INSO-ISO- IEC

15944-8

1st. Edition

Identical with
ISO/IEC 15944-8: 2012
2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National standardization Organization

استاندارد ایران- ایزو آی ای سی
۱۵۹۴۴-۸
چاپ اول
۱۳۹۲

فناوری اطلاعات – دیدگاه عملکردی کسب و کار – قسمت ۸: شناسایی الزامات حفاظت از حریم خصوصی به عنوان محدودیت‌های خارجی در تراکنش‌های کسب و کار

Information technology — Business Operational View — Part 8: Identification of privacy protection requirements as external constraints on business transactions

ICS:35.240.60

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 حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین‌شده تهیه می‌کنند، در کمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. به این ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران، شمارهٔ ۵، تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسهٔ استاندارد تشکیل می‌دهد، به تصویب رسیده باشند.

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

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی 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 می‌تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه-بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی 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 – دیدگاه عملکردی کسب و کار – قسمت ۸ : تعیین الزامات حفاظت از حریم خصوصی به عنوان محدودیت‌های خارجی در تراکنش‌های کسب و کار»

رئیس:	**سمت و /یا نمایندگی**
صمدیان، علی (لیسانس مهندسی الکترونیک)	معاون فناوری ارتباطات مرکز تحقیقات صنایع انفورماتیک
دبیر:	
یحیایی، مهری (فوق لیسانس مهندسی فناوری اطلاعات)	سرپرست آزمایشگاه فناوری اطلاعات مرکز تحقیقات صنایع انفورماتیک
اعضا: (اسامی به ترتیب حروف الفبا)	
آژ، رضوان (لیسانس مهندسی کامپیوتر)	کارشناس فنی مرکز تحقیقات صنایع انفورماتیک
تورانی، فرزام (لیسانس مهندسی کامپیوتر)	کارشناس فنی مرکز تحقیقات صنایع انفورماتیک
زندباف، عباس (لیسانس مهندسی الکترونیک-مخابرات)	کارشناس شرکت ارتباطات زیرساخت
شاهی، فرید (لیسانس مهندسی کامپیوتر)	کارشناس فنی مرکز تحقیقات صنایع انفورماتیک
عروجی، سیدمهدی (فوق‌لیسانس مدیریت فناوری اطلاعات)	کارشناس استاندارد سازمان تنظیم مقررات و ارتباطات رادیویی
نادری، مجید (دکترای مهندسی برق - الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

« فناوری اطلاعات - دیدگاه عملکردی کسب و کار- قسمت ۸ : تعیین الزامات حفاظت از حریم خصوصی به عنوان محدودیت‌های خارجی در تراکنش‌های کسب و کار» که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکز تحقیقات صنایع انفورماتیک بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide 21-1 (پذیرش منطقه‌ای یا ملی استانداردهای «بین‌المللی/منطقه‌ای» و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران، تهیه شده و در دویست و نود و ششمین اجلاسیه کمیته‌ی ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۲/۹/۱۹مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه 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 زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، همواره از آخرین تجدیدنظر آنها استفاده خواهد شد.

این استاندارد ملی بر اساس پذیرش استاندارد بین‌المللی به شرح زیر است:

ISO/IEC 15944-8: 2012, Information technology - Business Operational View - Part 8: Identification of privacy protection requirements as external constraints on business transactions

«فناوری اطلاعات – دیدگاه عملکردی کسب و کار – قسمت ۸: تعیین الزامات حفاظت از حریم خصوصی به عنوان محدودیت‌های خارجی در تراکنش‌های کسب و کار»

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین‌المللی ISO/IEC 15944-8:2012 تدوین شده است.

۱-۱ بیانیه هدف و دامنه کاربرد

این استاندارد ملی :

- روش(هایی) برای شناسایی، در فناوری‌های مُدل‌سازی ویرایش- باز[۱] و توسعه سناریوها، الزاماتی بیشتر در مشخصات دیدگاه عملکردی کسب و کار (BOV) [۲] برای تعیین محدودیت‌های خارجی بیشتر جهت استفاده در اطلاعات ثبتی در تراکنش‌های کسب و کار مربوط به اطلاعات شخصی هر فرد، چنانکه مورد درخواست الزامات قانونی و مقرراتی[۳] حوزه‌های کاربردی قضایی[۴] صاحب اختیار بر اطلاعات شخصی مبادله شده میان قسمت‌ها برای تراکنش‌های کسب و کار است را فراهم می‌نماید.

