عملیات PII	بایگانی و امحای PII
مدیریت PII			X		X		X
انتقال PII			X		X		
اعتبارسنجی PII				X			
مستعارسازی PII			X			X	
گمنام‌سازی PII			X			X	
اشتراک‌گذاری مخفی			X				
رمزگذاری PII			X				X
استفاده PII				X			
محاسبه امن				X			
مدیریت پرسمان				X			
سیاهه PII					X	X	X
افشای PII					X	X	
بایگانی و ابقای PII			X				
واقعه‌نگاری ممیزی					X	X	X

الف-۸ ارتباط با اصول حریم‌خصوصی

جدول الف-۴ نگاشت تطبیقی بین اصول ISO/IEC و ملاحظات سطح بالا در این پیوست را نشان می‌دهد.

پیوست ب

(اطلاعاتی)

سامانه تجمیع PII با محاسبه امن

ب-۱ مقدمه

این بند، مثال معماری برگرفته‌شده از چارچوب کاری معماری عمومی را ارائه می‌کند. این معماری از فناوری‌های بهسازی حریم خصوصی برای کمینه کردن افشای PII استفاده می‌کند. یادآوری می‌شود که این مثال، تنها برای اهداف تصویری است. هر کاربردی، به معماری مبتنی بر ارزیابی مناسب اهداف و الزامات مرتبط کاربرد مورد بحث، نیاز دارد.

این مثال، سامانه‌ای را توصیف می‌کند که PII را از طرف‌های ارتباط PII به طور امن از کانال های امن جمع‌آوری می‌کند. کنترل‌کننده PII سپس از اشتراک‌گذاری مخفی برای تبدیل PII به غیر PII استفاده می‌کند. نتیجه غیر PII سپس به سه پردازشگر PII ارسال می‌شود که از محاسبات امن برای پردازش PII مشترک مخفی استفاده می‌کند بدون این که قادر به پیوند مقادیر با طرف‌های ارتباط PII منفرد باشد. گره‌های پردازشگر PII که در محاسبات امن به کار گرفته می‌شود، نتیجه مشترک مخفی را دریافت می‌کنند و آن را به تحلیلگر داده انتقال می‌دهد که می‌تواند نتیجه را از اشتراک‌ها بازسازی کند.

ب-۲ هدف، بازیگران و استقرار

هدف از سامانه ICT، جمع‌آوری اطلاعات شخصی از تعدادی از طرف‌های ارتباط PII است. این جمع‌آوری توسط سازمانی که مطالعه آماری انجام می‌دهد سازمان‌دهی می‌شود. از آنجایی که خود سازمان دانش تحلیل آماری را ندارد، طراحی مطالعاتی واقعی و تحلیل داده را به یک دفتر تحلیل داده برون‌سپاری می‌کند.

اشتراک‌گذاری مخفی و محاسبه چندطرفه امن (SMC)[1] برای حفظ بیشتر PII استفاده می‌شود. استفاده از اشتراک‌گذاری مخفی و محاسبه چندطرفه امن در این فرانامه نیازمند حداقل سه سازمان برای مشارکت در پردازش امن PII است. این سازمان ها به گره‌های محاسبه چندطرفه امن تبدیل می‌شوند و نقش آنها ذخیره‌سازی PII مشترک مخفی و انجام محاسبه چندطرفه امن روی آن است.

اگر هیچ سازمانی که گره SMC را میزبانی می‌کند، پایگاه‌داده مشترک خود را منتشر نکند، برای سایر گره‌های SMC امکان بازسازی PII اصلی وجود دارد. گره‌ها SMC به صورت نوعی به عنوان نمایندگانی که با ذینفعان شراکتی ندارند انتخاب می‌شوند.

بازیگران برنامه کاربردی به شرح زیر هستند:

الف- افرادی که PII را فراهم می‌کنند طرف‌های ارتباط PII هستند؛

ب- هماهنگ‌کننده مطالعاتی به عنوان کنترل‌کننده PII عمل می‌کند؛ و

1 - Secure multiparty computation

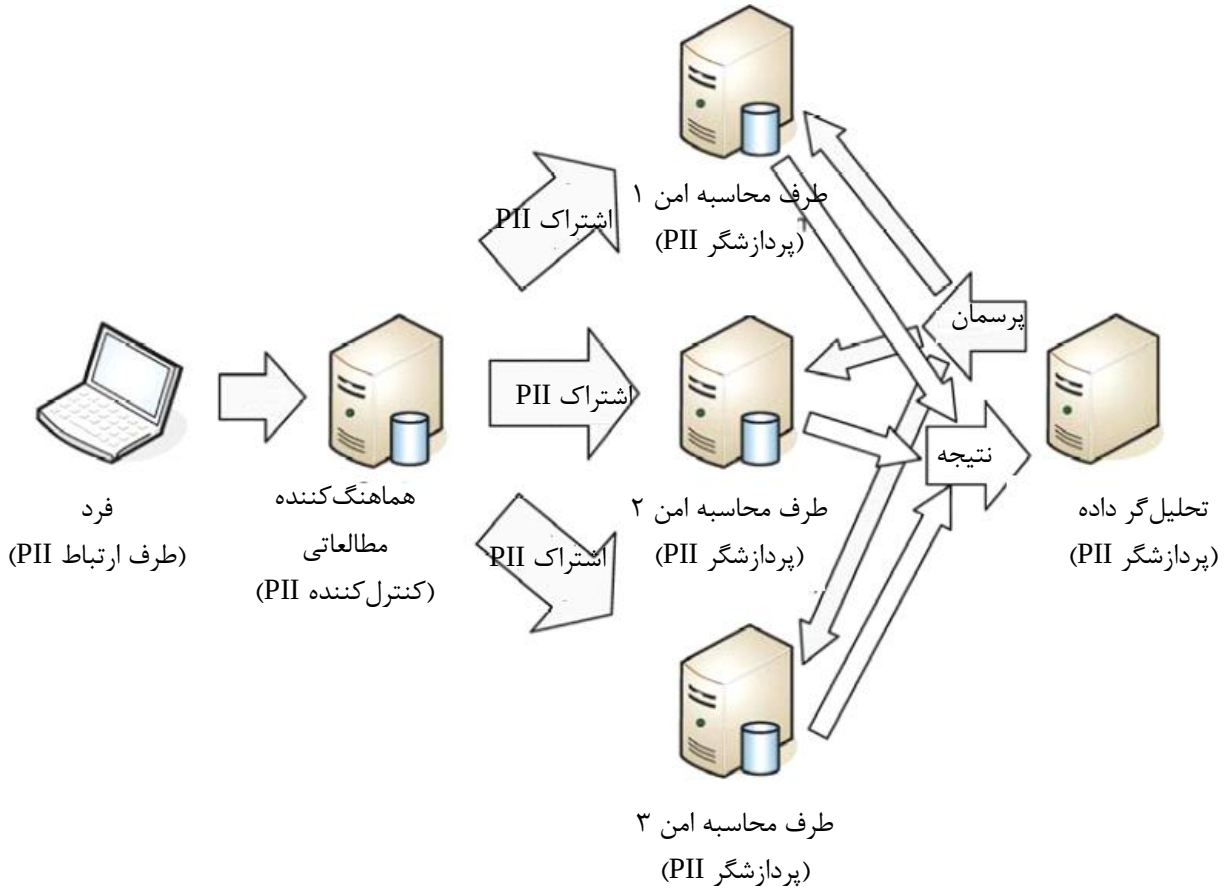
پ- گره‌های SMC و تحلیل‌گر داده، پردازشگرهای PII هستند.

سامانه ICT همانطور که در شکل ب-۲ نشان داده شده، مستقر می‌شوند؛

الف- سامانه ICT طرف ارتباط PII، یک برنامه کاربردی وب است که در مرورگر وب طرف ارتباط PII اجرا می‌شود. این سامانه در کارساز وب کنترل‌کننده PII میزبانی می‌شود.

