نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

مقالهٔ ترویجی

حسابرسی رعایت سیستم‌های اطلاعاتی تحت مقررات عمومی حفاظت داده‌ها: تضمین رعایت و ارتقای حفاظت‌داده‌های شخصی[۱،۲]

بیتا مشایخی*[۳] و مهدی صفایی[۴]

نشریه علمی حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال اول، پیاپی۱، بهار و تابستان ۱۴۰۴
صص۱۱۷ - ۱۴۴

تاریخ دریافت: ۱۴۰۳/۱۱/۲۸
تاریخ بازنگری: ۱۴۰۴/۰۵/۱۶
تاریخ پذیرش: ۱۴۰۴/۰۶/۱۱

چکیده

پژوهش حاضر، به بررسی جامع تأثیر مقررات عمومی حفاظت داده‌ها بر حسابرسی سیستم‌های اطلاعاتی می‌پردازد تا نقش کلیدی این مقررات در تضمین رعایت استانداردها و تقویت زیرساخت‌های امنیت داده‌ها را به‌طور دقیق تحلیل کند. با توجه به تغییرات گسترده‌ای که این مقررات در ساختارهای نظارتی ایجاد خواهد نمود، در این مطالعه چارچوب‌های قانونی آن و تأثیر آنها بر رویکرد حسابرسی سیستم‌های اطلاعاتی و مدیریت ریسک مورد تحلیل قرار گرفته است. در این راستا، ابتدا چارچوب‌های نظارتی موجود و ساختار اجرایی این مقررات و همچنین نحوه انطباق سازمان‌ها با الزامات آن، چالش‌های موجود و فرصت‌های پیش‌رو مورد بررسی قرار می‌گیرد. سپس، تأثیرات آن بر حسابرسی سیستم‌های اطلاعاتی، امنیت داده‌ها و فرآیندهای مدیریت ریسک تحلیل شده است. یافته‌های پژوهش نشان می‌دهد که رعایت الزامات مقررات عمومی حفاظت داده‌ها در فرآیندهای حسابرسی نه تنها به هم‌راستایی سازمان‌ها با مقررات منجر می‌شود، بلکه سطح حاکمیت داده‌ها و امنیت اطلاعات را نیز بهبود می‌بخشد. همچنین، پژوهش، بر نقش فناوری‌های نوین حسابرسی در بهینه‌سازی فرآیندهای نظارتی و افزایش کارایی حسابرسی‌های مرتبط با حفاظت داده‌ها تأکید می‌کند. با بهره‌گیری از تحلیل‌های ارائه‌شده، سازمان‌ها می‌توانند استراتژی‌های بهتری را برای افزایش شفافیت، کاهش ریسک‌های نظارتی و بهبود پاسخگویی در محیط‌های پیچیده داده‌محور، تدوین کنند.

واژه‌های کلیدی: *حسابرسی سیستم‌های اطلاعاتی، حسابرسی رعایت، مقررات عمومی حفاظت‌داده‌ها (GDPR).*
طبقه‌بندی موضوعی: *M42, M48, K20, L68.*

---

[1] https://doi.org/10.22034/JISTA. 2025.505314.1019

[۲]. مقاله منتخب دومین کنگره حسابرسی فناوری اطلاعات و اعتماد دیجیتال

[۳] استاد حسابداری، گروه حسابرسی، دانشکده حسابداری و علوم مالی، دانشکدگان مدیریت، دانشگاه تهران، تهران، ایران. (نویسندهٔ مسئول).
Email: mashaykhi@ut.ac.ir

[۴] دانشجوی دکتری، گروه حسابداری، دانشکده حسابداری و علوم مالی، دانشکدگان مدیریت، دانشگاه تهران، تهران، ایران. Email: safaei.mahdi@ut.ac.ir

مقدمه

در دوره‌ای که داده‌ها به شریان حیاتی اقتصادهای مدرن تبدیل شده‌اند، استفاده روزافزون از داده‌های کاربران به منظور رشد کسب‌وکار و تأثیرگذاری بر مشتریان توسط شرکت‌ها به حداکثر رسیده است. داده‌های شخصی به‌عنوان منبعی برای تحلیل‌های دقیق، پیش‌بینی روندهای بازار، بهبود خدمات، شخصی‌سازی تجربه مشتری و در نهایت ایجاد ارزش افزوده برای کسب‌وکارها عمل می‌کنند. بنابراین، داده‌ها در این زمینه به عنوان منبع کلیدی برای دستیابی به اهداف تجاری و رقابتی در دنیای مدرن اقتصاد دیجیتال شناخته می‌شوند. حفاظت از اطلاعات شخصی به یک موضوع حیاتی تبدیل شده است. مقررات عمومی حفاظت داده‌ها[1] (از این پس GDPR) که توسط اتحادیه اروپا تدوین شده است، چارچوبی را برای حفاظت از حریم‌خصوصی و داده‌های شخصی در اتحادیه اروپا ارائه می‌دهد. GDPR که در تاریخ ۲۵می۲۰۱۸ به اجرا درآمد، چارچوب نظارتی مهمی را ارائه می‌دهد که به منظور یکسان‌سازی قوانین حفاظت‌داده‌ها در اتحادیه اروپا طراحی شده است و به چالش‌های ناشی از پیشرفت‌های سریع فناوری پاسخ می‌دهد. این مقررات، الزامات سخت‌گیرانه‌ای را به سازمان‌هایی که داده‌های شخصی را پردازش می‌کنند، بدون توجه به موقعیت جغرافیایی آنها، تحمیل می‌کند، مشروط بر این‌که داده‌های متعلق به ساکنان اتحادیه اروپا را مدیریت کنند(آمو و همکاران[2]، ۲۰۲؛ شریفی کیا و شعبانی جهرمی، ۱۴۰۱).

اهمیت GDPR فراتر از رعایت قانونی است؛ این مقررات بر اهمیت ایجاد اعتماد و مسئولیت‌پذیری در دنیایی تأکید دارد که به‌طور فزاینده به داده‌ها وابسته می‌شود. نقض‌های داده‌ای، سوءاستفاده از اطلاعات شخصی و تدابیر ناکافی امنیتی آگاهی عمومی و نظارت‌های قانونی را افزایش داده و نیاز به سازوکارهای قوی برای تضمین رعایت را ضروری کرده است (برتولاکچینی و همکاران[3]، ۲۰۲۳).

با بررسی رویکردها و گونه‌شناسی کشورها سه رویکرد قانون‌گذاری برای حفظ حریم‌خصوصی اطلاعاتی شناسایی شد: ۱. کشورهای فاقد قوانین مدون(پاکستان، گواتمالا، هند،

[1] General Data Protection Regulation (GDPR)
[2] Amoo et al.
[3] Bertolaccini et al.

ترکیه، مالزی، مکزیک، فیلیپین، سنگاپور ونزوئلا) ۲. کشورهای دارای قانون‌گذاری بخشی[1] (ایالات متحده آمریکا و ژاپن) و ۳. کشورهای دارای قانون‌گذاری یکپارچه[2] (کره جنوبی، استرالیا، کانادا، اتریش، بلژیک، فرانسه، ایتالیا، کانادا، دانمارک، فنلاند، آلمان، یونان، بلژیک، نروژ، ایرلند، پرتغال، اسپانیا، سوئد، سوئیس و انگلستان). کشورهایی هم‌چون پاکستان، گواتمالا، هند، ترکیه، مالزی، مکزیک، فیلیپین، سنگاپور و ونزوئلا دارای کمبود قوانین در این حوزه هستند (ریس و همکاران[3]، ۲۰۲۴؛ تراکمن و همکاران[4]، ۲۰۲۰؛ نیسبم[5]، ۲۰۲۰).

براساس مطالعه رویکردها، دو رویکرد متفاوت در فضای حفاظت‌داده‌های کاربران وجود دارد که یکی از آن‌ها رویکرد ایالات متحده آمریکا و دیگری رویکرد اروپایی است (سیم و همکاران[6]، ۲۰۲۳). ایالات متحده آمریکا در فناوری اطلاعات و اینترنت هم از نظر فنّی و زیرساختی و هم از نظر قانون‌گذاری نسبت به دیگر کشورها پیشتاز بوده است، اما به نظر می‌رسد سیاست‌ها و قوانین این کشور دارای خلأهای زیادی در حوزه حفاظت از حریم‌خصوصی کاربران در فضای مجازی است. ایالات متحده آمریکا به دلیل اتخاذ روش موردی برای قانون‌گذاری درخصوص حریم‌خصوصی و رویکرد خودتنظیمی در بخش‌های مختلف این موضوع، فاقد قانونی جامع در این زمینه است(محمودی و همکاران، ۱۴۰۳). رویکرد اروپایی در مورد حریم‌خصوصی کاربران در فضای مجازی رویکردی یکپارچه است (هوفناگل و همکاران[7]، ۲۰۲۰). در این رویکرد، قوانین جامع و فراگیر در زمینه حمایت از داده‌ها، تعیین مراجع عمومی برای ثبت داده‌ها، پایگاه داده، حل اختلاف، اخذ رضایت قبلی در مورد پردازش برخی داده‌ها و... مد نظر قرار می‌گیرد(کاسترز و همکاران[8]، ۲۰۱۸). بسیاری از کشورهای غیراروپایی همچون استرالیا، کانادا، کره جنوبی، ژاپن و... نیز به تأسی از دیدگاه اروپایی، به تدوین قانونی جامع برای حفاظت از حریم‌خصوصی کاربران در فضای مجازی پرداخته‌اند و در آن، برخلاف ایالات متحده آمریکا، از داده‌های شخصی گردآوری شده توسط نهادهای دولتی نیز حمایت کرده‌اند.