- به یکپارچه‌سازی عناصر الزامی[۵] موجود در حمایت از الزامات حریم خصوصی و حفاظت داده[۶] در ویرایش‌های فعلی از استانداردهای ISO/IEC 14662، ISO/IEC 15994-1، ISO/IEC 15994-2، ISO/IEC 15994-4 و ISO/IEC 15994-5 که تعیین شده است می‌پردازد، و برای اطلاعاتی در رابطه با شناسایی افراد زنده به عنوان خریدار[۷] در یک تراکنش کسب و کار و یا کسانی که از اطلاعات شخصی آنها در تراکنش استفاده شده است به کار می‌رود؛

- بیانیه‌های عملکردی و فراگیر «بهترین شیوه[۸]» را برای فرآیندها، رویه‌ها و شیوه‌های مرتبط(و نه لزوما خودکار) و همچنین الزامات حاکمیتی را فراهم می‌نماید که باید در حمایت از پیاده‌سازی و تاکید بر ساز و کارهای فنی برای پشتیبانی از الزامات حفاظت داده/حریم خصوصی مورد نیاز برای پیاده‌سازی در محیط‌های تراکنش ویرایش- باز، عمل نمایند.

1-Open-edi modelling
2- Business Operational View
3- Regulatory
4- Applicable jurisdictional domains
5- Normative elements
6- Data protection
۷ - چنانکه در بندهای ۶-۲-۴ تا ۶-۲-۸ و شکل ۱۸ از استاندارد ISO/IEC 15944-1:2011 بیان شد، یک شخص حقیقی(طبیعی) که ارائه دهنده کالا، خدمت و/ یا حقوقی باشد یک سازمان فرض می‌شود. بیشتر حوزه‌های قضایی که فعالیتی غیر همبسته داشته، خدمت و/ یا حقوق را ارائه می‌دهند نیز یک سازمان فرض می‌شوند. {به استاندارد ISO/IEC 6523 مراجعه شود}.
8- Best practice

- یک نمونه سناریو و پیاده‌سازی (مورد استفاده) برای یک یا چند مورد استفاده از حفاظت داده /حریم خصوصی در تراکنش‌های کسب و کار را شناسایی و فراهم می‌نماید؛ و،
- راهنماهایی مرتبط با ساز و کارهای رَویه‌ای در رویدادی[1] که قوانین افشای اجباری تراکنشی باید اجرا گردد را فراهم می‌نماید،

این استاندارد ملی مرتبط با BOV بوده که الزامات اساسی (یا اولیه) مربوط به محیط حفاظت از حریم خصوصی را به عنوان الزامات قانونی که در حوزه‌های قضایی بر روی تراکنش‌های کسب و کار ارائه شده‌اند و همچنین الزامات فناوری اطلاعات و محیط‌های ارتباطاتی را یکپارچه می‌نماید.

این استاندارد ملی شامل روش‌شناسی و ابزاری برای تعیین رده‌های معمولِ محدودیت‌های خارجی از طریق ساختار «حوزه‌های قضایی» است و به طور واضح با استفاده از قوانین، الگوها و فنون توصیف رسمی[2](FDTs)، با مجموعه الزامات ISO/IEC 15944-1 و ISO/IEC 15944-2 مطابقت می‌نماید.

۱-۲ استثناها[3]

۱-۲-۱ دیدگاه خدمات کارکردی (FSV)[4]

این استاندارد ملی بر جنبه‌هایِ تراکنشِ کسب و کارِ BOV متمرکز بوده و به ساز و کارهای فنی مورد نیاز برای رسیدن به الزامات کسب و کار نمی‌پردازد. (جوانب FSV، شامل تعیین الزامات یک دیدگاه خدمات کارکردی (FSV) که در برگیرنده‌ی فنون و خدمات امنیتی، پروتکل‌های ارتباطاتی و غیره می‌باشد). دیدگاه خدمات کارکردی (FSV) شامل هرگونه استانداردی است (یا توسعه‌ی استانداردهای یک FSV)، که به تصدیق استانداردهای موجود در ISO, IEC, UN/ECE و/ یا ITU رسیده است.

۱-۲-۲ رفتار داخلی[5] سازمان‌ها (و ادارات عمومی)

قسمت مستثنی شده از هدف و دامنه کاربرد این استاندارد ملی، کاربرد الزاماتِ حفاظت از حریم خصوصی در یک سازمان است. مدل مرجع ویرایش- باز، این امر را به‌عنوان رفتارهای داخلی یک سازمان درنظر می‌گیرد و آن را با تراکنش‌های کسب و کار (که بر رفتارهای خارجی مرتبط[6] با تبادل داده‌های الکترونیک در میان قسمت‌های مستقل[7] یک تراکنش کسب و کار متمرکز می‌باشد) مربوط نمی‌داند. به همین ترتیب، دیگر موارد مستثنی شده از هدف و دامنه کاربرد این استاندارد ملی عبارتند از:

۱) استفاده و مدیریت داخلی اطلاعات ثبت شده وابسته به شخص سازمانی قابل شناسایی، سازمان (یا ادارات عمومی) درون یک سازمان؛ و،

1- Event
2- Formal Description Techniques
3- Exclusions
4- Functional Services View
5- Internal behaviour
6- Pertaining to
7- Autonomous

۲) پیاده‌سازی کنترل‌های مدیریت اطلاعات داخلی، کنترل‌های رَویه‌ی داخلی یا کنترل‌های عملکردی درون یک سازمان یا اداره عمومی، به‌منظور مطابقت با الزامات کاربردی حریم خصوصی که ممکن است برای رعایت قانونی یا حقوق قراردادی، وظایف و الزامات یک هستار قانونی[1] در حوزه(های) قضایی که قسمتی از آن می‌باشند، مورد نیاز هستند.