ب- سامانه ICT کنترل‌کننده PII یک برنامه کاربردی وب است که در کارساز وب کنترل‌کننده PII میزبانی می‌شود؛ و

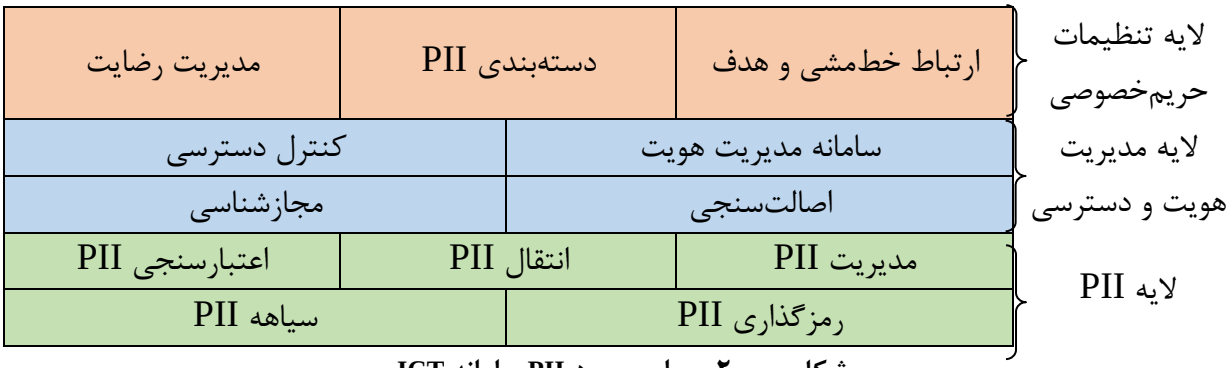
سامانه ICT پردازشگر PII، برنامه کاربردی تخصصی با سامانه محاسبه امن متصل برای ذخیره‌سازی داده مشترک مخفی است که برای پردازش ارسال شده است.



شکل ب-۱ – استقرار سامانه محاسبه امن

ب-۳ معماری برای برنامه کاربردی ورود PII

هماهنگ‌کننده مطالعاتی، سامانه ICT طرف ارتباط PII را آماده می‌کند. گرچه، هنوز شامل کل سه لایه چارچوب کاری معماری ISO/IEC 29101 است. شکل ب-۲ معماری برنامه کاربردی ورود PII را نشان می‌دهد.



شکل ب – ۲ معماری ورود PII سامانه ICT

این مولفه‌ها می‌توانند به صورت زیر پیاده‌سازی شوند:

لایه تنظیمات حریم‌خصوصی:

الف- **دسته‌بندی PII:** از آنجایی که از طرف ارتباط PII در مورد PII حساس سوال می‌شود، هر چیزی که PII وارد می‌کند به صورت خودکار حساس در نظر گرفته می‌شود، به استثنای حقیقت و زمان رضایت؛

ب- **مدیریت رضایت:** برنامه کاربردی ورود PII، بعد از ارائه خط‌مشی و هدف، به طور صریح از طرف ارتباط PII قبل از ارائه فرم ورود PII در مورد رضایت سوال می‌پرسد. همچنین تصمیم رضایت و تاریخ آن به سامانه ICT کنترل‌کننده PII ارسال می‌شود. یک مقدار تصادفی توسط سامانه ICT طرف ارتباط PII تولید و به سامانه ICT کنترل‌کننده PII همراه با رضایت جهت اجازه اصلاح یا صرف نظر کردن از رضایت انتقال داده می‌شود. برای اصلاح یا صرف نظر کردن از رضایت، طرف ارتباط PII با هماهنگ‌کننده مطالعاتی تماس برقرار می‌کند و مقدار تصادفی را ارائه می‌کند، که می‌تواند برای مراجعه به PII فراهم شده قبلی استفاده شود و آن را برای اصلاح یا حذف علامت گذاری کند؛ و

پ- **ارتباط خط‌مشی و هدف**: خط‌مشی حریم‌خصوصی و هدف جمع‌آوری PII به طرف ارتباط PII در محدوده برنامه کاربردی ورود PII که از کارساز وب بارگیری‌شده، تحویل می‌شود.

لایه مدیریت دسترسی و هویت:

الف- **سامانه مدیریت هویت:** طرف‌های ارتباط PII تا زمانی که ورود گمنام باشد، شناسایی نمی‌شوند. ارتباط هویت کنترل‌کننده PII از طریق برنامه کاربردی ورود PII برقرار می‌شود؛ و

ب- **کنترل دسترسی، اصالت‌سنجی و مجازشناسی**؛ دسترسی به برنامه کاربردی ورود PII با محدود کردن تحویل آن از کارساز کنترل‌کننده PII محدود می‌شود. طرف‌های ارتباط PII برای نگهداری گمنامی آنها اصالت‌سنجی نمی‌شوند (هیچ روش اصالت‌سنجی گروهی نیز استفاده نمی‌شود). طرف ارتباط PII، کارسازهای کنترل‌کننده PII را از طریق اتصال HTTP امن استاندارد اصالت‌سنجی می‌کند.

لایه PII:

الف- **مدیریت PII**: برنامه کاربردی ورود PII ذخیره‌سازی محلی را در مرورگر وب طرف ارتباط PII ارائه نمی‌کند. این برنامه، PII را به صورت مستقیم به کنترل‌کننده PII منتقل می‌کند؛

ب- **انتقال PII**: HTTP امن برای ارسال PII به کارسازهای کنترل‌کننده PII استفاده می‌شوند؛

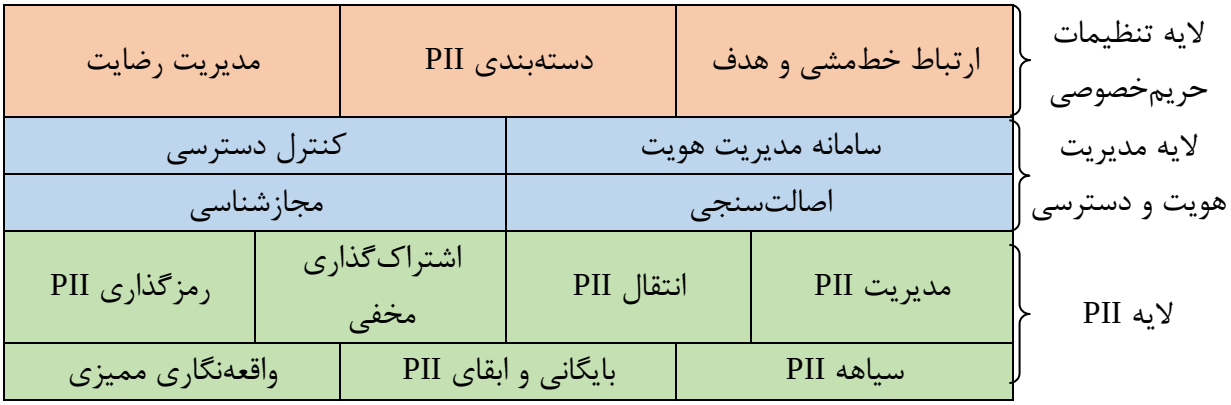
پ- **اعتبارسنجی PII**: فیلدهای فرم ورود PII، مقادیر فراداده‌ای را تخصیص می‌دهند که برای اعتبارسنجی این که مقادیر ورودی با قالب درست مطابقت داشته باشد استفاده می‌شود.

ت- **رمزگذاری PII**: رمزگذاری PII (و ادامه پیام‌های بین طرف ارتباط PII و کنترل‌کننده PII) با اتصال HTTP امن مدیریت می‌شود؛ و

ث- **سیاهه PII**: بعد از پر کردن فرم، برنامه کاربردی ورود PII به طرف ارتباط PII اجازه بازنگری پاسخ‌ها و ذخیره یا چاپ رونوشتی از PII با نام کنترل‌کننده PII و سازمان‌های پردازشگر PII و مقدار تصادفی ارسال‌شده با رضایت را می‌دهد.

ب-۴ معماری برای برنامه کاربردی کنترل مطالعه

کنترل‌کننده PII همچنین از یک سامانه ICT مبتنی بر وب با برخی قابلیت‌های بیشتر برای ساماندهی PII جمع‌آوری‌شده از چندین طرف ارتباط، ارسال آن به پردازشگرهای PII و اجرای ممیزی‌های بیشتر استفاده می‌کند. این معمار در شکل ب -۳ ارائه شده است.



شکل ب – ۳ معماری برای هماهنگ‌کننده مطالعاتی سامانه ICT

مولفه‌ها می‌توانند به صورت زیر پیاده‌سازی شوند:

لایه تنظیمات حریم‌خصوصی:

الف- **ارتباط خط‌مشی و هدف**: کنترل‌کننده PII ارتباط خط‌مشی و هدف را با طرف ارتباط PII با آماده سازی و تحویل برنامه کاربردی ورود PII برقرار می‌کند. کنترل‌کننده PII ارتباط خط‌مشی با پردازشگرهای PII را از طریق توافق‌نامه های قراردادی برقرار می‌کند.