---

[1] Omnibus
[2] Sectoral
[3] Reis et al.
[4] Trakman et al.
[5] Nissenbaum
[6] Sim et al.
[7] Hoofnagle et al.
[8] Custers et al.

GDPR مبتنی بر مجموعه‌ای از اصول اساسی است که بر نحوه جمع‌آوری، پردازش، ذخیره‌سازی و انتقال داده‌های شخصی نظارت دارد (تامبوری[1]، ۲۰۲۰؛ تانکارد[2]،۲۰۱۶؛گیلمن[3]، ۲۰۲۰). برخی از مهم‌ترین اصول این قانون شامل مسئولیت‌پذیری و شفافیت، حداقل‌سازی داده‌ها، حقوق موضوع داده‌ها، امنیت و حفاظت‌داده‌ها و اطلاع‌رسانی و گزارش‌دهی نقض داده‌ها می‌باشند. با توجه به الزامات سخت‌گیرانه GDPR، سازمان‌ها نیازمند اجرای فرآیندهای حسابرسی سیستماتیک برای ارزیابی سطح رعایت، شناسایی نقاط ضعف، بهبود امنیت داده‌ها و کاهش ریسک‌های نظارتی هستند. فرآیند حسابرسی در این زمینه شامل بررسی سیاست‌های حاکمیتی، تحلیل عملکرد تدابیر امنیتی، ارزیابی رعایت حقوق موضوع داده و کنترل فرآیندهای مدیریت ریسک می‌شود.

حسابرسی سیستم‌های اطلاعاتی به عنوان شروع رعایت GDPR ظاهر می‌شود و رویکردی ساختاریافته برای ارزیابی و بهبود شیوه‌های حفاظت‌داده‌های سازمان‌ها ارائه می‌دهد. با ارزیابی سیستم‌ها، فرآیندها و سیاست‌ها به صورت سیستماتیک، حسابرسی‌سیستم‌های‌اطلاعاتی، امکان عملی برای کاهش ریسک‌ها، بهبود شفافیت و تطابق شیوه‌های سازمانی با الزامات GDPR ارائه می‌دهد (تامبوری، ۲۰۲۰؛ گوبیو و همکاران[4]، ۲۰۲۲).

این پژوهش، از رویکردی تطبیقی برای بررسی اثرات GDPR بر حسابرسی سیستم‌های اطلاعاتی استفاده می‌کند، چراکه رعایت این مقررات نه‌تنها در سطح اتحادیه اروپا بلکه در بسیاری از کشورها و سازمان‌های بین‌المللی نیز به‌عنوان یک چالش مطرح است. مطالعات تطبیقی، که به‌وفور در تحقیقات حقوقی و مقرراتی مشاهده می‌شوند، امکان تحلیل دقیق‌تر شکاف‌های نظارتی، چالش‌های اجرایی و راهبردهای موفق را در حوزه رعایت GDPR فراهم می‌آورند.

در پژوهش حاضر، ضمن تحلیل چارچوب‌های قانونی GDPR، به بررسی تأثیر این مقررات بر شیوه‌های حسابرسی سیستم‌های اطلاعاتی و راهبردهای مدیریت ریسک پرداخته شده است. ساختار مقاله با تمرکز بر اصول کلیدیGDPR، نقش حسابرسی رعایت در تضمین

[1] Tamburri
[2] Tankard
[3] Gilman
[4] Gobeo et al.

امنیت داده‌ها، چالش‌های اجرایی سازمان‌ها و آینده استانداردهای حسابرسی تنظیم شده است تا تصویر جامعی از ارتباط میان قانون GDPR و حرفه و ابعاد حسابرسی ارائه دهد.

در ادامه، ابتدا مبانی قانونی و اصول حسابرسی رعایت مورد بررسی قرار گرفته، سپس ابعاد اجرایی نظارت و کنترل در سطوح حکمرانی داده‌ها، مدیریت ریسک، حقوق موضوع داده، تدابیر فنّی و نظارت بر اشخاص ثالث تحلیل شده است. این ساختار به‌گونه‌ای تنظیم شده که ضمن ارائه چارچوبی تطبیقی برای بررسی نقش GDPR در حسابرسی رعایت، تصویر جامعی از چالش‌ها، استانداردهای جهانی و جهت‌گیری‌های آتی نیز ارائه شود.

حسابرسی رعایت GDPR

حسابرسی رعایت GDPR، یک فرآیند حیاتی است که اطمینان حاصل می‌کند سازمان‌ها به الزامات سخت‌گیرانه حفاظت‌داده‌های شخصی تحت این مقررات پایبند هستند(دونیس[1]، ۲۰۱۷). این حسابرسی به شناسایی نقاط ضعف در رعایت، ارزیابی اثربخشی تدابیر حفاظت‌داده‌ها و کاهش ریسک‌های مرتبط با نقض داده‌ها کمک می‌کند (لا توره و همکاران[2]، ۲۰۲۱).

حسابرسی رعایت، به ارزیابی سیستماتیک رعایت استانداردهای قانونی، نظارتی و داخلی توسط سازمان اشاره دارد. حسابرسی رعایت دو هدف شامل اطمینان از رعایت الزامات نظارتی توسط سازمان‌ها و تقویت فرهنگ مسئولیت‌پذیری و شفافیت در زمینه GDPR دارد(فکیده و همکاران[3]، ۲۰۲۳). اهمیت حسابرسی رعایت تحت GDPR را نمی‌توان نادیده گرفت.

حسابرسی مؤثر رعایت GDPR، به روش‌شناسی‌ها و چارچوب‌های مستقر وابسته است که رویکردهای ساختاریافته‌ای برای ارزیابی شیوه‌های حفاظت‌داده‌ها ارائه می‌دهند. اجزای کلیدی این روش‌شناسی‌ها به این شرح هستند: (۱) چارچوب‌ها و استانداردهای حسابرسی از جمله ایزو۲۷۰۰۱، کوبیت[4] و انجمن ملی فناوری و استانداردها[5] و (۲) رعایت GDPR به عنوان یک ابزار عملی برای حسابرسان.

---

[1] Dounis
[2] La Torre et al.
[3] Fakeyede et al.
[4] Control Objectives for Information and Related Technologies(COBIT)
5 National Institute of Standards and Technology (NIST)

حکمرانی و مدیریت داده‌ها

حکمرانی مؤثر داده‌ها برای رعایت GDPR ضروری است؛ زیرا تعیین می‌کند که داده‌های شخصی چگونه جمع‌آوری، ذخیره، پردازش و به اشتراک گذاشته می‌شوند (پاندیت[1]، ۲۰۲۳). چارچوب‌های مناسب مدیریت داده‌ها به سازمان‌ها کمک می‌کند تا سیاست‌های روشنی را برای طبقه‌بندی داده‌ها، نگهداری و کنترل دسترسی تعیین و از رعایت الزامات قانونی اطمینان حاصل کنند(سارگیتیس[2]، ۲۰۲۴).

GDPR تأثیر عمیقی بر تغییر چارچوب‌های حکمرانی داده‌ها داشته و سازمان‌ها را وادار کرده است تا رویکردهای خود را در مدیریت داده‌ها بازنگری کنند. در اصل، GDPR مسئولیت‌پذیری و شفافیت در چگونگی جمع‌آوری، پردازش، ذخیره‌سازی و حذف داده‌های شخصی را الزامی می‌کند. این موضوع، ادغام اصول حفاظت‌داده‌ها را در هر جنبه‌ای از چارچوب‌های حکمرانی ضروری کرده است(زیچیچی و همکاران[3]، ۲۰۲۲). علاوه بر این، GDPR موجب پذیرش رویکردهای مبتنی بر ریسک در حکمرانی شده است. سازمان‌ها اکنون باید تأثیر فعالیت‌های پردازش داده‌های خود را بر حریم‌خصوصی افراد ارزیابی کنند که معمولاً از طریق ارزیابی‌های تأثیر بر حفاظت‌داده‌ها[4] انجام می‌شود(دمتزو[5]، ۲۰۱۹). این ارزیابی‌ها رویکردی سیستماتیک برای شناسایی و کاهش ریسک‌ها ارائه می‌دهند و اطمینان حاصل می‌کنند که چارچوب‌های حکمرانی به حفاظت‌داده‌ها به عنوان یک هدف اساسی اولویت می‌دهند.

نقش حسابرسی در فهرست‌برداری و طبقه‌بندی داده‌ها

فهرست‌برداری[6] و طبقه‌بندی[7] داده‌ها محور رعایت مؤثر با GDPR را تشکیل می‌دهند و حسابرسی سیستم‌های اطلاعاتی، نقش مهمی در اطمینان از دقت و جامعیت آن‌ها دارد. فهرست‌برداری به سازمان‌ها کمک می‌کند تا انواع داده‌های شخصی که پردازش می‌کنند، منابع این داده‌ها و اهداف استفاده از آن‌ها را شناسایی و فهرست‌برداری کنند. این فهرست جامع برای

[1] Pandit
[2] Sargiotis
[3] Zichichi et al.
[4] Data Protection Impact Assessments (DPIA)
[5] Demetzou
[6] Data Inventory
[7] Data Classification

برآورده کردن الزامات شفافیت و مسئولیت‌پذیری GDPR ضروری است (راهلا و همکاران[1]، ۲۰۲۱). علاوه بر این، حسابرسی، شناسایی داده‌های قدیمی یا غیرضروری را تسهیل می‌کند و به سازمان‌ها این امکان را می‌دهد که سیاست‌های حداقلی‌سازی و نگهداری داده‌ها را به طور مؤثر پیاده‌سازی کنند. حسابرسی، با هم‌راستا کردن شیوه‌های فهرست‌برداری و طبقه‌بندی داده‌ها با اصول GDPR به سازمان‌ها کمک می‌کند تا پایه‌ای محکم را برای رعایت پایدار ایجاد کنند.