این امر به این معنی تلقی شود که سازمانی نتواند این استاندارد ملی را برای طرح‌ریزیِ رفتار، تطبیق دهد که در زمان انتقالِ اطلاعاتِ شخصی در داخل سازمان آن را بیان نماید.

۱-۲-۳ « شخص سازمانی»

از منظر[2] الزامات حفاظت از حریم خط‌مشی عمومی، یک «شخص سازمانی» یک «شخص حقیقی» می‌باشد که به نیابت عمل نموده و تعهداتی را از جانب سازمانی (یا اداره عمومی) که آن شخص حقیقی «قسمتی از سازمان» است، اعمال می‌نماید. اما، به عنوان یک «شخص سازمانی» این افراد دارای حقوق ذاتی و طبیعی در حریم خصوصی نمی‌باشند. الزامات حفاظت از حریم خصوصی که در مورد یک شخص سازمانی به کار گرفته می‌شوند در مفهوم یک کارمند-کارفرما با عناصر قراردادی مربوطه، قرار می‌گیرند. به علاوه، برخی حوزه‌های قضایی دارای قوانین و مقررات حفاظت از حریم خصوصی می‌باشند که به طور ویژه برای کارمندان ادارات عمومی آنها به کار گرفته می‌شوند.

همین طور، از دیدگاه تراکنش کسب و کار، این یک رفتار داخلی برای سازمان بوده و مربوط به کسی است که تعهدات را از جانب سازمان یا اداره عمومی اتخاذ می‌کند. اینکه چرا و چگونه اشخاص سازمانی اقدام به اتخاذ تصمیمات و تعهدات می‌نمایند که به هدف و دامنه کاربرد این استاندارد ملی مربوط نمی‌باشد. {به استاندارد ISO/IEC 15944-1:2011، بند ۶-۲، «*اشخاص و محدودیت‌های خارجی: شخص، سازمان و ادارات عمومی*» و شکل ۱۷ مربوط به آن یعنی « *نمونه‌ای از تبادل تعهدات در مقابل تبادل اطلاعات برای سازمان، قسمت(های) سازمانی و شخص (اشخاص) سازمانی*» مراجعه شود.}

۱-۲-۴ هم‌پوشانی[3] و/ یا تضاد میان حوزه‌های قضایی به عنوان منابع الزامات حفاظت از حریم خصوصی

یک تراکنش کسب و کار، نیازمندِ تبادلِ تعهدات میان قسمت‌های مستقل می‌باشد. تعهد به معنی ایجاد یا قبول یک حق، یک الزام، شایستگی[4] یا پاسخگویی[5] توسط شخص می‌باشد. در مفهوم تراکنش کسب و کار، ایجاد تعهدات نیازمند انتقال کالا، خدمت و / یا حقوق مابین افراد مورد بحث می‌باشد.

درنتیجه، این یک اتفاقِ غیرمعمول نمی‌باشد، بسته به هدف و ماهیت تراکنش کسب و کار که افراد (و قسمت‌های مربوطه) در حوزه‌های قضایی مختلف دارند و مجموعه‌های چندگانه از محدودیت‌های خارجی که

1- Legal entity
2-Perspective
3- Overlap
4- Liability
5- Responsibility

به‌کار برده می‌شوند، و هم‌پوشانی رخ خواهد داد. وجود هم‌پوشانیِ محدودیت‌های خارجی و / یا تضاد میان این مجموعه محدودیت‌های خارجی نیز امری غیر معمول نمی‌باشد. این مورد با توجه به قوانین و مقررات ماهیت حفاظت از حریم خصوصی نیز می‌باشد. حل و فصل مسائلی از این قبیل، خارج از هدف و دامنه کاربرد این استاندارد ملی می‌باشد.

اگرچه، مدل‌سازی تراکنش کسب و کار با در نظر گرفتن سناریو و عناصر سناریو به عنوان مباحث قابل استفاده مجدد، می‌تواند روش‌شناسیِ مفیدی در شناسایی هم‌پوشانی‌ها و تضادها باشد (از طریق بکارگیری به عنوان ابزاری برای هماهنگی آنها، تنها با مفهوم یک تراکنش خاص).

کاربردِ فنونِ توصیفِ معناییِ کسب و کار در قوانین و مقررات حوزه‌های قضایی و مدل‌سازی مجموعه محدودیت‌های خارجی به عنوان سناریو و عناصر سناریو، گامی اساسی در کاربرد آنها به شیوه‌ای نظام‌مند[1] در تراکنش‌های (الکترونیکی) کسب و کار (و به ویژه دولت- الکترونیک، تجارت- الکترونیک، آموزش- الکترونیک و غیره) می‌باشد.
روش‌شناسی‌های فنونِ توصیفِ توافقِ کسب و کارِ ویرایش- باز را می‌توان به عنوان ابزاری برای هماهنگی و تسهیل محدودیت‌های خارجی برخاسته از حوزه‌های قضایی به‌کار برد.