ب- **دسته‌بندی PII**: سامانه ICT کنترل‌کننده PII شامل قواعد داخلی برای طبقه‌بندی PII از طرف‌های ارتباط PII در PII حساس است (به استثنای اطلاعات رضایت)؛ و

پ- **مدیریت رضایت**: کنترل‌کننده PII اطلاعات رضایت را از برنامه کاربردی ورود PII دریافت می‌کند و آن را به همراه PII ذخیره می‌کند. مقدار تصادفی مرتبط می‌تواند بعدتر برای انجام تغییر یا برگشت رضایت استفاده شود.

لایه مدیریت دسترسی و هویت:

الف- **سامانه مدیریت هویت**: هیچ اطلاعات هویتی در مورد طرف‌های ارتباط PII ذخیره نمی‌شود. سامانه ICT کنترل‌کننده PII به طور افزوده، اطلاعاتی در مورد گره‌های SMC و تحلیل داده ذخیره می‌کند؛ و

ب- **کنترل دسترسی، اصالت‌سنجی و مجازشناسی**: دسترسی به برنامه کاربردی ورود PII با فعال یا غیرفعال کردن تحویل و غیرفعال کردن خدمت جمع‌آوری PII کنترل می‌شود. فنون استاندارد (کارت هوشمند، زیست‌سنجی، گذرواژه‌ها و غیره) برای اجازه دسترسی به سامانه ICT کنترل‌کننده PII استفاده می‌شود.

لایه PII:

الف- **مدیریت PII**: سامانه ICT هماهنگ‌کننده مطالعاتی، PII را از برنامه‌های کاربردی ورود PII دریافت می‌کند و آن را در پایگاه‌داده ذخیره می‌کند. سامانه ICT قادر به انتقال PII به سامانه ICT پردازشگر PII است؛

انتقال PII: سامانه ICT می‌تواند درخواست‌های HTTP امن را از برنامه کاربردی ورود PII دریافت کند. این سامانه همچنین می‌تواند کانال‌های امنی را برای سامانه‌های پردازشگر PII جهت انتقال اشتراک‌ها PII باز کند؛

اشتراک‌گذاری مخفی: برای انتقال PII به سامانه محاسبات امن، سامانه ICT از اشتراک‌گذاری مخفی برای تقسیم مقادیر منفرد در اشتراک‌ها استفاده می‌کند. هر اشتراک به تنهایی هیچ اطلاعاتی در مورد مقادیر ورودی آشکار نمی‌کند.

رمزگذاری PII: رمزگذاری در زمان انتقال PII از برنامه کاربردی ورود PII استفاده می‌شود. به‌علاوه، اشتراک‌های PII در انتقال به پردازشگرهای PII رمزگذاری می‌شوند. یادآوری می‌شود که تا زمانی که اشتراک‌گذاری مخفی از محرمانگی PII در حین ذخیره‌سازی اطمینان حاصل می‌کند، اشتراک‌ها نیازی به رمزگذاری ندارند؛

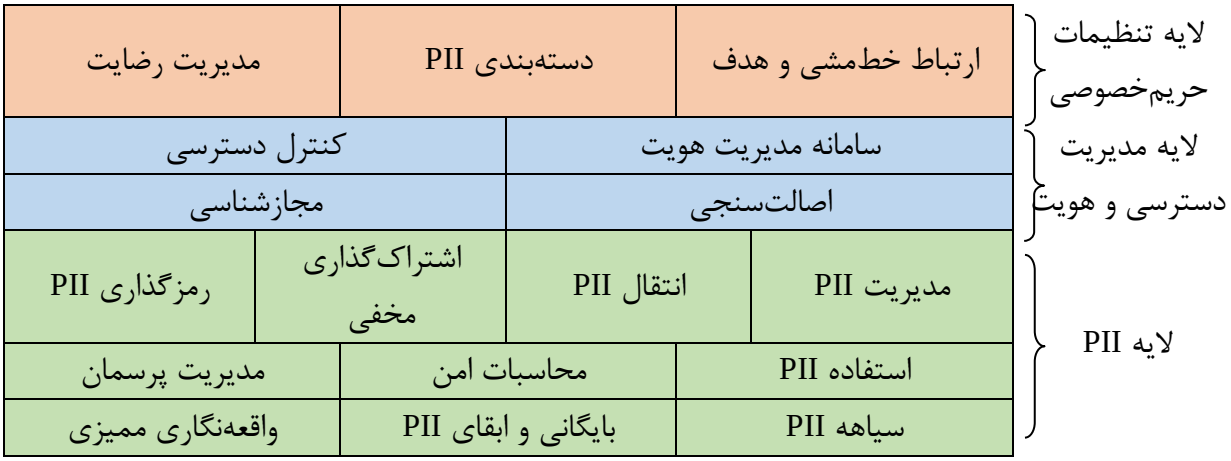
سیاهه PII: سامانه ICT می‌تواند تعداد طرف‌های ارتباط PII که PII را برای مطالعه فراهم کرده اند ارائه کند.

بایگانی و ابقای PII: بعد از اتمام مطالعه، محتویات پایگاه‌داده مطالعه به طور امن بایگانی می‌شود. ابزارهای خاص سامانه مدیریت پایگاه‌داده برای پشتیبان‌گیری استفاده می‌شود؛ و

واقعه‌نگاری ممیزی: سامانه‌های ICT هر ورود PII، هر اقدام انجام‌شده توسط کنترل‌کننده PII با استفاده از سامانه ICT و هر انتقال PII به پردازشگرهای PII را ثبت می‌کند.

ب – ۵ معماری برای برنامه کاربردی تحلیل PII امن

سامانه ICT تحلیل‌گر داده، سامانه توزیع‌شده شامل ذخیره‌سازی امن و سامانه محاسبه چندطرفه امن و برنامه کاربردی کارخواه برای ایجاد پرسمان‌هایی برای سامانه محاسباتی امن است. معماری زیر، کل سامانه توزیع‌شده را پوشش می‌دهد. توجه شود که در توضیح معماری زیر، گره SMC به معنی نرم افزار سامانه محاسباتی امن است که توسط سازمان های میزبان سامانه SMC اجرا می‌شود. شکل ب – ۴ این معماری را نشان می‌دهد.



شکل ب -۴ معماری برای برنامه کاربردی تحلیل داده امن

این مولفه‌ها می‌توانند به شرح زیر پیاده‌سازی شوند:

لایه تنظیمات حریم‌خصوصی:

الف- **ارتباط خط‌مشی و هدف**: تحلیل‌گر داده و گره‌های SMC، خط‌مشی و هدف را با قرارداد تحلیل از کنترل‌کننده PII دریافت می‌کند.

ب- **دسته‌بندی PII**: اطلاعات ذخیره‌شده با استفاده از اشتراک‌گذاری مخفی به عنوان PII حساس دسته‌بندی می‌شود و با استفاده از محاسبه چندطرفه امن پردازش می‌شود. غیرPII ها، در صورت وجود با استفاده از روش‌های استاندارد پردازش می‌شوند؛ و

پ- **مدیریت رضایت**: هماهنگ‌کننده مطالعاتی اطمینان حاصل می‌کند که فقط PII را طرف‌های ارتباط رضایت به پردازشگرهای PII عبور می‌دهد. اگر طرف ارتباط PII، رضایت را اصلاح یا از رضایت صرف نظر کند، هماهنگ‌کننده مطالعاتی به تحلیلگر داده و گره‌های SMC اطلاع می‌دهد که کدام قسمت باید اشتراک‌های مرتبط را از سامانه‌های خود حذف کند.

لایه مدیریت دسترسی و هویت:

الف- **سامانه مدیریت هویت**: امنیت محاسبه چندطرفه امن به گره‌های SMC که هویت یکدیگر را می‌دانند و ذینفعان حریم‌خصوصی که از سامانه (سامانه ICT هماهنگ‌کننده مطالعاتی، PII و سامانه ICT تحلیل داده ارائه‌دهنده پرسمان را به نمایش می‌گذارد) استفاده می‌کنند بستگی دارد. به طور مشابه، سامانه ICT تحلیلگر داده باید هویت‌های گره‌های SMC و هماهنگ‌کننده مطالعاتی را بشناسد؛ و

ب- **کنترل دسترسی، اصالت‌سنجی و مجازشناسی**: گره‌های SMC قبل از پذیرفتن PII از سامانه ICT هماهنگ‌کننده مطالعاتی، هویت سامانه را اصالت‌سنجی و آن را مجاز می‌کند. به طور مشابه، گره‌های SMC

قبل از پذیرفتن پرسمان‌ها، سامانه ICT هماهنگ‌کننده داده را اصالت‌سنجی و آن را مجاز می‌کند. سامانه ICT تحلیلگر داده از فنون استاندارد برای اصالت‌سنجی و مجازشناسی پردازشگر PII استفاده می‌کند.