حسابرسی سیستم‌های اطلاعاتی، در ارزیابی اثربخشی سیاست‌های نگهداری[2]، که به نحوه نگهداری داده‌های شخصی و زمان حذف آن‌ها می‌پردازند، نقش کلیدی دارد. حسابرسان بررسی می‌کنند که آیا سازمان‌ها دوره‌های نگهداری مشخصی برای دسته‌های مختلف داده‌ها تعیین کرده‌اند و آیا این دوره‌ها با الزامات قانونی، نظارتی و تجاری هم‌راستا هستند یا خیر (راهلا و همکاران، ۲۰۲۱).

ارزیابی و مدیریت ریسک

ارزیابی ریسک، جزء بنیادی از رعایت GDPR است و به سازمان‌ها کمک می‌کند تا به‌طور پیشگیرانه، نقاط ضعف امنیت داده‌ها را شناسایی کنند و کاهش دهند. کسب‌وکارها از طریق چارچوب‌های ساختاریافته مدیریت ریسک می‌توانند احتمال و تأثیر نقض داده‌ها را ارزیابی و تدابیر مناسب را پیاده‌سازی کنند و نشان دهند که مراقبت لازم را انجام داده‌اند. حسابرسی سیستم‌های اطلاعاتی، نقش حیاتی در ارزیابی استراتژی‌های مدیریت ریسک و اطمینان از بهبود مداوم در شیوه‌های حفاظت‌داده‌ها ایفا می‌کند (دشتی و رانیسه[3]، ۲۰۲۰).

ارزیابی‌های ریسک، یکی از ارکان رعایت GDPR هستند و به سازمان‌ها این امکان را می‌دهند که تهدیدات بالقوه برای داده‌های شخصی را شناسایی، ارزیابی و کاهش دهند. GDPR به صراحت از سازمان‌ها می‌خواهد که برای فعالیت‌های پردازش با ریسک بالا، مانند پروفایل‌سازی داده‌های کلان یا استفاده از فناوری‌های نوآورانه، ارزیابی‌های تأثیر بر حفاظت‌داده‌ها انجام دهند. این ارزیابی‌ها به سازمان‌ها کمک می‌کنند تا تأثیر بالقوه فعالیت‌های پردازش داده‌های خود بر حریم‌خصوصی افراد را درک کنند و اقداماتی پیشگیرانه را برای مقابله

[1] Rhahla et al.
[2] Retention Policies
[3] Dashti & Ranise

با ریسک‌ها انجام دهند(کسیرزاده و کلیفورد[1]، ۲۰۲۱). علاوه بر رعایت، ارزیابی‌های ریسک به ایجاد اعتماد با ذینفعان و انجام مسئولیت اجتماعی کمک می‌کنند و نشان‌دهنده تعهد به حفاظت‌داده‌های شخصی هستند. آن‌ها همچنین چارچوبی برای سازمان‌ها فراهم می‌کنند تا منابع و سرمایه‌گذاری‌ها را اولویت‌بندی و بر روی زمینه‌هایی تمرکز کنند که بالاترین ریسک و تأثیر بالقوه را دارند(حجمان و راب[2]، ۲۰۱۸).

نقش حسابرسی سیستم‌های اطلاعاتی در شناسایی آسیب‌پذیری‌ها

حسابرسی سیستم‌های اطلاعاتی ابزاری حیاتی برای شناسایی آسیب‌پذیری‌ها در شیوه‌های حفاظت‌داده‌ها است. حسابرسی با ارزیابی سیستم‌ها، فرایندها و سیاست‌های یک سازمان به طور سیستماتیک، نمای کلی از ریسک‌های بالقوه و مناطق عدم رعایت ارائه می‌دهد(لا توره و همکاران، ۲۰۲۱).

حسابرسی به طور معمول، آسیب‌پذیری‌هایی مانند نرم‌افزارهای قدیمی، کنترل‌های دسترسی یا شیوه‌های رمزگذاری ناکافی را شناسایی می‌کند. به عنوان نمونه، یک حسابرسی ممکن است نشان دهد که داده‌های شخصی حساس از طریق کانال‌های غیررمزگذاری شده منتقل می‌شوند و آن‌ها را در معرض شنود قرار می‌دهند. حسابرسی، با شناسایی این آسیب‌پذیری‌ها، به سازمان‌ها این امکان را می‌دهد که اقداماتی اصلاحی انجام دهند و وضعیت امنیت کلی خود را تقویت کنند.

همچنین، حسابرسی، علاوه بر آسیب‌پذیری‌های فنّی، ریسک‌های سازمانی مانند آموزش ناکافی یا کمبود آگاهی در بین کارکنان را ارزیابی می‌کند. رسیدگی به این مسائل این اطمینان را ایجاد می‌کند که شیوه‌های حفاظت‌داده‌ها در فرهنگ سازمان ادغام شده‌اند و به این ترتیب، احتمال خطای نیروی انسانی را کاهش می‌دهد (ذاکرحسینی، ۱۳۹۹).

پیامدهای نقض داده‌ها و یافته‌های حسابرسی

نقض داده‌ها، یکی از خطرات عمده برای سازمان‌ها تحت GDPR به شمار می‌رود و عواقب شدیدی را برای افراد متأثر و جریمه‌های قابل‌توجهی را برای عدم‌رعایت به همراه دارد. یافته‌های حسابرسی نقش حیاتی در پیشگیری از نقض‌ها دارند و آسیب‌پذیری‌ها را قبل از سوءاستفاده، شناسایی و برطرف می‌کنند. هنگامی‌که نقضی رخ می‌دهد، یافته‌های حسابرسی،

[1] Kasirzadeh & Clifford
[2] Hijmans & Raab

گزارش‌هایی در مورد علل ریشه‌ای و عوامل مؤثر ارائه می‌دهند. به عنوان نمونه، یک حسابرسی ممکن است نشان دهد که رویه‌های ناکافی پاسخ به حوادث یا قابلیت‌های نظارتی ناکافی به نقض کمک کرده‌اند. سازمان‌ها با رسیدگی به این ضعف‌ها می‌توانند تاب‌آوری خود را بهبود بخشند و احتمال وقوع حوادث آینده را کاهش دهند. علاوه بر این، حسابرسی به سازمان‌ها کمک می‌کند تا در پی نقض، مسئولیت‌پذیری خود را نشان دهند. سازمان‌ها با ارائه مدارک مستند از تلاش‌های خود برای رعایت GDPR می‌توانند جریمه‌های نظارتی را کاهش دهند و اعتماد را با ذینفعان بازسازی کنند (گروه آی.جی.پی[1]، ۲۰۲۵).

ادغام اصول حریم خصوصی در سیستم‌های اطلاعاتی

طراحی و پیاده‌سازی حریم‌خصوصی، سازمان‌ها را ملزم می‌دارد که تدابیر حفاظت‌داده‌ها را از ابتدا در سیستم‌ها، فرایندها و خدمات خود، ادغام کنند. این رویکرد پیشگیرانه، ریسک عدم رعایت را به حداقل می‌رساند و اعتماد کاربران را افزایش می‌دهد. **حریم‌خصوصی در طراحی و تنظیمات** (یا به‌طور پیش‌فرض)[2]، اصول بنیادی GDPR هستند که از سازمان‌ها می‌خواهند حفاظت‌داده‌ها را در توسعه و عملیات سیستم‌های خود ادغام کنند. این کار شامل ادغام ملاحظات حریم‌خصوصی در هر مرحله از چرخه توسعه سیستم، از طراحی اولیه تا استقرار و نگهداری است. سازمان‌ها باید اطمینان حاصل کنند که سیستم‌ها به گونه‌ای طراحی شده‌اند که جمع‌آوری، پردازش و ذخیره‌سازی داده‌ها را به حداقل برسانند و به اصل حداقلی‌سازی داده‌ها پایبند باشند. به عنوان نمونه، سیستم‌ها باید تنها داده‌های لازم برای هدف مورد نظر خود را جمع‌آوری کرده و سازوکارهایی را برای حذف ایمن داده‌ها پیاده‌سازی کنند. علاوه بر این، سازمان‌ها باید تنظیمات پیش‌فرضی را پیاده‌سازی کنند که حریم‌خصوصی را در اولویت قرار دهند؛ از جمله این تنظیمات می‌توان به سازوکارهای رضایت اختیاری و اشتراک‌گذاری محدود داده‌ها اشاره کرد (سایانکار[3]، ۲۰۱۳).

---

[1] I. G. P Team

[2] Privacy by design and by default

این اصل به معنای آن است که حریم خصوصی باید از ابتدا و در تمام مراحل طراحی سیستم‌ها لحاظ شود و همچنین پیش‌فرض‌های سیستم باید حداکثر حفاظت از حریم خصوصی را تضمین کنند.