یادآوری- این استاندارد ملی بر مبنای فرضیات زیر می‌باشد:

۱) الزامات حفاظت از حریم خصوصی فرد، به عنوان خریدار در تراکنش کسب و کار، الزاماتی از حوزه قضایی هستند که در آن شخص تعهدات مرتبط با تراکنش کسب و کار معرفی شده را ایجاد می‌کند؛ و،
۲) جایی‌که فروشنده در حوزه قضایی دیگری غیر از حوزه قضایی فرد خریدار باشد، این ویرایش از این استاندارد ملی دربرگیرنده و پشتیبان «راهنماهای[2] در حفاظت از حریم خصوصی و جریان‌های داده‌های ارتباطات میان مرزی برای اطلاعات شخصی » می‌باشد.[به زیر بند ۲-۲ مراجعه شود].

۱-۲-۵ اطلاعات شخصی در دسترس عموم

قسمت مستثنی شده از هدف و دامنه کاربرد این استاندارد ملی، «اطلاعات شخصی در دسترس عموم» یا (PAPI)[3] می‌باشد. در مفهوم تراکنش کسب و کار، فروشنده اقدام به جمع‌آوری اطلاعات شخصی از این قبیل در مورد فرد (به خصوص در «مرحله برنامه‌ریزی» از فرآیند کسب و کار) نمی‌نماید.

برای مثال، فروشنده در تبلیغ محصول برای بازار می‌تواند:

۱) اطلاعات شخصی که جزء اطلاعات شخصی در دسترس عموم می‌باشند، را منتشر نماید. مانند آنچه در دفترچه‌های راهنمای تلفن یافت می‌شود.
۲) از طریق مقرراتی بر پایه قوانین یا مقررات قابل اجرای حوزه قضایی، از هرگونه اطلاعات شخصی اعلام شده برای اطلاع عموم بهره ببرد؛ و، یا

1- Systematic manner
2- OECD
3- Publicly Available Personal Information

۳) از اطلاعات خود شخص، آنها را در دسترس عموم قرار داده است، شامل شود. (برای مثال از طریق یک یا چند برنامه اینترنتی مانند "Facebook").

مفهوم حفاظت از حریم خصوصی، اطلاعات شخصی در دسترس عموم مطابق زیر تعریف می‌شود:

اطلاعات شخصی در دسترس عموم(PAPI)

اطلاعات شخصی یک فرد است که فرد آنها را با آگاهی در دسترس عموم قرار می‌دهد یا در دسترس قرار گرفتن آنها را اجازه می‌دهد یا به طور قانونی از الف) اطلاعات ثبتی دولت که در دسترس عموم است یا ب) اطلاعاتی که از جانب قانون در دسترس عموم قرار می‌گیرد، دسترسی داشته و بدست آورده است.

مثال ۱- مثال‌هایی از اطلاعات شخصی که فرد آنها را با آگاهی در دسترس عموم قرار می‌دهد یا در دسترس قرار گرفتن آنها را اجازه می‌دهد شامل: اطلاعات موجود در دفترچه‌های راهنمای تلفن عمومی، تبلیغات در روزنامه‌ها، موارد منتشر شده، پیغام‌هایی با مضمون مشابه که در محیط اینترنت گذاشته می‌شوند و غیره.

مثال ۲- مثال‌هایی از اطلاعات ثبتی دولت که در دسترس عموم قرار می‌گیرد شامل: ثبت نام افرادی که در رأی‌گیری، خرید یا فروش دارایی‌ها شرکت دارند یا هرگونه اطلاعات شخصی دیگر که مورد درخواست حوزه قضایی در دسترس عموم می‌باشد.

تشخیص اینکه اطلاعات شخصی از نوع اطلاعات حقیقی[1] می‌باشند یا خیر، مستثنی شده از هدف و دامنه کاربرد این استاندارد ملی می‌باشد.

۱-۳ جوانبی که در حال حاضر مورد بررسی قرار نمی‌گیرند

این استاندارد ملی بر روی جنبه‌های اساسی و بنیادی الزامات حفاظت از حریم خصوصی متمرکز می‌باشد. هدف از این بند، شناسایی جوانبی است که در حال حاضر مورد توجه قرار نمی‌گیرند. این موارد در قسمت‌های زیر نیز مورد بحث قرار خواهند گرفت:

الف) اصلاحیه‌ای بر این استاندارد ملی،
ب) ویرایش‌های جدید این استاندارد ملی،
پ) از طریق قسمت جدیدی از این استاندارد ملی،
ت) در ویرایشی جدید از قسمت موجود این استاندارد ملی (در صورت کاربرد).
ث) از طریق ویرایشی جدید از استانداردهای موجود ISO/IEC JTC1، یا استاندارد موجود دیگر در ISO/ IEC JTC1/SC ، یا ISO، IEC یا ITU؛ و / یا،
ج) استاندارد(های) جدید هر یک از کمیته‌های اشاره شده در بالا.