لایه PII:

الف- **مدیریت PII**: گره‌های SMC، PII را در فرم اشتراک مخفی ذخیره می‌کند. سامانه ICT تحلیلگر داده باید قابلیت ذخیره پرسمان‌ها و نتایج آنها را داشته باشد؛

ب- **سیاهه PII**: گره‌های SMC می‌تواند اطلاعاتی در مورد تعداد سوابق در پایگاه‌داده‌های اشتراک مخفی ارائه کند؛

پ- **استفاده PII**: تحلیلگر داده دستی، پرس‌وجو کرده و آنها را به گره‌های SMC ارسال می‌کند. گره‌های SMC ، PII را در حالی که از حریم‌خصوصی محافظت می‌کند، پردازش می‌کند و نتایج پرسمان را به تحلیلگر داده برمی‌گرداند. تحلیلگر داده گزارش‌ها را برای هماهنگ‌کننده مطالعاتی ساختاربندی می‌کند.

ت- **انتقال PII**: گره‌های SMC از کانال‌های امن برای دریافت PII اشتراک مخفی و پرسمان‌ها و همچنین برای انجام محاسبه چندطرفه امن استفاده می‌کند. نتایج مطالعه با استفاده از پیام‌های رایانامه رمزگذاری‌شده از تحلیلگر داده به هماهنگ‌کننده مطالعاتی منتقل می‌شوند؛

ث- **اشتراک‌گذاری مخفی**: اشتراک‌گذاری مخفی در سامانه محاسبه چندطرفه امن برای ذخیره PII و مطابق پروتکل‌های محاسبه امن استفاده می‌کند؛

ج- **رمزگذاری PII**: رمزگذاری در انتقال یا PII، PII اشتراک مخفی، پرسمان‌ها و نتایج استفاده می‌شود. به طور اختیاری، نتایج مطالعه در یک فرم رمزگذاری‌شده منتقل می‌شود؛

چ- **مدیریت پرسمان**: گره‌های SMC از پاسخ به پرسمانها در صورتی که از تعداد سوابق PII از پیش تعریف شده کمتر باشد، امتناع می‌کنند. همچنین آنها به تحلیلگر داده تنها نتایج نهایی الگوریتم‌های آماری را ارائه می‌دهد. مقادیر میانی در فرم اشتراک مخفی حفظ می‌شوند. تنها موافقت پیشین در مورد روال‌های آماری استفاده می‌شود؛

ح- **محاسبات امن**: این سامانه از محاسبه چندطرفه امن با سه گره استفاده می‌کند؛

خ- **بایگانی و ابقای PII**: در این برنامه کاربردی، گره‌های SMC باید پایگاه‌داده‌های خود را در همان فرم اشتراک مخفی بایگانی کنند یا PII را به صورتی امن امحا کنند. تحلیلگر داده به صورتی امن نتایج مطالعه را بایگانی می‌کند. دسترسی و واقعه‌نگاری پرسمان باید هم توسط گره‌های SMC و هم سامانه ICT تحلیلگر داده بایگانی شوند؛ و

د- **واقعه‌نگاری ممیزی**: گره‌های SMC باید ثبتی از همه رویدادهای زیر نگهداری کند: ۱) PII دریافت‌شده از هماهنگ‌کننده مطالعاتی، ۲) پرسمان‌های دریافت شده از تحلیلگر داده، ۳) نتایج برگشت داده شده به تحلیلگر داده. سامانه ICT تحلیلگر داده باید واقعه‌نگاری تمامی پرسمان‌های ایجادشده و همه نتایج دریافت‌شده را نگهداری کند.

ب-۶ نتیجه

معماری ارائه شده نشان می‌دهد که چگونه یک سامانه ICT ساده می‌تواند با حفاظت حریم‌خصوصی بسیار خوب با استفاده از فناوری‌های بهسازی حریم‌خصوصی ایجاد شود. یادآوری می‌شود که استفاده از الگوهای محاسبه امن متفاوت ممکن است منتج به استقرار متفاوت و حفاظت امنیتی متفاوت شود. راه حل توصیف‌شده در این معماری از سامانه محاسبه امن استفاده می‌کند که ساده‌تر کردن سامانه را جهت درک به توسعه‌دهنده موتور پایگاه‌داده نمونه یادآوری می‌کند.

این سامانه ویژگی‌های امنیتی زیر را دارد که با فنون دیگر به سختی تضمین می‌شوند:

الف- مقادیر انفرادی PII توسط هیچ کس به جز طرف ارتباط PII گواهی نمی‌شود؛

ب- سازمان‌هایی که پایگاه‌داده محاسبه اشتراک را میزبانی می‌کنند، تا زمانی که پایگاه‌داده‌های اشتراکی، چیزی را در مورد مقادیر PII انفرادی آشکار نکنند، مخاطره کاهش یافته چشمگیری از حملات داخلی دارند؛ و

پ- اگر پایگاه‌داده هر طرف مفروضی به خطر افتاده یا به سرقت برود، روال محاسبه چندطرفه ویژه به نام اشتراک‌گذاری مجدد می‌تواند برای محاسبه اشتراک‌های جدید PII استفاده شود، تا قبل از این که طرف‌های بیشتری به خطر افتادند، مخاطره‌های مربوط به PII کمینه شود.

پیوست پ

(اطلاعاتی)

سامانه مستعار با حریم‌خصوصی دوستانه، برای مدیریت کنترل دسترسی و هویت[1]

پ-۱- مقدمه

این پیوست، معماری نمونه برای یک سامانه ارزیابی دوره دانشگاهی را توصیف می‌کند، که به دانشجویان امکان ارزیابی دوره را به صورت برخط بدون الزام به آشکار کردن اطلاعات شخصی آنها می‌دهد. این برنامه کاربردی قادر به اصالت‌سنجی دانشجویان است به طوری که تنها دانشجویان واجد شرایط بتوانند در ارزیابی دوره شرکت کنند، اما هویت دانشجوی واقعی، ناشناخته باقی بماند.

معماری نمونه بر اساس روش اعتبارنامه‌های مبتنی بر خصیصه (ABC) [2]ساخته می‌شود. ABC به مالک اعتبارنامه مبتنی بر خصیصه این امکان را می‌دهد که اثبات رمزنگاری مالکیت خصیصه‌های قطعی را ایجاد کند (به طور مثال اثبات این که آنها دانشجویان دانشگاه هستند و برای این دوره ثبت‌نام کرده‌اند) .

در این مثال، دانشگاه نقش ارائه‌دهنده خدمت اعتبارنامه[3] را دارد که اعتبارنامه معتبر را برای دانشجو صادر می‌کند، که درستی PII حاوی آن را تضمین می‌کند. با کسب چنین اعتبارنامه هایی، دانشجو می‌تواند PII حاوی آنها را به یک نشان[4] جدید تبدیل کند، که شامل PII گمنام‌شده و اثبات مرتبط است و آن را به برنامه کاربردی ارزیابی دوره نشان می‌دهد که به ترتیب باید مناسب تائید اعتبار نشان باشد.

پ-۲ هدف، بازیگران و استقرار

هدف این سامانه، قادر ساختن دانشجویان واجد شرایط برای ارزیابی دوره دانشگاهی به صورت مستعار است. در شروع دوره، دانشگاه باید اعتبارنامه‌های دیجیتالی (رقمی) را برای دانشجویانی صادر کند، که نام‌نویسی آنها برای نیمسال جاری و ثبت‌نام آنها برای دوره دانشگاهی را اعتباربخشی می‌کند. به‌علاوه، مشارکت دانشجو در سخنرانی باید همچنین برای هر استاد مرتبط، تائید شود.

در پایان دوره، دانشجو ممکن است بخواهد دوره را ارزیابی کند، اما او میخواهد گمنام باشد. از سوی دیگر، دانشگاه می‌خواهد نتایج ارزیابی را تنها از دانشجویان همان دانشگاه دریافت کند که برای دوره ثبت‌نام کرده اند. برای رضایت علاقمندی‌های دو طرف، سامانه ارزیابی دوره می‌تواند درخواست‌های تولیدشده از اعتبارنامه های دانشجویان را بپذیرد، این اطمینان را حاصل می‌کند که درخواست ها درست هستند، در حالی که دانشجوی پشت هر ارزیابی شناسایی نمی‌شود.