[3] Sayankar

چالش‌های پیاده‌سازی حریم‌خصوصی

پیاده‌سازی حریم‌خصوصی حریم‌خصوصی در طراحی و تنظیمات، به رغم اهمیت آن، چالش‌های قابل‌توجهی را برای سازمان‌ها ایجاد می‌کند. یکی از چالش‌های رایج، نیاز به تعادل بین الزامات حریم‌خصوصی و کارایی و تجربه کاربر است. به عنوان نمونه، کنترل‌های سختگیرانه حریم‌خصوصی ممکن است با نیاز به جمع‌آوری داده‌های کاربر برای شخصی‌سازی یا تجزیه و تحلیل در تضاد باشد (سالتارلا و همکاران[1]، ۲۰۲۱).

چالش دیگر، پیچیدگی سیستم‌های اطلاعاتی مدرن است که اغلب شامل چند لایه فناوری و ادغام‌های شخص ثالث هستند. اطمینان از این‌که اصول حریم خصوصی به طور مداوم در این لایه‌ها اعمال می‌شوند، نیازمند همکاری نزدیک بین تیم‌های فنّی، کارشناسان حقوقی و مسئولان حفاظت‌داده‌ها است (لی و همکاران[2]، ۲۰۲۲). برای غلبه بر این چالش‌ها، سازمان‌ها باید بهترین شیوه‌ها را برای توسعه و حسابرسی سیستم‌های متمرکز بر حریم‌خصوصی، شامل انجام ارزیابی‌های تأثیر بر حفاظت‌داده‌ها در مرحله طراحی، پیاده‌سازی کنترل‌های دسترسی قوی و آزمایش منظم سیستم‌ها برای شناسایی آسیب‌پذیری‌ها اتخاذ کنند.

حقوق موضوع داده و سوابق حسابرسی

GDPR حقوقی مانند حق دسترسی، اصلاح و حذف داده‌های شخصی را به افراد، اعطا می‌کند. سازمان‌ها باید سازوکارهایی را برای حفظ این حقوق برقرار کنند و سوابق (یا زنجیره عطف) حسابرسی را برای نشان دادن رعایت نگهداری نمایند. لاگ‌های حسابرسی، شفافیت در فعالیت‌های پردازش داده‌ها را فراهم و به سازمان‌ها کمک می‌کنند تا به درخواست‌های قانونی و اختلافات حقوقی پاسخ دهند.

GDPR به افراد مجموعه‌ای از حقوق را بر روی داده‌های شخصی خود از جمله حق دسترسی، اصلاح و حذف داده‌های خود فرد تحت عنوان حقوق موضوع داده‌ها[3] اعطا می‌کند. اطمینان از رعایت این حقوق مسئولیتی کلیدی برای سازمان‌ها است و به فرایندهای سیستماتیک برای رسیدگی به درخواست‌های موضوع داده‌ها نیاز دارد (روزنبرگر و همکاران[4]، ۲۰۲۱).

---

[1] Saltarella et al.
[2] Li et al.
[3] Data Subject Rights
[4] Rosenberger et al.

حسابرسی، اثربخشی این فرایندها را ارزیابی و بررسی می‌کند که آیا درخواست‌ها به طور به‌موقع و شفاف رسیدگی می‌شوند یا خیر. به عنوان نمونه، یک حسابرسی ممکن است بررسی کند که سازمان چقدر سریع به درخواست‌های دسترسی پاسخ می‌دهد و آیا توضیحات روشنی از فعالیت‌های پردازش داده‌های خود ارائه می‌دهد یا خیر.

اهمیت نگهداری سوابق حسابرسی

سوابق حسابرسی برای نشان دادن رعایت GDPR ضروری است و سوابق فعالیت‌های پردازش داده‌ها و تصمیمات سازمانی را فراهم می‌کند. این سوابق، به سازمان‌ها این امکان را می‌دهند که به مقامات نظارتی و ذینفعان نشان دهند که اقدامات مناسب را برای حفاظت داده‌های شخصی انجام داده‌اند. حسابرسی، نقش حیاتی در اطمینان از رعایت الزامات GDPR برای حفظ حقوق افراد دارد. طبق GDPR، به افراد مجموعه‌ای از حقوق داده‌ها شده است که شامل حق دسترسی به داده‌های شخصی، حق اصلاح، حق حذف، حق جابه‌جایی داده‌ها و حق اعتراض به پردازش داده‌ها می‌شود. این حقوق با هدف دادن کنترل بیشتر به افراد بر اطلاعات شخصی‌شان و ایجاد اعتماد در محیط دیجیتال طراحی شده‌اند. با نگهداری سوابق دقیق از فعالیت‌های پردازش داده‌ها و زنجیره‌های حسابرسی، سازمان‌ها مسئولیت‌پذیری و شفافیتی را نشان می‌دهند که اصول بنیادی GDPR هستند. حسابرسی همچنین نقاط ضعفی را در توانایی سازمان برای حفظ این حقوق شناسایی می‌کند و اقدامات اصلاحی به‌موقع را در رابطه با ریسک‌هایی امکان‌پذیر می‌سازد که عدم رعایت را کاهش می‌دهد و اعتماد را در بین ذینفعان افزایش می‌دهد (گروه آی.جی.پی، ۲۰۲۵).

مدیریت ریسک‌های اشخاص ثالث

سازمان‌ها معمولاً برای فعالیت‌های پردازش داده‌ها به تأمین‌کنندگان برون‌سازمانی یا همان اشخاص ثالث اتکا می‌کنند، بنابراین، ارزیابی و مدیریت ریسک‌های تأمین‌کنندگان مذکور ضروری است. GDPR از کسب‌وکارها می‌خواهد اطمینان حاصل کنند که تأمین‌کنندگان به الزامات حفاظت‌داده‌ها پایبند هستند. حسابرسی، نقش کلیدی در ارزیابی قراردادهای تأمین‌کنندگان، کنترل‌های امنیتی و شیوه‌های مدیریت ریسک ایفا می‌کند. تأمین‌کنندگان، از ارائه‌دهندگان خدمات ابری گرفته تا آژانس‌های بازاریابی، معمولاً نقشی حیاتی را در

فعالیت‌های پردازش داده‌های یک سازمان ایفا می‌کنند. با این حال، واگذاری این فعالیت‌ها، ریسک‌های اضافی را به همراه دارد، به‌ویژه اگر تأمین‌کنندگان نتوانند الزامات GDPR را رعایت کنند. بنابراین، ارزیابی رعایت الزامات GDPR توسط تأمین‌کنندگان جنبه‌ای ضروری از راهبرد کلی GDPR یک سازمان است. حسابرسی، در ارزیابی رعایت الزامات توسط تأمین‌کنندگان با بررسی تدابیر حفاظت داده‌هایی که تأمین‌کنندگان پیاده‌سازی کرده‌اند، نقش مهمی دارد. این فرآیند معمولاً شامل بررسی قراردادها برای اطمینان از این موضوع است که توافق‌نامه‌های پردازش داده‌ها شامل بندهایی هستند که رعایت GDPR را الزامی می‌کنند. این توافق‌نامه‌ها باید دامنه پردازش داده‌ها، تدابیر امنیتی و رویه‌های اطلاع‌رسانی درباره نقض داده‌ها را مشخص کنند (کینگ[1]، ۲۰۱۹).

آموزش و آگاهی‌بخشی

نیروی انسانی آگاه برای رعایت GDPR ضروری است، زیرا خطای انسانی، یکی از علل اصلی نقض داده‌ها است. سازمان‌ها باید برنامه‌های آموزشی مداوم را برای آموزش اصول حفاظت‌داده‌ها، بهترین شیوه‌های امنیتی و الزامات قانونی به کارمندان پیاده‌سازی کنند. حسابرسی، به ارزیابی اثربخشی این ابتکارات آموزشی، شناسایی نقاط ضعف دانش و ارائه پیشنهاد برای بهبود کمک می‌کند. آموزش و آگاهی برای رعایت مقررات GDPR ضروری است، زیرا اطمینان حاصل می‌کند که کارکنان مسئولیت‌های خود را در حفاظت‌داده‌های شخصی درک می‌کنند. با این حال، اثربخشی برنامه‌های آموزشی باید به‌طور منظم ارزیابی تا اطمینان حاصل شود که نیازهای سازمانی و الزامات قانونی را برآورده می‌کند.

رویکرد آموزش حسابرسی سیستم‌های اطلاعاتی، رویکردی ساختاریافته را برای برنامه‌های آموزشی ارائه می‌دهند و محتوای آن‌ها روش‌های ارائه و نتایج را بررسی می‌کنند. به عنوان نمونه، می‌توان مواد آموزشی حسابرسی سیستم‌های اطلاعاتی را ارزیابی کرد تا مطمئن شد که آیا آموزش، موضوعات اساسی GDPR، مانند حقوق موضوع داده‌ها، سازوکارهای پاسخ به نقض داده‌ها[2] و اصول حفاظت‌داده‌ها را پوشش می‌دهد یا خیر. همچنین ممکن است فراوانی جلسات آموزشی و میزان تطابق آن‌ها با نقش‌ها و مسئولیت‌های مختلف کارکنان نیز مورد

[1] King
[2] Data Breach Response Mechanisms

ارزیابی قرار گیرد. سازوکارهای بازخورد مانند نظرسنجی‌ها و آزمون‌ها، اطلاعاتی را دربارهٔ اثربخشی برنامه‌های آموزشی ارائه می‌دهند. مدیران این بازخورد را تجزیه و تحلیل می‌کنند تا نقاط ضعف در دانش و زمینه‌های قابل‌بهبود را شناسایی کنند. برای نمونه، اگر کارکنان به‌طور مداوم در پاسخ به سوالات مربوط به پاسخ به نقض داده‌ها مشکل داشته باشند، سازمان ممکن است به تقویت این جنبه از برنامه آموزشی نیاز داشته باشد (بایر و همکاران[1]، ۲۰۲۲).