این استاندارد ملی الزامات زیر را نیز مورد بررسی قرار می‌دهد:

1 -PAPI

۱) تفاوت در برابری استفاده از زبان‌های رسمی توسط فرد، در آگاهی یافتن و اعمال حقوق حریم خصوصی در یک حوزه قضایی[۱]؛

۲) تعامل میان حفاظت از حریم خصوصی و الزامات حمایت از مصرف کننده به عنوان دو مجموعه از محدودیت‌های خارجی کاربردی برای فرد خریدار در یک تراکنش کسب و کار.

۳) شناسایی و ثبت طرح‌واره‌های شامل کنترل و مدیریت نام‌های قانونی به رسمیت شناخته شده (LRNs) به عنوان اشخاص و شناساگرهای منحصر بفرد مرتبط، برای شناسایی بدون ابهام یک فرد و/ یا شرایط نقش فرد در یک مفهوم خاص.

۴) مدیریت اطلاعات کامل‌شده و الزامات ممیزی مربوط به حصول اطمینان از حفاظت اطلاعات شخصی، باید به‌وسیله سازمان‌ها و ادارات عمومی به‌عنوان طرف‌های یک تراکنش کسب و کار، به تصویب رسیده باشد.

۵) قوانینِ کامل‌شده و متن مربوط به آن در رابطه با چشم اندازBOV با در نظر گرفتن جریان‌های داده میان مرزی اطلاعات شخصی.

۶) عملکرد متقابل میان حوزه‌های قضایی که دارای معادل‌های مشخصی برای الزامات حفاظت خود (قابلیت همکاری) نمی‌باشند یا فقط دارای الزامات حفاظت متفاوتی می‌باشند.

۷) نمونه‌هایی از تداوم استفاده از الزامات حفاظت در رابطه با اطلاعات شخصی یک فرد پس از فوت وی.

به علاوه، از دیدگاه تراکنش کسب و کار، در الزامات حفظ حریم خصوصی می‌تواند پیوستگی وجود داشته باشد، (برای مثال مواردی که مربوط به جنبه‌های موقت جنبه‌های پس از- تحقق[۲] یک تراکنش کسب و کار می‌باشد، (برای مثال مسائل مربوط به مراقبت‌های بهداشتی، ضمانت نامه‌های محصولات، قراردادهای خدمات، حقوق (شامل IP) و غیره.) تراکنش‌های کسب و کار ممکن است نیازمند حفظ اطلاعات شخصی و تداوم حفاظت از آن پس از فوت شخص باشند.

یادآوری ۱- این امر ممکن است در بر گیرنده حل و فصل مسائل مربوط به وصیت نامه‌ها[۳]، انحصار وراثت[۴]، سرمایه گذاری‌ها[۵] و غیره در ارتباط با شخص فوت شده باشد.

---

[۱] - این استاندارد ملی بر جنبه‌های ابتدایی و ضروری حوزه‌های قضایی به عنوان منابع محدودیت‌های خارجی تمرکز دارد، همچنین این نگارش از این استاندارد ملی به بررسی تفاوت وضعیت میان زبان‌های رسمی موجود که ممکن است در یک حوزه قضایی وجود داشته باشد نمی‌پردازد. جایی‌که یک حوزه قضایی دارای سه زبان رسمی و یا بیشتر می‌باشد، غیرمعمول نیست که تمامی این زبان‌ها دارای وضعیت‌های مشابه نباشند. برای مثال، برای استفاده از برخی زبان(های) رسمی در یک حوزه قضایی، معیارهایی اعم از « چه‌وقت و کجا اعداد معتبرند» ، «تقاضای قابل توجهی برای برقراری ارتباط و خدمات به آن زبان، از یک اداره عمومی وجود دارد » و غیره می‌تواند وجود داشته باشد. این امور هم زبانی را که اطلاعات شخصی، توسط آن در ادارات عمومی و یا سازمان‌ها به ثبت رسیده و هم زبان ارتباطات فرد با سازمان‌ها در تراکنش کسب و کار را تحت تاثیر قرار می‌دهند.

1-Post-actualization
2- Wills
3- Pribate
4- Investments

یادآوری ۲- فیلد اطلاعات مالیات که ۶-۴ سال الزامات حفظ سابقه در بیشتر حوزه‌های قضایی را دارد. در برخی حوزه‌های قضایی، امور مالیاتی محرمانه بوده و در برخی دیگر عمومی می‌باشد. وضعیت اطلاعات شخصی، ممکن است به عنوان نتیجه‌ای از دعوی قضایی[1] و دادرسی عمومی[2]، تغییر یابد.