بازیگران برنامه کاربردی در این معماری نمونه به شرح زیر هستند:

---

1 - A privacy-friendly, pseudonymous system for identity and access control management

2 - attribute-based credentials

۳- اصطلاح مربوط به اعتبارنامه در این پیوست در ISO/IEC 29115 تعریف شده است.

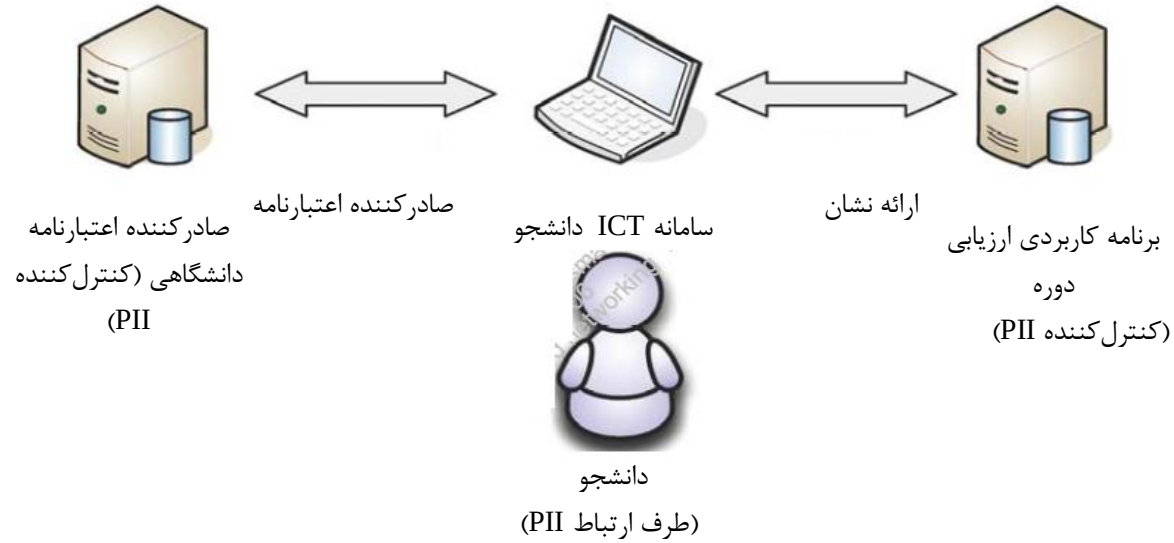
4 - Token

الف- دانشجو، طرف ارتباط PII است. سامانه ICT دانشجو دو مورد استفاده اصلی دارد. اول، به او این امکان را می‌دهد که با صادرکننده اعتبارنامه دانشگاهی برای درخواست صدور یک اعتبارنامه تعامل داشته باشد. دوم، اعتبارنامه می‌تواند بعدا برای ایجاد درخواست‌های شناسایی در مورد دانشجو برای دسترسی به خدمت پیشنهادشده توسط برنامه کاربردی ارزیابی دوره استفاده شود؛

ب- صادرکننده اعتبارنامه دانشگاهی تا زمانی که PII را از دانشجویان درخواست کننده صدور اعتبارنامه پردازش می‌کند، به عنوان کنترل‌کننده PII ایفای نقش می‌کند. صدور اعتبارنامه ها باید با استفاده از یک سامانه ICT اختصاصی انجام شود که باید برای دانشجو به صورت برنامه کاربردی برخط یا برنامه کاربردی که به صورت محلی اجرا می‌شود در محوطه صادرکننده اعتبارنامه دانشگاهی در دسترس باشد. در مورد آخر، ممکن است دانشجویان نیاز به ارائه PII خود با مراجعه حضوری داشته باشند؛ و

پ- برنامه کاربردی ارزیابی دوره، یک سامانه ICT است که توسط دانشگاه ارائه شده و به عنوان یک کنترل‌کننده PII ایفای نقش می‌کند. این برنامه کاربردی باید درخواست‌های دریافت شده از دانشجویان را برای تائید یا رد دسترسی آنها به ارزیابی دوره برخط تائید کند. برای اجازه یا رد دسترسی به ارزیابی دوره، این سامانه ICT باید اثبات‌های اصالت‌سنجی ارائه‌شده توسط طرف ارتباط PII را تائید کند. در این مورد، تا زمانی که بر درستی اطلاعات اعتبارنامه صادرشده توسط صادرکننده اعتبارنامه دانشگاهی تکیه می‌شود، یک رابطه اعتماد بین برنامه کاربردی ارزیابی دوره و صادرکننده اعتبارنامه دانشگاهی شکل می‌گیرد.

در اصل، حتی اگر یک سازمان انفرادی (به طور مثال یک بخش معین از دانشگاه) هم صدور اعتبارنامه‌ها و هم ارزیابی دوره را مدیریت کند، اقدامات صدور و ارائه مرتبط نمی‌تواند به طرف ارتباط PII پیوند بخورد. این معماری نمونه پردازشگرهای PII اختصاصی را شامل نمی‌شود. شکل پ-۱ مروری بر بازیگران سامانه و تعاملات آنها را ارائه می‌دهد.



شکل پ-۱ – مروری بر معماری – بازیگران و تعاملات آنها [۱]

۱- جریان‌های داده که در اینجا آمده است تنها مروری از نمونه معماری را نشان می‌دهد، استقرارهای خاص ممکن است با تبادل‌های داده بیشتری همکاری داشته باشد.

پ-۳ معماری سامانه ICT صادرکننده اعتبارنامه دانشگاهی

صادرکننده اعتبارنامه دانشگاهی باید قادر به صدور اعتبارنامه‌ها برای دانشجو و تضمین درستی PII محتـوی چنین اعتبارنامه‌هایی باشد. متعاقباً، صادرکننده اعتبارنامه دانشگاهی می‌تواند به عنوان یک کنترل‌کننده PII درک شود که به درخواست‌های صدور اعتبارنامه طرف ارتباط PII پاسخ می‌دهد. شکل پ-۲ معماری سامانه ICT صادرکننده اعتبارنامه دانشگاهی را نشان می‌دهد.

لایه تنظیمات حریم‌خصوصی	ارتباط خط‌مشی و هدف	مدیریت رضایت
لایه مدیریت دسترسی و هویت	سامانه مدیریت هویت	کنترل دسترسی
	اصالت‌سنجی	مجازشناسی
لایه PII	مدیریت PII	انتقال PII
	سیاهه PII	واقعه‌نگاری ممیزی

شکل پ-۲ – معماری سامانه ICT صادرکننده اعتبارنامه دانشگاهی

لایه تنظیمات حریم‌خصوصی:

الف- **ارتباط خط‌مشی و هدف**: سامانه ICT صادرکننده اعتبارنامه دانشگاهی باید یک خط‌مشی به سـامانه ICT دانشجو تحویل دهد، که PII دانشجویی را توصیف می‌کند که باید آن را برای دریافت اعتبارنامـه صـادر شده آشکار کند. علاوه بر این، صادرکننده باید هدف چنین جمع‌آوری داده‌ای را مشخص کند؛ و

ب- **مدیریت رضایت**: دانشجو درخواست صدور اعتبارنامه را خواهد داد و باید رضایت بـرای پـردازش PII را قبل از به کارگیری پروتکل صدور ارائه کند.

لایه مدیریت دسترسی و هویت:

الف- **سامانه مدیریت هویت**: صادرکننده اعتبارنامه دانشـگاهی بایـد درسـتی PII موجـود در اعتبارنامـه را ضمانت کند. برای ارائه تضمین، صادرکننده اعتبارنامه دانشگاهی باید وارسی سازگاری با PII ای که کاربر در حین پردازش آشکار می‌کند را قبل از صدور اعتبارنامه انجام دهد؛ و

ب- **کنترل دسترسی، اصالت‌سنجی و مجازشناسی**: برای شروع صدور اعتبارنامه، صادرکننده اعتبارنامـه دانشگاهی باید دانشجو را اصالت‌سنجی کند. به‌علاوه، جهـت اطمینـان از امنیـت، بایـد یـک سـامانه کنتـرل دسترسی مناسب با محدودیت دسترسی کاربران به سامانه صدور اعتبار نامه (گواهی نامه)، مستقر شود.