تدابیر فنی و سازمانی

برای دستیابی به رعایت GDPR، سازمان‌ها باید ترکیبی از تدابیر فنّی و سازمانی[2] را پیاده‌سازی کنند که از داده‌های شخصی محافظت کند. کنترل‌های فنّی مانند رمزنگاری و کنترل‌های دسترسی، داده‌ها را از دسترسی غیرمجاز محافظت می‌کنند، در حالی که تدابیر سازمانی سیاست‌ها و چارچوب‌های حکمرانی را برای رعایت تعیین می‌کنند.

تدابیر فنی و سازمانی، برای رعایت GDPR بنیادی هستند، زیرا زیرساخت لازم را برای حفاظت‌داده‌های شخصی فراهم می‌کنند. حسابرسی نقش حیاتی در ارزیابی کفایت این تدابیر دارد و اطمینان حاصل می‌کند که آن‌ها با الزامات قانونی و بهترین شیوه‌های صنعتی هم‌راستا هستند (ناک و انوانکو[3]، ۲۰۲۲).

سازمان‌ها در طیف وسیعی از کنترل‌های امنیتی، از جمله رمزنگاری، کنترل‌های دسترسی و نظارت بر شبکه را طول حسابرسی ارزیابی می‌کنند. این ارزیابی‌ها، آسیب‌پذیری‌هایی را شناسایی می‌کند که می‌تواند امنیت داده‌ها را به خطر بیندازد و بهبودهایی را برای کاهش ریسک‌ها پیشنهاد می‌دهند. برای نمونه، یک حسابرسی ممکن است نشان دهد که شیوه‌نامه‌های رمزنگاری یک سازمان، قدیمی هستند و به ارتقای آن‌ها به الگوریتم‌های امن‌تر نیاز است.

تدابیر سازمانی مانند سیاست‌ها و رویه‌ها، به همان اندازه مهم هستند. حسابرسی، بررسی می‌کند که آیا این تدابیر به طور مؤثر پیاده‌سازی و اجرا شده‌اند یا خیر. این کار شامل ارزیابی برنامه‌های پاسخ به حوادث، سیاست‌های نگهداری داده‌ها و برنامه‌های آموزشی کارکنان است (بایر و همکاران، ۲۰۲۲)

[1] Bowyer et al.
[2] Technical and Organizational Measures (TOM)
[3] Knoke & Nwankwo

اقدامات سازمانی و پیامدهای حسابرسی

اقدامات سازمانی با ایجاد فرهنگی از رعایت و مسئولیت‌پذیری در داخل یک سازمان، مکمل تدابیر فنّی هستند. این اقدامات شامل ایجاد چارچوب‌های حاکمیتی، توسعه سیاست‌ها و رویه‌ها و آموزش‌های مداوم برای کارکنان می‌شود. انتصاب یک مسئول حفاظت‌داده‌ها، اقدام سازمانی حیاتی است که برای برخی سازمان‌ها تحت GDPR الزامی است. نقش مسئول حفاظت‌داده‌ها شامل نظارت بر رعایت، مشاوره در مورد تعهدات حفاظت‌داده‌ها و رابطی برای تماس برای مقامات ناظر است (گشادزه[1]، ۲۰۲۰).

سیاست‌ها و رویه‌ها، پایه و اساس رعایت سازمانی را تشکیل می‌دهند. خطوط راهنمای واضح در مورد مدیریت داده‌ها، پاسخ به حوادث و مدیریت ریسک‌های شخص ثالث اطمینان می‌دهد که تمام ذینفعان مسئولیت‌های خود را درک کنند. به‌روزرسانی منظم این سیاست‌ها در پاسخ به تغییرات قانونی و یافته‌های حسابرسی اطمینان می‌دهد که سازمان‌ها همچنان با الزامات GDPR هم‌راستا می‌مانند.

تأثیر GDPR بر استانداردهای حسابرسی

GDPR تغییراتی بنیادی را در استانداردهای حسابرسی ایجاد و سازمان‌ها را به بازنگری و هم‌سویی مجدد چارچوب‌های رعایت خود وادار کرده است. GDPR به عنوان قانون جامع حفاظت‌داده‌ها، بر اصول مسئولیت‌پذیری، شفافیت و حقوق حریم‌خصوصی افراد تأکید دارد که به طور قابل‌توجهی انتظارات مربوط به استانداردهای حسابرسی را تغییر داده است. حسابرسی که به‌طور سنتی بر روی کارایی عملیاتی و دقت مالی متمرکز بود، اکنون نیاز به یک لایه اضافی از بررسی دارد تا از رعایت الزامات حریم‌خصوصی و دستورات حفاظت‌داده‌ها اطمینان حاصل کند. GDPR با بازتعریف ساختار استانداردهای حسابرسی، حریم‌خصوصی و حفاظت‌داده‌ها را به اجزای اصلی ارزیابی حسابرسی تبدیل کرده است. چارچوب‌های حسابرسی باید تکامل یابند تا الزامات خاص GDPR مانند حقوق موضوع داده‌ها، الزامات اطلاع‌رسانی در مورد نقض و اصل حداقل‌سازی داده‌ها را در بر بگیرند. حسابرسان اکنون انتظار دارند که نه تنها رعایت فنّی

[1] Goshadze

را بررسی کنند، بلکه ابعاد اخلاقی شیوه‌های پردازش داده‌ها مانند اطمینان از وجود مبنای قانونی برای جمع‌آوری داده‌ها و تأیید تناسب سیاست‌های نگهداری داده‌ها را نیز ارزیابی کنند.

یکی از تغییرات قابل توجه شامل گنجاندن چک‌لیست‌ها و شیوه‌نامه‌های هم‌سو با GDPR در استانداردهای بین‌المللی مانند ایزو۲۷۰۰۱ است که به سیستم‌های مدیریت امنیت اطلاعات می‌پردازد. این تغییرات، ضرورت هم‌سویی فرآیندهای مدیریت ریسک سازمان‌ها با تأکید GDPR بر اصول حریم‌خصوصی در طراحی و تنظیمات را نشان می‌دهد. علاوه بر این، نیاز به مستندسازی و اثبات رعایت، توجه بیشتری را به مسیرهای حسابرسی و مدیریت سوابق جلب کرده است. الزام ماده ۳۰ GDPR برای نگهداری سوابق فعالیت‌های پردازش یک نمونه بارز است، زیرا حسابرسان باید تأیید کنند که سازمان‌ها سوابق جامع، دقیق و به‌روز را به عنوان بخشی از تلاش‌های رعایت GDPR حفظ می‌کنند (مقررات[1]، ۲۰۱۹).

دیگر تغییر قابل‌توجه، تمرکز بر مدیریت ریسک شخص ثالث است. در پی گسترش اصل مسئولیت‌پذیری GDPR به پردازش‌کنندگان داده‌ها، اکنون سازمان‌ها ملزم به انجام حسابرسی منظم از تأمین‌کنندگان و ارائه‌دهندگان خدمات خود هستند تا اطمینان حاصل کنند که آن‌ها استانداردهای رعایت GDPR را رعایت می‌کنند.

تأثیر بر حسابرسی فناوری‌اطلاعات و امنیت اطلاعات

GDPR، حسابرسی سیستم‌های اطلاعاتی را به منظور امنیت اطلاعات در کانون توجه قرار داده است، زیرا این حوزه برای دستیابی و حفظ رعایت حیاتی هستند. سیستم‌های فناوری اطلاعات که غالباً ستون فقرات جمع‌آوری، ذخیره‌سازی و پردازش داده‌ها را تشکیل می‌دهند، اکنون تحت نظارت GDPR قرار دارند تا اطمینان حاصل شود که تدابیر فنّی کافی در جای خود قرار دارد. این حسابرسی، با وجود GDPR، فراتر از ارزیابی زیرساخت، شیوه‌نامه‌های رمزگذاری، کنترل‌های دسترسی، سیستم‌های تشخیص نفوذ و سایر تدابیر فنّی ضروری برای تأمین امنیت داده‌های شخصی را ارزیابی می‌کند.

یکی از مهم‌ترین جنبه‌های حسابرسی سیستم‌های اطلاعاتی تحت GDPR، تأیید حفاظت داده‌هاست. حسابرسی سیستم‌های اطلاعاتی، نقش مهمی در شناسایی شکاف‌ها در این پیاده‌سازی‌ها و توصیه به بهبودها به منظور اطمینان از رعایت ایفا می‌کند. به عنوان نمونه،

[1] Regulation

حسابرسان ارزیابی می‌کنند که آیا سیستم‌ها به گونه‌ای طراحی شده‌اند که تنها حداقل مقدار داده‌های شخصی موردنیاز برای اهداف خاص را جمع‌آوری کنند، که مطابق با اصل حداقل‌سازی داده‌ها است.