یادآوری ۳- تراکنش‌های کسب و کار ممکن است به نگهداری اطلاعات شخصی و تداوم در حافظت از آنها پس از فوت فرد نیاز داشته باشند، (برای مثال بسیاری از توافق‌نامه‌های مربوط به کارت‌های اعتباری پس از فوت دارنده کارت اعتباری نیز برقرار می‌باشند).

یادآوری ۴- ممکن است کسی بلافاصله پس از فوت به افزودن یک بند دیگر در حفاظت از حریم خصوصی و اطلاعات شخصی افراد نیاز داشته باشد.

۸) اطلاعات شخصی یافت شده در گزارش‌های روزنامه ای[3]:

کاربرد اطلاعات شخصی در تراکنش کسب و کار که در گزارش‌های روزنامه‌ای شامل موارد خبری، پخش عمومی، موارد منتشر شده توسط رسانه‌های خبری در رابطه با یک فرد، اطلاعات شخصی منتشر شده که از طریق طرف‌های سوم در محیط اینترنت قرار می‌گیرند، (برای مثال از طریق Google، Facebook، Twitter و غیره) که در برخی حوزه‌های قضایی برای «منافع عمومی» نگهداری می‌شوند، شامل این استاندارد ملی نمی‌شود.

دلایل این پیشگیری را می‌توان در این دانست که یک گزارش روزنامه‌ای شامل اطلاعات شخصی، در رابطه با فرد می‌باشد که:

- ممکن است شامل اطلاعات نادرست و ادعاها باشد، بنابراین نباید (و نمی‌تواند) به عنوان« اطلاعات شخصی» به‌کار برده شود.
- ممکن است توسط فرد در معرض اتهام و یا دیگر اقدامات قانونی باشد.
- غیره.

دیگر امور مرتبط با حفاظت از حریم خصوصی درمقابل گزارش‌های روزنامه‌ای برای افراد مشخص که منجر به انتشار اطلاعات شخصی می‌شود، یک « محدوده خاکستری » می‌باشد که دادگاه‌ها در حوزه‌های مختلف قضایی به بررسی آن می‌پردازند و بنابراین هنوز حل و فصل نشده است.

۹) این استاندارد ملی به بررسی مساله توافق که بحث شد نمی‌پردازد، بلکه به آسان‌ترین حالتی‌که یک سناریو ممکن است ثبت گردد که شامل نوع خاصی از توافق در درون آن است، را در نظر می‌گیرد.

۱۰) استفاده از مشخصه‌ها و خواص زیستی یک فرد که نیاز به حضور فیزیکی فرد می‌باشد و به صورت فیزیکی در یک محتوای مشخص و برای یک نقش مشخص از فرد گرفته می‌شود.

1- Litigation
2- Public hearings
3- Journalistic reports

این امر شامل استفاده از زیست سنجی، زیستی (مثل نمونه‌های مو، خون و DNA)، سوابق دندان‌پزشکی و غیره می‌باشد.

۱۱) کاربرد حقوق افرادی که طبق بیانیه « کنوانسیون سازمان ملل متحد در مورد حقوق افراد دارای ناتوانی » در سال ۲۰۰۶ [۱] ناتوان اعلام شده باشند.

یکی از مواردی که اهمیت ویژه‌ای دارد، این است که کنوانسیون سازمان ملل متحد، مبنای کار خود را پشتیبانی از افراد دارای معلولیت می‌داند که به اعضای کاملا کارا برای جامعه تبدیل شوند، بدان معنی که اطلاعات ضروری برای این افراد ناتوان برای این‌که قادر به ایجاد تعهداتی از جمله تعهدات یک تراکنش کسب و کار باشند، باید به شکل و قالبی در دسترس قرار گیرد که معانی به‌طور کامل، منتقل شده و فرد قادر به داشتن توافق آگاهانه باشد و غیره.

۱۲) این استاندارد ملی به بررسی نقش «دیوان عدالت اداری[۲]»، «مامور عالی رتبه[۳] در حریم خصوصی»، «مامور عالی رتبه در حفاظت داده» و غیره نمی‌پردازد. که به عنوان یک حاکم مستقل در رسیدگی به شکایات عمل می‌کند و انطباق با الزامات حفاظت از حریم خصوصی (از جمله درون یک سازمان یا ادارات عمومی) را تضمین می‌نماید ؛

بسیاری از حوزه‌های قضایی نقش دیوان عدالت اداری که ممکن است نقشی مشابه در ادارات عمومی باشد را فراهم می‌نمایند.

۱۳) قوانین کامل‌شده مربوط به استفاده از نمایندگان و/ یا طرف‌های سوم توسط فروشندگان در یک تراکنش کسب و کار

این مورد در برگیرنده صلاحیت و تضمین انطباق آنها با الزامات حفاظت از حریم خصوصی مربوط به اطلاعات شخصی در یک تراکنش کسب و کار می‌باشد.