لایه PII:

الف- **مدیریت PII**: صـادرکننده اعتبارنامـه دانشـگاهی، پایگـاه‌داده PII دانشـجویان را بـا سـوابق در مـورد دانشجویان ثبت‌نام‌شده، شماره هویت دانشجویی، نام، تاریخ تولد، دوره‌هایی که انتخاب کرده‌اند و PII مرتبط دیگر نگهداری می‌کند. این اطلاعات باید به اندازه کـافی امـن شـده باشـد و سـازوکارهای مـدیریت امنیتـی مناسب باید برای اطمینان از محرمانگی PII مستقر شود.

ب- **انتقال PII**: زمانی که PII، بـه طـور مثـال اعتبارنامـه‌هـا، در اینترنـت منتقـل مـی‌شـود، سـامانه ICT صادرکننده اعتبارنامه باید قادر به شکل دهی اتصالات اصالت‌سنجی‌شده امن احراز باشد تا محرمـانگی PII را حفظ کند و هویت دریافت کننده نهایی را اصالت‌سنجی کند.

پ- **سیاهه PII**: صادرکننده اعتبارنامه دانشگاهی باید یک پایگاه‌داده با سوابق همه دانشجویان ثبت‌نام شده، به همراه PII آنها به طـور مثـال شـماره هویـت دانشـجویی و اطلاعـات تمـاس داشـته باشـد. سـامانه ICT صـادرکننده اعتبارنامـه دانشـگاهی بایـد سـیاهه اعتبارنامـه‌هـای صادرشـده بـه دانشـجویان را بـه همـراه واقعه‌نگاری‌های تراکنش برای اهداف ممیزی نگهداری کنند. سـامانه ICT بایـد قـادر بـه تولیـد تعـداد کـل درخواست‌های دریافت شده و تعداد تراکنش های صدور موفق و ناموفق باشد؛ و

ت- **واقعه‌نگاری ممیزی**: صادرکننده اعتبارنامه دانشگاهی باید واقعه‌نگاری مـوارد تـراکنش را بـرای اهـداف ممیزی نگهداری کند.

پ-۴ معماری سامانه ICT دانشجو

سامانه ICT دانشجو باید با هر دو سامانه‌های ICT دیگر ارتباط داشته باشد. اگر فرایند صـدور اعتبارنامـه بـه صورت الکترونیکی باشد، باید اعتبارنامه‌ها را از صادرکننده اعتبارنامه دانشگاهی درخواست کند. ایـن سـامانه باید با برنامه کاربردی ارزیابی دوره برای ارزیابی دوره تعامل داشته باشد.

درحالی که دانشجو ممکن است در تعامل خود با صادرکننده اعتبارنامه دانشگاهی اصالت‌سنجی شود، او زمان تعامل با برنامه کاربردی ارزیابی دوره گمنام باقی مـی انـد. در مـورد آخـر، دانشـجو بایـد اثبـاتی از مالکیـت اختیارات ویژه لازم را به جای آشکار کردن هر PII ارائه دهد. سامانه ICT دانشـجو ممکـن اسـت ترکیبـی از مولفه ذخیره‌سازی با امنیت بالا برای ذخیره‌سازی مورد مخفی مربوط به اعتبارنامـه‌هـا و مولفـه نـرم‌افـزاری مرتبط باشد تا با کاربر تعامل کند و با سامانه‌های ICT دیگر در این معماری در ارتباط باشد.

ارتباط خط‌مشی و هدف		مدیریت رضایت	لایه تنظیمات حریم‌خصوصی
سامانه مدیریت هویت		طرح مستعارسازی	لایه مدیریت
کنترل دسترسی	اصالت‌سنجی	مجازشناسی	دسترسی و هویت
مدیریت PII	انتقال PII	مستعارسازی PII	لایه PII
گمنام‌سازی PII		سیاهه PII	

شکل پ-۳ – معماری سامانه ICT دانشجو

لایه تنظیمات حریم‌خصوصی:

الف- **ارتباط خط‌مشی و هدف**: دانشجو باید دو نوع خط‌مشی را دریافت کند: ارائه خط‌مشی در زمان تعامل با برنامه کاربردی ارزیابی دوره و خط‌مشی صدور در زمان تعامل با صادرکننده اعتبارنامه دانشگاهی. در هر دو مورد، سامانه ICT دانشجو باید قادر به مـدیریت ارائـه مـرتبط و خـط‌مشـی‌هـای صـدور و خـط‌مشـی‌هـای حریم‌خصوصی مرتبط باشد؛ و

ب- **مدیریت رضایت**: سامانه ICT دانشجو باید رضایت آگاهانه از دانشجو را قبل از انتقال هر PII به سامانه‌های ICT دیگر در این معماری درخواست کند.

لایه مدیریت دسترسی و هویت:

الف- **سامانه مدیریت هویت**: سامانه ICT دانشجو باید اطلاعات در مورد اعتبارنامه‌هایی که طرف ارتباط در مالکیت خود دارد را ذخیره کند.

ب- **طرح مستعارسازی**: با طراحی، سامانه ICT دانشجو باید طرح مستعارسازی را پیاده‌سازی کند که سازگار با طراحی باشد که توسط برنامه کاربردی ارزیابی دوره پشتیبانی می‌شود. سامانه ICT دانشجو باید استفاده از نام مستعار منفرد برای هر دوره برنامه کاربردی ارزیابی دوره را اجباری کند تا قادر به روزآمد ارزیابی آن باشد. برنامه کاربردی ارزیابی دوره باید دانشجو را از تولید بیش از یک نام مستعار در هر دوره محدود کند، تا از ارسال بیش از یک ارزیابی توسط دانشجو ممنوع شود؛ و

پ **کنترل دسترسی، اصالت‌سنجی و مجازشناسی**: سامانه ICT دانشجو باید هویت سامانه ICT برنامه کاربردی ارزیابی دوره را با استفاده از اصالت‌سنجی واقعی اصالت‌سنجی کند. سامانه ICT دانشجو باید اثبات‌های لازم برای تکمیل الزامات جهت اصالت‌سنجی گمنام را برای برنامه کاربردی ارزیابی دوره ایجاد کند.

لایه PII:

الف- **مدیریت PII:** سامانه ICT دانشجو باید قادر به ذخیره‌سازی اعتبارنامه‌های خود در یک محل با سطح امنیت بالا باشد.

ب- **انتقال PII:** سامانه ICT دانشجو باید قادر به پردازش اعتبارنامه‌های ذخیره‌سازی خارجی باشد، به طور مثال نشان‌های سخت افزاری یا خدمات برخط. به طور کلی، PII از سامانه ICT دانشجو به برنامه کاربردی ارزیابی دوره منتقل نمی‌شود. گرچه، سامانه ICT دانشجو ممکن است در زمان درخواست صدور اعتبارنامه‌ها نیاز به آشکار کردن PII معینی به صادرکننده اعتبارنامه دانشگاهی داشته باشد؛

پ- **مستعارسازی PII:** سامانه ICT دانشجو باید احتمال ایجاد نشان‌هایی را فراهم کند که به یک نام مستعار منفرد در دوره محدود باشد؛

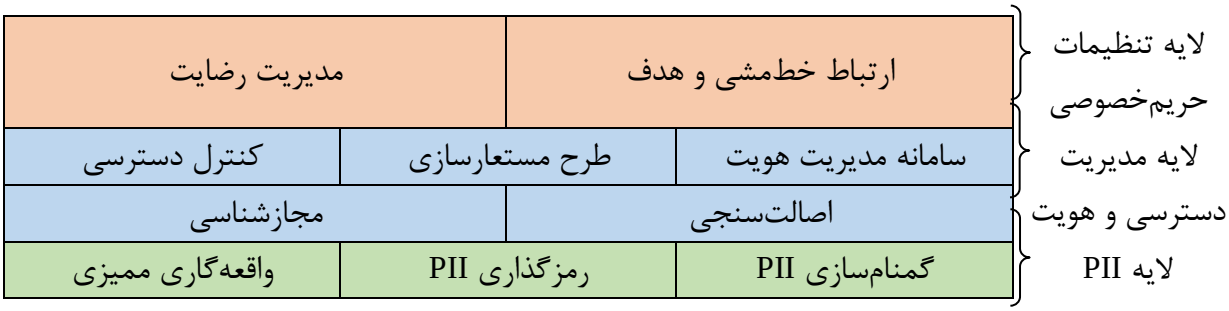
ت- **گمنام‌سازی PII:** سامانه ICT دانشجو باید قادر به انجام عملیات رمزنگاری لازم باشد که PII موجود در اعتبارنامه ها را قبل از انتشار آنها به برنامه کاربردی ارزیابی دوره گمنام می‌کند. در همین زمان، اعتبارنامه‌های مبتنی بر خصیصه باید برای متقاعد کردن برنامه کاربردی ارزیابی دوره در مورد درستی درخواست‌های دانشجو استفاده شود؛ و

ث- **سیاهه PII:** سامانه ICT دانشجو باید اعتبارنامه های با مالکیت دانشجو را در انباره اختصاصی که می‌تواند کارت هوشمند یا خدمت برخط باشد، ذخیره کند. سامانه ICT می‌تواند اعتبارنامه‌های با مالکیت دانشجو را فهرست کند. این اعتبارنامه‌ها محدود به مورد مخفی معین هستند، که برای ایجاد اثبات‌های رمزنگاری لازم که باید به صورتی امن ذخیره شوند استفاده می‌شود (به طور مثال استفاده از یک نشان سخت‌افزاری).