علاوه بر این GDPR اهمیت حسابرسی امنیت سایبری را به ویژه در زمینه نقض داده‌ها افزایش داده است. ماده ۳۳ GDPR الزام می‌کند که کنترل‌کنندگان داده‌ها نقض‌ها را ظرف ۷۲ ساعت به مقام ناظر اطلاع دهند(مقررات، ۲۰۱۹)، در حالی که ماده ۳۴ الزامات اطلاع‌رسانی موضوع داده‌های تحت تأثیر را در صورتی که نقض خطر بالایی برای حقوق و آزادی‌های آنها داشته باشد، مشخص می‌کند(آلونژه[1]، ۲۰۲۱). بنابراین، حسابرس فناوری‌اطلاعات نیاز دارد که سازوکارهای شناسایی، پاسخ و گزارش‌دهی نقض سازمان را ارزیابی کند تا از منطبق بودن آن‌ها با زمان‌های قانونی اطمینان حاصل کند.

حوزه دیگری که حسابرسی سیستم‌های اطلاعاتی را تحت تأثیر قرار داده است، حوزه کنترل دسترسی و اعتبارسنجی کاربر است. GDPR از سازمان‌ها می‌خواهد که تدابیری را پیاده‌سازی کنند که دسترسی به داده‌های شخصی را بر اساس ضرورت و تناسب، محدود کند. حسابرسان موظف هستند تأیید کنند که کنترل‌های دسترسی نه تنها از نظر فنّی صحیح هستند بلکه به طور منظم برای جلوگیری از دسترسی غیرمجاز مورد بررسی قرار می‌گیرند. استفاده از تأیید هویت چندعاملی، کنترل‌های دسترسی مبتنی بر نقش و سازوکارهای ثبت دقیق به یک معیار برای رعایت تبدیل شده است (کاسات و ابِرت[2]، ۲۰۲۰).

جهت‌گیری‌های آتی برای چارچوب‌های حسابرسی

با ادامه تحول مقررات حفاظت داده‌ها، چارچوب‌های حسابرسی باید برای مقابله با چالش‌ها و انتظارات نوظهور تطبیق یابند. یکی از بارزترین روندها، ادغام فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشین در شیوه‌های حسابرسی است. این فناوری‌ها می‌توانند کارایی و دقت حسابرسی را با خودکارسازی شناسایی ناهنجاری‌ها، تجزیه و تحلیل داده‌های وسیع و ارائه بینش‌های پیش‌بینی‌کننده در مورد ریسک‌های رعایت افزایش دهد (فدیک و همکاران[3]،

[1] Alunge
[2] Casutt & Ebert
[3] Fedyk et al.

۲۰۲۲؛لئوکادیو و همکاران[1]، ۲۰۲۴). به عنوان نمونه، ابزارهای مبتنی بر هوش مصنوعی می‌توانند برای ارزیابی اثربخشی شیوه‌های ناشناس‌سازی داده‌ها یا نظارت بر پیاده‌سازی ارزیابی‌های تأثیر حریم‌خصوصی[2]، مورد استفاده قرار گیرند.

جهت‌گیری آتی دیگر، استانداردسازی شیوه‌نامه‌های حسابرسی خاص GDPR است. در حالی‌که چارچوب‌هایی مانند ایزو۲۷۷۰۱ برای تکمیل GDPR با ارائه راهنمایی در زمینه مدیریت اطلاعات مربوط به حریم خصوصی توسعه یافته‌اند، هنوز هم جای بیشتری برای هماهنگی بیشتر در صنایع و حوزه‌های قضایی وجود دارد(لاچاد[3]، ۲۰۲۰). با توجه به رویکرد یکپارچه اتحادیه اروپا برای حفاظت‌داده‌های شخصی برخلاف رویکرد خود تنظیم ایالات متحده، یک رویکرد استانداردشده نه تنها تلاش‌های رعایت را برای سازمان‌هایی که در مناطق مختلف فعالیت می‌کنند، ساده‌تر می‌کند، بلکه با شفافیت بیشتری برای حسابرسان، رعایت GDPR فراهم می‌کند.

روند پیش‌بینی‌شده بعدی توسعه چارچوب‌های حسابرسی خاص صنعت است که به چالش‌های منحصر به فرد بخش‌های مختلف می‌پردازد. به‌عنوان نمونه، سازمان‌های بهداشتی ممکن است به چارچوب‌های تخصصی برای ارزیابی رعایت مقررات GDPR در مورد داده‌های حساس بهداشتی نیاز داشته باشند. با سفارشی‌سازی چارچوب‌ها برای زمینه‌های خاص، حسابرسان می‌توانند توصیه‌های هدفمند و مؤثرتری ارائه دهند.

علاوه بر این، افزایش انتقال داده‌های فرامرزی و پیچیدگی‌های مرتبط با اطمینان از رعایت در یک اقتصاد دیجیتال جهانی به احتمال زیاد، آینده چارچوب‌های حسابرسی را تحت تأثیر قرار خواهد داد. باطل شدن سپر حریم خصوصی اتحادیه اروپا-آمریکا[4] در سال ۲۰۲۰ و معرفی چارچوب نوین حریم خصوصی داده‌ها بین اتحادیه اروپا و ایالات متحده، ناپایداری سازوکارهای انتقال داده را برجسته می‌کند. حسابرسان باید از این تحولات مطلع بمانند و ارزیابی‌های رعایت انتقال داده را در روش‌های حسابرسی خود بگنجانند (فاهی و ترپان[5]، ۲۰۲۳).

[1] Leocádio et al.
[2] Privacy Impact Assessments
[3] Lachaud
[4] EU-U.S. Privacy Shield
[5] Fahey & Terpan

سرانجام، با ظهور مقررات جدید مانند قانون خدمات دیجیتال[1] و قانون بازارهای دیجیتال[2] در کنار GDPR، چارچوب‌های حسابرسی باید برای سازگاری با این چشم‌اندازهای چندوجهی رعایت توسعه یابند (توریلازی و همکاران[3]، ۲۰۲۳؛ جرادین و همکاران[4]، ۲۰۲۲). همگرایی این مقررات نیاز به رویکردی یکپارچه را برای حسابرسی نشان می‌دهد که تعامل بین حفاظت‌داده‌ها، قوانین رقابت و حاکمیت پلتفرم‌های دیجیتال را در نظر می‌گیرد. در پایان، تأثیر GDPR بر استانداردهای حسابرسی تحول‌آفرین خواهد بود و نیاز به یک رویکرد جامع و آینده‌نگر به حسابرسی رعایت را ایجاب می‌کند.

روندها و چالش‌های آتی

چشم‌انداز در حال تحول مقررات حفاظت‌داده‌ها

چشم‌انداز مقررات حفاظت‌داده‌ها که در حال تحول مداوم است، تحت تأثیر پیشرفت‌های سریع فناوری و افزایش شناخت از حریم‌خصوصی داده‌ها به عنوان یک حق اساسی بشر قرار دارد. GDPR، به عنوان یکی از جامع‌ترین قوانین حفاظت‌داده‌ها، استاندارد جهانی را تعیین کرده و بر ابتکارات قانونی در سرتاسر جهان تأثیر گذاشته است. کشورهایی مانند ژاپن، برزیل، کره جنوبی و هند، تا حدی قوانین خود را براساس GDPR مدل‌سازی کرده و چارچوب‌های محکم‌تری را برای حفاظت‌داده‌های شخصی معرفی کرده‌اند. در ایران نیز تلاش‌هایی برای بهبود سازوکارهای حفاظت داده‌های شخصی از طریق قوانین و مقرراتی شده است که بر حریم خصوصی داده‌ها و امنیت اطلاعات تأکید دارند. لایحه حفاظت داده‌های شخصی، نمونه‌ای از تلاش‌ها در این حوزه است. هرچند که هنوز به طور کامل با GDPR هماهنگ نیست، تلاش‌های داخلی نشان‌دهنده شناخت آن از حفاظت‌داده‌ها به عنوان یک موضوع حیاتی در عصر دیجیتال است.

همچنین، استفاده روزافزون از هوش مصنوعی و یادگیری ماشین، قانون‌گذاران را به تدوین قوانینی واداشته است که بر استفاده اخلاقی و شفاف از این فناوری‌ها نظارت کند. قانون

[1] Digital Services Act (DSA)
[2] Digital Markets Act (DMA)
[3] Turillazzi et al.
[4] Geradin et al.

پیشنهادی هوش مصنوعی اتحادیه اروپا[1] و قانون خدمات دیجیتال[2]، این روند را منعکس می‌کند و آینده‌ای را نشان می‌دهد که در آن، مقررات حفاظت‌داده‌ها با نگرانی‌های گسترده‌تری در مورد استفاده اخلاقی از فناوری تلاقی می‌کند(سوورانو و همکاران[3]، ۲۰۲۲؛ نانینی و همکاران[4]، ۲۰۲۴).