۱۴) نماینده‌ای که از جانب یک شخص عمل می‌نماید

ممکن است فرد نماینده‌ای را درخواست نماید که از جانب او عمل نماید و این امر می‌تواند شامل تقاضای فرد برای فاش ننمودن هویت و یا هرگونه اطلاعات شخصی‌اش باشد یا نباشد. برای مثال بعنوان یک «مشتری» ناشناس برای نماینده تلقی شود.

۱۵) قوانین کامل‌شده‌ی حاکم بر الزامات برای علامت گذاری (یا برچسب زدن) سطح عناصر داده (یا فیلدها) که قسمتی از اطلاعات شخصی را برای یک فرد به صورتی که مورد درخواست تراکنش(های) کسب و کار و BTI مربوط به آن می‌باشد، تشکیل می‌دهند.

---

[۱] - بیشتر حوزه‌های قضایی و نه همه آن‌ها، از اعضای نوع P کمیته ISO/IEC JTC1 هستند که این کنوانسیون را در سازمان ملل متحد امضا نموده‌اند و الزامات سازمان ملل متحد را با قوانین داخلی کشور خود تصویب می‌نمایند.

[۲] - مقام دولتی که به بررسی شکایات مردم علیه دولت می پردازد. (ombudsperson)

1- Commissioner

۱۶) ادغام‌ها[۱] و تصرف‌ها[۲]

اینگونه فرض می‌شود که وقتی سازمان «الف» با سازمان «ب» ادغام و یا به تصرف آن در می‌آید، الزامات حفاظت از حریم خصوصی که تحت کنترل سازمان « الف » بوده است، در مورد اطلاعات شخصی به اجرا در آمده و اجباری است. همچنین فرض می‌شود، اطلاعات شخصی که تحت کنترل سازمان « الف » بوده است، همچنان تحت کنترل آن سازمان باقی مانده و ادغام شدن با سازمان « ب » و یا به تصرف آن در آمدن، سازمان « ب » را برای دسترسی به اطلاعات شخصی افراد و / یا استفاده از اطلاعاتی که توسط سازمان « الف » نگهداری می‌شود، بدون اعلام نمودن و داشتن رضایت آگاهانه از افرادی که اطلاعات شخصی آن‌ها در سازمان « الف » بوده/هست، مجاز نمی‌نماید.

۱۷) فناوری اطلاعات و ارتباطات (ICT) [۳] و دیگر ارائه کنندگان خدمت

این‌گونه فرض می‌شود که ارائه کنندگان خدمات (یا دیگر) ICT که تحت قرارداد ارائه خدمات ICT به سازمان و یا اداره عمومی (که اطلاعات شخصی را تحت کنترل خود دارد) می‌باشند، به اطلاعات شخصی افراد که به عنوان قسمتی از خدمات ارائه شده به آن سازمان عمل می‌نمایند، نباید دسترسی داشته باشند یا از آن‌ها استفاده نمایند، مگر اینکه توافقنامه قراردادی و رسمی در تطابق با الزامات کاربردی حفاظت از حریم خصوصی داشته باشند.

۱۸) داده کاوی[۴]

این‌گونه فرض می‌شود که یک سازمان باید اطمینان حاصل نماید که هرگونه فعالیت داده کاوی که توسط آن (یا از طریق نماینده یا طرف سوم از جانب سازمان) انجام می‌شود، باید در تطابق با الزامات کاربردی حفاظت از حریم خصوصی باشد و هیچ‌گونه استفاده ثانویه یا هر استفاده دیگری از اطلاعات شخصی را در صورتی که افراد رضایت را به‌روشنی اعلام نکرده باشند، شامل نشود.

۱۹) بیانیه‌های انطباق رسمی

بند ۱۳ در ارتباط با الزامات انطباق در بیشترین سطوح ابتدایی می‌باشد. بیانیه‌های انطباق رسمی کامل‌شده به همراه قوانین و رویه‌های مرتبط با پیاده سازی مورد نیاز می‌باشند. همچنین لازم است تا از « مورد تأیید بودن[۵] » هرگونه بیانیه انطباقی که توسط سازمان یا ادارات عمومی اعلام شده است، اطمینان حاصل شود.

۲۰) پیوندها و شباهت‌ها میان الزامات حفاظت از حریم خصوصی و الزامات حمایت از مصرف کننده

2- Mergers
3- Acquisitions
1- Information and Communication Technology
2- Data mining
3- Vrifiable

بسیاری از محدودیت‌های خارجی مربوط به اطلاعات شخصی که دارای ماهیت حفاظت از حریم خصوصی در تراکنش کسب و کار می‌باشند، مشابه الزامات حمایت از مصرف کنندگان می‌باشند.{به زیربند ۷-۲-۲ مراجعه شود}.

انتظار می‌رود که برخی یا همه این الزامات در ویرایش‌های بعدی این استاندارد ملی یا استانداردهای هماهنگ یا گزارش‌های فنی (شامل قسمت‌های جدید و ممکن از استاندارد ISO/IEC 15944) مورد بررسی قرار گیرد.