پ-۵ معماری برنامه کاربردی ارزیابی دوره

برنامه کاربردی ارزیابی دوره می‌تواند برای جمع‌آوری بازخورد از دوره‌های دانشگاهی مورد استفاده قرار گیرد. سامانه ICT باید با سامانه ICT دانشجو تعامل داشته باشد و بر درستی اطلاعات موجود در اعتبارنامه‌هایی که توسط صادرکننده اعتبارنامه دانشگاهی صادر شده است اعتماد داشته باشد.

تعامل بین سامانه ICT دانشجو و برنامه کاربردی ارزیابی دوره زمانی که دانشجو تصمیم به ارزیابی دوره دانشگاهی می‌گیرد، شروع می‌شود. سامانه ICT دانشجو باید درخواستی را به برنامه کاربردی ارزیابی دوره ارسال کند که باید به ترتیب با خط‌مشی به آن پاسخ دهد، در این خط‌مشی بیان شده است که دانشجو باید اثبات این که او دانشجوی دانشگاه است، برای این دوره خاص ثبت‌نام کرده و حداقل در چند سخنرانی شرکت داشته است را ارائه دهد. سامانه ICT دانشجو باید از اعتبارنامه های ذخیره‌شده برای ایجاد اثبات درخواست‌شده استفاده کند و آن را به برنامه کاربردی ارزیابی دوره ارائه کند که به ترتیب درخواست‌های ارائه‌شده را بدون شناسایی دانشجو درستی‌سنجی می‌کند. اگر درستی‌سنجی موفقیت آمیز بود، دانشجو واجد شرایط در نظر گرفته می‌شود و دسترسی به فرم ارزیابی دوره به او اعطا می شود.



شکل پ-۴ – معماری برنامه کاربردی ارزیابی دوره

لایه تنظیمات حریم‌خصوصی:

الف- **ارتباط خط‌مشی و هدف**: برنامه کاربردی ارزیابی دوره باید پیوندی به خط‌مشی حریم‌خصوصی برنامه کاربردی ارزیابی دوره سامانه ICT دانشجو داشته باشد. این خط‌مشی باید مشخص کند که درخواست چه نوعی از PII را در حین اصالت‌سنجی گمنام اثبات می‌کند. سامانه ICT دانشجو باید دانشجو را مجبور به خواندن خط‌مشی کند؛ و

ب- **مدیریت رضایت**: برنامه کاربردی ارزیابی دوره باید رضایت آگاهانه را از دانشجو به منظور دنبال کردن اصالت‌سنجی و ارزیابی دوره کسب کند. برنامه کاربردی ارزیابی دوره باید قادر به ثبت اقدام واگذاری رضایت باشد.

لایه مدیریت دسترسی و هویت:

الف- **سامانه مدیریت هویت**: برنامه کاربردی ارزیابی دوره باید اثبات‌های ارائه‌شده توسط دانشجو را ذخیره کند. این کار شامل اطلاعات مربوط به انواع اعتبارنامه، شناسانه‌های اعتبارنامه و سایر شواهد رمزنگاری ایجادشده توسط کاربر است. این اطلاعات می‌تواند برای اهداف غیر انکار و برای پردازش مناسب درخواست‌های قبلی در مورد ارزیابی تکراری (برای مثال زمانی که دانشجو می‌خواهد یک ارائه را روزآمد

کند) استفاده شود. دانشجو همچنان گمنام باقی می‌ماند اما ارزیابی‌های متفاوت می‌توانند به آن پیوند داشته باشند.

ب- **طرح مستعارسازی**: برنامه کاربردی ارزیابی دوره باید استفاده از نام های مستعار را پشتیبانی کند، به طوری که قابلیت پیوند کنترل‌شده را برای دانشجویان فراهم می‌آورد، اما هیچ PII ای در مورد دانشجو را بعد از نام مستعار آشکار نکند. برنامه کاربردی ارزیابی دوره باید با سامانه ICT دانشجو برای مذاکره طرح مستعارسازی که هر دو سامانه ICT آن را پشتیبانی می‌کنند، تعامل کند؛ و

پ- **کنترل دسترسی، اصالت‌سنجی و مجازشناسی**: برنامه کاربردی ارزیابی دوره باید اثبات ارائه‌شده توسط سامانه ICT را درستی‌سنجی کند. اصالت‌سنجی دانشجو باید گمنام و مبتنی بر اعتمادی انجام شود که برنامه کاربردی ارزیابی دوره در درستی PII موجود در اعتبارنامه‌های صادر شده توسط صادرکننده اعتبارنامه دانشگاهی دارد.

لایه PII:

الف- **واقعه‌نگاری ممیزی**: برنامه کاربردی ارزیابی دوره باید واقعه‌نگاری‌های تراکنش‌های انجام‌شده برای فرایند ممیزی را حفظ کند. این برنامه همچنین فهرستی از موارد رمزنگاری دریافت‌شده همچون نام‌های مستعار را ذخیره می‌کند.

پ-۶ نتیجه

این معماری نمونه در این استاندارد یک برنامه کاربردی ارزیابی دوره را نشان می‌دهد که دانشجویان را بدون پرسش در مورد آشکار کردن PII آنها اصالت‌سنجی می‌کند. این معماری می‌تواند گسترش بیشتری یابد و در جایی که اصالت‌سنجی مشابه موردنظر است، با دیگر فرانامه‌ها تطبیق داده شود. این معماری مبتنی بر ویژگی‌ها و مفاهیمی از اعتبارنامه‌های مبتنی بر خصیصه است که اصالت‌سنجی حریم‌خصوصی مساعد را درحالی فعال می‌کند که قابلیت جداسازی و قابلیت عدم ردیابی برای طرف ارتباط PII را ارائه می‌دهد.

این مثال همچنین مثالی از یک الگوی معماری است که می‌تواند برای برنامه‌های کاربردی مختلف تکرار شود. این معماری ترکیبی از مولفه‌های بخش اصلی این استاندارد، مثل مدیریت رضایت، مدیریت هویت و اصالت‌سنجی است.

این معماری فواید کلی زیر را فراهم می‌کند:

الف- قابلیت جداسازی بین صدور و ارائه اعتبارنامه؛

ب- اصالت‌سنجی امن و گمنام طرف ارتباط PII؛

پ- قابلیت پیوند کنترل‌شده، در زمان موردنظر؛ و

ت- حذف نیاز به افشای PII در حین اصالت‌سنجی، بنابراین کاهش نیاز به مولفه‌های حفاظت بیشتر.

فناوری‌های مبتنی بر اعتبارنامه‌های مبتنی بر خصیصه همچنین می‌توانند ویژگی‌های بیشتری را فراهم کنند، مثل گمنامی، افشای کمینه اطلاعات و ابطال اعتبارنامه‌هایی که از آنها سوء استفاده شده است.

پیوست ت

(اطلاعاتی)

اصول حریم‌خصوصی مربوط به کنترل‌های امنیت اطلاعات

تقریبا تمامی نقض‌های حریم‌خصوصی (مثل سوء استفاده از PII) – چه عمدی و چه سهوی– تاثیر مستقیمی بر محرمانگی، یکپارچگی و/یا دسترس‌پذیری PII دارند.

کنترل‌های امنیتی پیاده‌سازی‌شده برای حفاظت از دارایی‌های اطلاعاتی همچنین می‌تواند از PII پردازش‌شده در سامانه ICT محافظت کند. برای مثال، خط‌مشی‌هایی که از یکپارچگی داده اطمینان حاصل می‌کنند، از نفوذ یا از دست دادن داده جلوگیری کرده، می‌تواند به عنوان کنترل‌های حریم‌خصوصی به همراه کنترل‌های امنیتی عمل کنند.