گسترش قوانین حفاظت داده‌ها در حوزه‌های قضایی مختلف هم فرصت‌ها و هم پیچیدگی‌هایی را برای سازمان‌ها ایجاد می‌کند. از یک سو، این مقررات، اهمیت اتخاذ رویکردی جهانی را برای حاکمیت داده‌ها پررنگ می‌نماید. از سوی دیگر، چالش‌هایی را در اطمینان از رعایت الزامات قانونی متعدد و گاهی متضاد، پیش می‌آورند. به عنوان نمونه، تصمیم Schrems II که توافق‌نامه حریم‌خصوصی بین اتحادیه اروپا و ایالات متحده را باطل کرد، سازمان‌ها را با عدم قطعیت در مورد انتقال داده‌های فرامرزی مواجه کرده است (دالی[5]، ۲۰۲۱). همان‌طور که مقررات به تکامل ادامه می‌دهند، سازمان‌ها باید به سرعت با چشم‌اندازهای قانون‌های جدید تطابق یابند و پیشرو باقی بمانند.

چالش‌های پیش روی سازمان‌ها به‌هنگام رعایت

رعایت مقررات حفاظت‌داده‌ها، به ویژه GDPR، چالشی چندوجهی برای سازمان‌ها است. یکی از موانع اصلی، در پیچیدگی و جزئیات الزامات GDPR نهفته است. سازمان‌ها باید اطمینان حاصل کنند که در طیف وسیعی از الزامات، از به‌دست آوردن رضایت معتبر برای پردازش داده‌ها تا پیاده‌سازی تدابیر فنّی و سازمانی برای امنیت داده‌ها، رعایت دارند. نیاز به توازن این الزامات با کارایی عملیاتی و نوآوری برای بسیاری چالشی دشوار است.

چالش دیگری که باید به آن توجه کرد، سرعت پیشرفت فناوری است. گسترش فناوری‌هایی مانند اینترنت اشیا[6]، رایانش ابری و بلاک‌چین ابعاد جدیدی را به حفاظت‌داده‌ها اضافه کرده است(سئو و همکاران[7]، ۲۰۱؛ ژو و همکاران[8]، ۲۰۲۴). این فناوری‌ها اغلب مقادیر

[1] The Eu’s Proposed Ai Act
[2] The Digital Services Act (DSA)
[3] Sovrano et al.
[4] Nannini et al.
[5] Duli
[6] Internet of Things (IoT)
[7] Seo et al.
[8] Zhou et al.

زیادی داده تولید می‌کنند که نگهداری فهرست جامع از داده‌های شخصی پردازش‌شده را برای سازمان‌ها دشوار می‌سازد. افزون بر این، ماهیت غیرمتمرکز برخی فناوری‌ها، مانند بلاک‌چین، چالش‌های منحصر به فردی را در اطمینان از رعایت اصول GDPR، مانند حق حذف و حداقلی‌سازی داده‌ها، به وجود می‌آورد (بلن ساگلام و همکاران[1]، ۲۰۲۳).

عوامل انسانی نیز در چالش‌های رعایت نقش حیاتی دارند. کمبود آگاهی و آموزش در میان کارکنان می‌تواند منجر به نقض‌های غیرعمدی داده‌ها یا عدم رعایت الزامات GDPR شود. این مسئله به ویژه در نقاطی از فعالیت شدیدتر است که قوانین حفاظت‌داده‌ها نسبتاً جدید هستند یا فرهنگی از حریم‌خصوصی هنوز به طور کامل شکل نگرفته است. به عنوان نمونه، در حالی که در داخل کشور، در زمینه حفاظت‌داده‌ها پیشرفت‌هایی صورت گرفته است، پرورش نیروی کاری که این اصول را درک کند و به آن پایبند باشند، ممکن است برای سازمان‌ها چالش‌برانگیز باشد.

محدودیت‌های مالی و منابع نیز چالش‌های رعایت به ویژه برای شرکت‌های کوچک و متوسط[2] را تشدید می‌کند. برخلاف شرکت‌های بزرگ که تیم‌های رعایت اختصاصی دارند، شرکت‌های کوچک و متوسط اغلب برای تخصیص منابع لازم برای پیاده‌سازی تدابیر مطابق با GDPR مشکل دارند(بوردین[3]، ۲۰۱۹). هزینه استخدام یک مسئول حفاظت داده‌ها، انجام حسابرسی منظم و سرمایه‌گذاری در سیستم‌های فناوری اطلاعات امن برای سازمان‌های کوچک می‌تواند بسیار سنگین باشد.

نقش حسابرسی سیستم‌های اطلاعاتی در راهنمایی سازمان‌ها برای چالش‌های رعایت آینده

حسابرسی سیستم‌های اطلاعاتی، نقش محوری در کمک به سازمان‌ها برای هدایت چشم‌انداز پیچیده و درحال تحول رعایت حفاظت داده‌ها دارد. همان‌طور که GDPR و دیگر مقررات الزامات مسئولیت‌پذیری سنگینی را به وجود می‌آورند، حسابرسی سیستم‌های اطلاعاتی ابزاری حیاتی برای شناسایی شکاف‌های رعایت، کاهش ریسک‌ها و اطمینان از بهبود مستمر در

[1] Belen-Saglam et al.
[2] Small and Medium Enterprises (SME)
[3] Bordin

شیوه‌های حاکمیت داده‌ها است. یکی از مهم‌ترین مزایای حسابرسی سیستم‌های اطلاعاتی، توانایی آن‌ها در ارائه ارزیابی شفاف و عینی از وضعیت رعایت سازمان‌ها است. حسابرسی سیستم‌های اطلاعاتی از طریق ارزیابی‌های سیستماتیک سیاست‌ها، فرایندها و کنترل‌های فنّی به سازمان‌ها کمک می‌کند تا نقاط ضعفی را شناسایی کنند که در رعایت الزامات GDPR وجود دارد. همچنین حسابرسی سیستم‌های اطلاعاتی در ایجاد فرهنگ مسئولیت‌پذیری درون سازمان‌ها نقش حیاتی دارند. حسابرسی سیستم‌های اطلاعاتی منظم، همراه با سازوکارهای گزارش‌دهی شفاف، کارکنان تمام سطوح را تشویق می‌کند تا به حفاظت‌داده‌ها اهمیت دهند. این تغییر فرهنگی به ویژه در داخل کشور اهمیت ویژه‌ای دارد که آگاهی از اصول حفاظت‌داده‌ها هنوز درحال‌توسعه است (گروه آی.جی.پی، ۲۰۲۵).

عملکرد مهم دیگری که حسابرسی‌سیستم‌های‌اطلاعاتی دارد، ارزیابی اثربخشی تدابیر فنّی و سازمانی است. همان‌طور که پیشرفت‌های فناوری منجر به شکل‌گیری مجدد چشم‌انداز حفاظت‌داده‌ها می‌شوند، حسابرسی‌سیستم‌های‌اطلاعاتی سازوکاری را برای اطمینان از رعایت چشم‌اندازها فراهم می‌کند که سازمان‌ها باید با این تغییرات همگام باشند. علاوه بر این، حسابرسی سیستم‌های اطلاعاتی برای مدیریت ریسک‌های اشخاص ثالث، که در زمینه رعایت GDPR به طور فزاینده‌ای مرتبط هستند، حیاتی است. سازمان‌ها اغلب به فروشندگان و ارائه‌دهندگان برون‌سازمانی خدمات برای فعالیت‌های پردازش داده‌ها وابسته‌اند و بنابراین باید اطمینان حاصل کنند که اشخاص ثالث به الزامات GDPR پایبند هستند (گروه آی.جی.پی، ۲۰۲۵).

با نگاهی به آینده، به احتمال زیاد نقش حسابرسی‌سیستم‌های‌اطلاعاتی با ادامه تکامل مقررات حفاظت‌داده‌ها گسترش خواهد یافت. انتظار می‌رود فناوری‌های پیشرفته حسابرسی، مانند تجزیه‌وتحلیل‌های مبتنی بر هوش مصنوعی و ردپای حسابرسی مبتنی بر بلاک‌چین نقش برجسته‌تری را در افزایش کارایی و دقت حسابرسی‌سیستم‌های‌اطلاعاتی ایفا کنند. سازمان‌ها با استفاده از این فناوری‌ها می‌توانند نگرش عمیق‌تری در مورد ریسک‌های رعایت خود به دست آورند و تصمیم‌های بهتری را در مورد چگونگی پرداختن به آن‌ها اتخاذ کنند.

بحث و نتیجه‌گیری

یافته‌های پژوهش نشان می‌دهد که GDPR تأثیر عمیقی بر حسابرسی سیستم‌های اطلاعاتی خواهد داشت و مدل‌های حاکمیت داده، مدیریت ریسک و رعایت مقررات را در سازمان‌ها به‌طور بنیادین دگرگون می‌نماید. یکی از مهم‌ترین تغییرات مربوط به حوزه حاکمیت داده است، جایی که الزامات GDPR مانند نگهداری سوابق فعالیت‌های پردازش، انتصاب مسئول حفاظت‌داده‌ها و اجرای سیاست‌های سخت‌گیرانه نگهداری داده‌ها سازمان‌ها را وادار به بازنگری ساختارهای مدیریت داده‌ها کرده است. در نتیجه، حسابرسی‌ها دیگر صرفاً بر ارزیابی کنترل‌های امنیتی فناوری اطلاعات متمرکز نیست، بلکه معیارهای حاکمیتی و مسئولیت‌پذیری مدیریتی را نیز دربرمی‌گیرد. سازمان‌هایی که در زمینه رعایت مقررات موفق هستند، اغلب سیاست‌های دقیقی در مورد طبقه‌بندی و دوره‌های نگهداری داده‌ها دارند که هم با نیازهای عملیاتی آن‌ها و هم با اصل محدودیت نگهداری داده درGDPR هم‌سو است.