۱-۴ بی‌طرفی محیط سامانه‌های فناوری اطلاعات [1]

این استاندارد ملی هیچگونه محیط سامانه مشخص، سامانه مدیریت پایگاه داده، الگوی طراحی پایگاه داده[2]، روش‌شناسی توسعه سامانه، زبان تعریف داده‌ها، زبان فرماندهی، واسط سامانه، واسط کاربر، ترکیب، طرح محاسباتی یا هرگونه فناوری مورد نیاز برای پیاده‌سازی را فرض و یا تأیید نمی‌کند، به بیان دیگر در فناوری اطلاعات بی‌طرف می‌باشد. این استاندارد ملی همزمان، دسترسی به فناوری اطلاعات فعال‌شده برای پیاده-سازی و قابلیت همکاری معنایی را بیشینه می‌نماید[3].

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 می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آنها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ مراجع از ISO/IEC , ISO و ITU

2-1 ISO 639-2:1998(E/F), *Codes for the representation of names of languages — Part 2: Alpha-3 code/Codes pour la représentation des noms de langue — Partie 2: Code alpha-3*

2-2 ISO 1087-1:2000(E/F), *Terminology work — Vocabulary — Part 1: Theory and application/Travaux terminologiques — Vocabulaire — Partie 1: Théorie et application*

2-3 ISO/IEC 2382 (all parts) (E/F), *Information technology — Vocabulary/Technologies de l'information — Vocabulaire*

2-4 ISO 3166-1:2006(E/F), *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes/Codes pour la représentation des noms de pays et de leur subdivisions — Partie 1: Codes pays*

1- IT-systems environment neutrality
2- Datebase design paradigm
3- Maximizes

2-5 ISO 3166-2:2007(E/F), *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code/Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 2: Code pour les subdivisions de pays*

2-6 ISO 5127:2001(E), *Information and documentation — Vocabulary*

2-7 ISO/IEC 5218:2004(E/F), *Information technology — Codes for the representation of human sexes/ Technologies de l'information — Codes de représentation des sexes humains*

2-8 ISO/IEC 6523-1:1998(E/F), *Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes/Technologies de l'information — Structures pour l'identification des organisations et des parties d'organisations — Partie 1: Identification des systèmes d'identification d'organisations*

2-9 ISO/IEC 6523-2:1998(E/F), *Information technology — Structure for the identification of organizations and organization parts — Part 2: Registration of organization identification schemes/Technologies de l'information — Structures pour l'identification des organisations et des parties d'organisations — Partie 2: Enregistrement des systèmes d'identification d'organisations*

2-10 ISO/IEC 7501-1:2008(E), *Identification cards — Machine readable travel documents — Part 1: Machine readable passport*

2-11 ISO/IEC 7501-2:1997(E), *Identification cards — Machine readable travel documents — Part 2: Machine readable visa*

2-12 ISO/IEC 7501-3:2005(E), *Identification cards — Machine readable travel documents — Part 3: Machine readable official travel documents*

2-13 ISO/IEC 7812-1:2006(E), *Identification cards — Identification of issuers — Part 1: Numbering system*

2-14 ISO/IEC 7812-2:2007(E), *Identification cards — Identification of issuers — Part 2: Application and registration procedures*

2-15 ISO 8601:2004(E), *Data elements and interchange formats — Information interchange — Representation of dates and times*

2-16 ISO/IEC 14662:2010(E/F), *Information technology — Open-edi reference model/Technologies de l'information — Modèle de référence EDI-ouvert*

2-16 ISO/IEC 15944-1:2011(E), *Information technology — Business Operational View — Part 1: Operational aspects of Open-edi for implementation*

2-17 ISO/IEC 15944-2:2006(E), *Information technology — Business Operational View — Part 2: Registration of scenarios and their components as business objects*

2-18 ISO/IEC 15944-4:2007(E), *Information technology — Business Operational View — Part 4: Business transactions and scenarios — Accounting and economic ontology*

2-19 ISO/IEC 15944-5:2008(E), *Information technology — Business Operational View — Part 5: Identification and referencing of requirements of jurisdictional domains as sources external constraints*

2-20 ISO/IEC 15944-7:2009(E), *Information technology — Business Operational View — Part 7: eBusiness vocabulary*

2-21 ISO 19108:2002(E), *Geographic information — Temporal schema*

2-22 ISO/IEC 19501:2005(E), *Information technology— Open Distributed Processing — Unified Modeling Language (UML) Version 1.4.2*

2-23 ISO 22857:2004(E), *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information*

۲-۲ ویژگی‌های مراجع

APEC Privacy Framework. (2005)

Charter of the United Nations (as signed 1945 and Amended 1965, 1968, and 1973+), United Nations (UN).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) Directive

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

UN Convention on the Rights of Disabled Persons (2006+)

Vienna Convention of the Law of Treaties (1969), United Nations (UN)

کلیه بندهای استاندارد بین‌المللی ISO/IEC 15944-8:2012 در مورد این استاندارد معتبر و الزامی است.