الزامات حریم‌خصوصی باید به طور عادی با کنترل‌های امنیت فناوری اطلاعات مربوطه هماهنگ باشد، گرچه گاهی اوقات ممکن است با انتظارات طرف‌های ارتباط PII تداخل داشته باشد. برای مثال، کنترل‌های امنیتی که قصد حفاظت از ذینفع حریم‌خصوصی را در مقابل فریبکاری دارند و این کار به پایش فعالیت‌های خاص کارکنان نیاز دارد ممکن است با حقوق کارمندان برای حریم‌خصوصی تداخل داشته باشد. تمامی نیازهای قانونی باید در نظر گرفته شود و به اندازه بیشینه مقدار ممکن در شرایط داده‌شده مورد توجه قرار گیرد.

جدول ت-۱ رابطه اصول حریم‌خصوصی ISO/IEC 20100 را با کنترل‌های امنیت اطلاعات نشان می‌دهد:

جدول ت-۱ – اصول حریم‌خصوصی و کنترل‌های امنیت اطلاعات مربوط به آنها

اصول حریم‌خصوصی	کنترل‌های امنیت اطلاعات	بخش مرجع ISO/IEC 27002:2005
رضایت و انتخاب	رضایت و انتخاب طرف ارتباط PII باید تحت قوانین محرمانگی و به تبع آن مطابق نقش‌ها و مسئولیت‌های موافقت‌شده در سازمان باشد. کنترل‌کننده PII باید بیشتر سنجه‌های امنیتی معقول و مناسب را تعیین و پیاده‌سازی کند که دخالت‌ها را با الزامات حریم‌خصوصی مرتبط به حداقل برساند. به طور مثال، جایی که مناسب است، اصالت‌سنجی می‌تواند استفاده شود تا به اطمینان از این که فردی که رضایت می‌دهد همان فردی است که ادعا می‌کند، کمک کند.	۶-۱-۵- الف)، ب)، ت) و ج) در بین دیگر موارد.
قانونی‌بودن و ویژگی هدف	پیاده‌سازی کنترل‌های دسترسی مناسب برای اطمینان از این که تنها آنها مجاز به پردازش PII هستند، اطمینان از این که افراد خاص مسئول مدیریت دارایی‌های PII هستند و اطمینان از این که سامانه‌های فناوری اطلاعات با حریم‌خصوصی موردنظر توسعه یافته‌اند از مدیریت حریم‌خصوصی به خوبی پشتیبانی می‌کنند.	۱۱-۲، ۷-۱، ۱۲-۵

اصول حریم‌خصوصی	کنترل‌های امنیت اطلاعات	بخش مرجع ISO/IEC 27002:2005
محدودیت جمع آوری	سنجه کلی برای کاهش مخاطرات، کاهش مقدار اطلاعات حریم‌خصوصی و دارایی‌های حیاتی است که نیاز به محافظت دارد. محدود کردن جمع‌آوری اطلاعات PII برای کمینه قطعی موردنیاز از هدف امنیت اطلاعات کلی پشتیبانی می‌کند.	۴-۲ الف) و پ)
کمینه‌سازی داده	در حالی که استانداردهای امنیتی معمولا برای پایش تمامی فعالیت‌ها، پرونده‌های واقعه‌نگاری، سامانه‌های ردیابی و سایر مستنداتی که ممکن است شامل PII باشند فراخوانده می شوند، بنابراین می‌توانند با حریم‌خصوصی تداخل داشته باشند. پیاده‌سازی روال‌های طبقه‌بندی داده برای دستیابی به پردازش متفاوت PII و راهبرد کمینه‌سازی PII توصیه می‌شود. استفاده از مستعارسازی و گمنام‌سازی نیز توصیه می‌شود.	۵-۴-۷، ۵-۷-۵، ۵-۷-۶، و ۱۰-۱۰
محدودیت استفاده، ابقا و افشا	محدودکردن افشا می‌تواند در میان موارد دیگر، با استفاده مناسب از توافق‌نامه‌های محرمانگی، طبقه‌بندی و کنترل دسترسی کنترل شود. نگهداری گسترده داده – قابل توصیه از دیدگاه امنیتی – ممکن است تهدیدی برای حریم‌خصوصی باشد.	۶-۱-۵، ۷-۲ و ۱۱
دقت و کیفیت	از آنجایی که دقت و کیفیت داده در همه جا اساسی است، کنترل‌های معقول و مناسب باید از قبل در اغلب سازمان‌ها پیاده‌سازی شده باشد. این کنترل‌ها می‌توانند به PII بدون اصلاحات گسترده اعمال شوند و به کنترل PII کمک کنند.	۱۲-۲-۴
بازبودن، شفافیت و اطلاع	از آنجایی که این کار با در دسترس قرار دادن اطلاعات تنها برای طرف ارتباط PII سروکار دارد، تحققاین اهداف نیازمند سطح بالایی از امنیت است. کنترل‌های معقول و مناسب و سنجه‌های امنیتی که زمان تبادل و آشکارکردن اطلاعات اعمال می‌شود، بنابراین برای برآورده ساختن این اهداف نیز اعمال می‌شود.	۱۰-۸-۱، ۱۰-۸-۴، ۱۰-۹-۱، و ۱۰-۱۰-۱
مشارکت انفرادی و دسترسی	قواعد کنترل دسترسی باید در هر سازمانی وجود داشته باشد. ارئه‌دهندگان PII می‌توانند خط‌مشی‌های اصالت‌سنجی را برای درخواست به کار برند. کنترل‌های موجود می‌توانند برای شمول این درخواست‌ها بدون تغییرات جزئیات گسترش یابند.	۱۰-۸، ۱۰-۹ و ۱۱
پاسخگویی	تخصیص نقش‌ها و مسئولیت‌های خاص در هر چارچوب امنیتی یک بخش یکپارچه را ایفا می‌کند. پاسخگویی برای حریم‌خصوصی مربوط به خط‌مشی‌ها و روال‌ها باید به اندازه تخصیص مدنظر قرار گیرد و با ابزارهای کنترل‌های موجود تشخیص داده شود.	۷-۱ و ۸-۱-۱

اصول حریم‌خصوصی	کنترل‌های امنیت اطلاعات	بخش مرجع ISO/IEC 27002:2005
کنترل‌های امنیت اطلاعات	استانداردهای امنیتی موجود همچون ISO/IEC 27002:2005 پیشنهادات جامعی را در کنترل‌های امنیتی فراهم می‌کند که باید به طور صریح برای اطمینان از امنیت داده پیاده‌سازی شود. به طور خاص، کنترل‌های امنیتی زیر باید پیاده‌سازی شود (فهرست زیر جامع نیست): _ - دسترسی به تسهیلات پردازش داده باید برای اشخاص غیرمجاز ممنوع شود؛ _ اشخاص غیرمجاز نباید اجازه دسترسی به سامانه‌های رایانه‌ای را داشته باشند؛ _ افراد مجاز تنها باید قادر به دسترسی به PII در محدوده اختیار دسترسی خود باشند؛ _ جابجایی فیزیکی و الکترونیکی یا انتقال PII باید به طور معقول و مناسب در مقابل دسترسی غیرمجاز امن باشد؛ _ واقعه‌نگاری‌ها باید برای مستندکردن هر دسترسی و اعلام به PII به طور خاص PII حساس، نگهداری شود؛ _ ساماندهی PII توسط طرفین قرارداد باید با محدود کردن شرایط قرارداد پوشش داده شود. _ PII باید در مقابل افشای سهوی یا غیرمجاز، اصلاح، از دست رفتن، حذف یا تخریب امن باشد؛ _ PII با ویژگی‌های هدف متفاوت باید به طور جداگانه ساماندهی شود؛ و _ روال‌های مناسب برای مدیریت نقص حریم‌خصوصی باید وجود داشته باشد.	۷-۲، ۹-۱، ۱۰، ۱۱ و ۱۲-۳
انطباق	انطباق با استانداردهای امنیتی همچون ISO/IEC 27002:2005 پیروی از الزامات کنترل امنیتی را برای حفاظت از PII فراهم می‌کند که پیش شرط اجرای خط‌مشی حریم‌خصوصی است.	

کنترل‌های امنیت اطلاعات ارائه‌شده، نمونه‌هایی تصویری از کنترل‌های امنیتی پیشنهادشده هستند و به طور طبیعی الزامی نیستند.