مدیریت ریسک نیز به‌عنوان یکی از ارکان کلیدی حسابرسی رعایت ظاهر شده است، به‌ویژه از طریق اجرای ارزیابی‌های تأثیر بر حفاظت‌داده‌ها این ارزیابی‌ها ابزاری حیاتی برای شناسایی و ارزیابی پردازش‌های پرریسک مانند نمایه‌سازی داده‌ها در مقیاس وسیع و تصمیم‌گیری خودکار محسوب می‌شوند. بررسی‌های انجام‌شده نشان می‌دهد که سازمان‌های فعال در صنایع تحت نظارت دقیق، چارچوب‌های پیشرفته‌ای برای انجام ارزیابی‌های تأثیر بر حفاظت‌داده‌ها دارند، اما کسب‌وکارهای کوچک و متوسط به دلیل محدودیت‌های منابع و کمبود تخصص در رعایت مقررات، با چالش‌های عملی در پیاده‌سازی مؤثر مدیریت ریسک مواجه هستند. با وجود افزایش آگاهی در مورد الزام ۷۲ ساعته GDPR برای اعلام نقض داده، یافته‌های پژوهش تطبیقی حاکی از آن است که فقدان سیاست‌های مؤثر برای پاسخگویی به رخدادهای امنیتی و ابزارهای نظارت خودکار بر رخدادهای امنیتی خطر عدم رعایت مقررات را افزایش می‌دهد.

یکی دیگر از چالش‌های کلیدی که در پژوهش شناسایی شده است، اجرای اصول حریم‌خصوصی در سیستم‌های اطلاعاتی است. اگرچه چالش گنجاندن تدابیر حریم خصوصی مانند ناشناس‌سازی داده‌ها همواره وجود داشته است، اما استنتاج‌های‌های قانون حفاظت عمومی از داده‌ها حاکی از آن است که در اغلب موارد، این تدابیر به‌عنوان ویژگی‌های اضافی و پس از توسعه سیستم پیاده‌سازی شده‌اند. این رویکرد افزوده‌شده حریم‌خصوصی به‌جای یکپارچگی

ذاتی، باعث کاهش اثربخشی تدابیر حفاظتی و افزایش مخاطرات عدم رعایت مقررات می‌شود. سازمان‌هایی که موفق به نهادینه‌سازی اصول حفاظت‌داده‌ها در کلیه مراحل توسعه سیستم شده‌اند، معمولاً راهبردهای یکپارچه‌ای را برای رعایت مقررات اتخاذ کرده‌اند، اما بر اساس تحیل پژوهش از GDPR در بسیاری از سازمان‌ها همچنان یک رویکرد واکنشی به جای پیشگیرانه در پیاده‌سازی حریم‌خصوصی مشاهده می‌شود.

همچنین، یافته‌های پژوهش بر نقش حیاتی ارزیابی ریسک تأمین‌کنندگان شخص ثالث در حسابرسی‌های رعایت GDPR تأکید دارد. از آنجا که GDPR مسئولیت‌پذیری را فراتر از کنترل‌کنندگان داده‌ها به پردازش‌کنندگان داده نیز گسترش داده است، سازمان‌ها ملزم به بررسی دقیق سازگاری تأمین‌کنندگان هستند. تحلیل‌های پژوهش نشان می‌دهد که مفهوم «بررسی دقیق» در GDPR، شامل فرآیندهای دقیقی همچون ارزیابی و به‌روزرسانی دوره‌ای قراردادهای تأمین‌کنندگان، اجرای حسابرسی‌های امنیتی منظم بر آن‌ها و تدوین سیاست‌های شفاف برای گزارش‌دهی و اطلاع‌رسانی در مورد رخدادهای نقض داده‌ها است. با این حال استنتاج و تحلیل پژوهش از متن GDPR نشان می‌دهد که بسیاری از سازمان‌ها هنوز سازوکارهای استانداردی برای ارزیابی رعایت مقررات توسط تأمین‌کنندگان خود ندارند که این موضوع، می‌تواند منجر به نقض مقررات ناشی از عملکرد شخص ثالث شود.

در بُعد فنّی، یافته‌های پژوهش، نقش کلیدی رمزنگاری، کنترل‌های دسترسی و نظارت بلادرنگ را در اطمینان از رعایت GDPR نشان می‌دهد. سازمان‌هایی که چارچوب‌های امنیتی خود را با استانداردهای بین‌المللی مانند ایزو۲۷۰۰۱ هم‌سو کرده‌اند، معمولاً مدیریت کلیدهای رمزنگاری پیشرفته‌تر، آزمون نفوذ ساختاریافته و سازوکارهای احراز هویت قوی‌تر دارند. این مسائل بر ضرورت سرمایه‌گذاری مستمر در به‌روزرسانی کنترل‌های امنیتی و تطبیق آن‌ها با استانداردهای نوظهور امنیت سایبری تأکید دارد.

علاوه بر تدابیر فنّی، یافته‌های پژوهش نشان می‌دهد که فرهنگ سازمانی، نقشی اساسی در پایدارسازی رعایت مقررات GDPR دارد. برنامه‌های آموزشی کارکنان و افزایش آگاهی درباره مفاهیم حفاظت‌داده‌ها از جمله مهم‌ترین عوامل کاهش خطای انسانی در نقض داده‌ها هستند.

به‌طور کلی، نتایج پژوهش تأیید می‌کند که حسابرسی‌های رعایتGDPR ، نقشی حیاتی در هم‌راستایی سازمان‌ها با الزامات مقررات دارند، اما اثربخشی آن‌ها مستلزم اتخاذ رویکردی جامع است که شامل مدیریت ریسک، حاکمیت داده‌ها، تدابیر فنّی و آموزش نیروی انسانی باشد. سازمان‌هایی که راهبردهای منسجم و ساختاریافته‌ای برای رعایت GDPR ازجمله ارزیابی مستمر ریسک‌ها، اجرای اصول حریم‌خصوصی در طراحی، مدیریت دقیق تأمین‌کنندگان و برگزاری آموزش‌های مداوم، تدوین کرده‌اند، در مقایسه با سایرین در رعایت این مقررات، عملکرد بهتری دارند و همچنین، اعتماد و شفافیت بیشتری در تعاملات داده‌ای خود ایجاد کرده‌اند. با این حال، یافته‌های پژوهش تطبیقی حاکی از آن است که مقررات‌عمومی حفاظت از داده‌ها چالش‌هایی پایدار را در میان کسب‌وکارهای کوچک و متوسط و سازمان‌هایی برجسته می‌کند که از زیرساخت‌های قدیمی استفاده می‌کنند. نتایج پژوهش، ضرورت توسعه راهکارهای مقیاس‌پذیر برای رعایت GDPR ، ارائه دستورالعمل‌های نظارتی متناسب با صنایع مختلف و همکاری‌های بین‌سازمانی برای بهبود اکوسیستم حفاظت‌داده‌ها را روشن می‌سازد.

ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنا بر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

منابع

ذاکرحسینی، سیدمحمد. (۱۳۹۹). بررسی عملکرد فرآیند حسابرسی مبتنی بر دانش حسابرسان از فناوری‌اطلاعات . *چشم انداز حسابداری و مدیریت*، ۳(۳۳)، ۹۸-۷۳.

محمودی پرچینی، مرتضی؛ ریاضی، لادن و پور ابراهیمی، علیرضا . (۱۴۰۳). مقایسه قوانین حفاظت‌داده‌های شخصی: مقررات‌عمومی منحصر به فرد تحت مقررات حفاظت‌داده‌های عمومی اتحادیه اروپا (GDPR) و قوانین ایالات متحده. *فصلنامه علوم خبری*، ۱۳ (۴)، ۲۲۴-۲۰۴.

شریفی کیا، محمد علی و شعبانی جهرمی، فریده . (۱۴۰۱). شرط شخصی تلقی شدن داده‌ها در فضای سایبر بررسی تطبیقی مقررات‌عمومی اروپایی حفاظت از داده و حقوق ایران .*مجله علمی "حقوق خصوصی"*، ۱۹(۱)، ۲۲۱-۲۴۵.

References

Alunge, R. (2021). Breach of security vs personal data breach: effect on EU data subject notification requirements. *International Data Privacy Law*, *11*(2), 163-181.

Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), 1338-1347.

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, *4*(2), 100129.

Bertolaccini, L., Falcoz, P. E., Brunelli, A., Batirel, H., Furak, J., Passani, S., & Szanto, Z. (2023). The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database. *European Journal of Cardio-Thoracic Surgery*, *64*(3), ezad289.

Bowyer, A., Holt, J., Go Jefferies, J., Wilson, R., Kirk, D., & David Smeddinck, J. (2022, April). Human-GDPR interaction: practical experiences of accessing personal data. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-19).

Casutt, N., & Ebert, N. (2020, October). Data protection officers: Figureheads of privacy or merely decoration. In *Proc. 16th Eur. Conf. Manage., Leadership Governance* (p. 39).

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34*(2), 234-243.

Dashti, S., & Ranise, S. (2020). Tool-assisted risk analysis for data protection impact assessment. *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14*, 308-324.

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk'in the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105342.

Dounis, N. P. (2017). GDPR Regulatory Compliance and the Role of Internal Audit: Theoretical and Practical Approach. *Int'l. In-House Counsel J.*, *11*, 1.

Duli, B. (2021). *Data transfers between the EU and US: the impact of schrems I and schrems II for cross-border data flows, privacy, and national security* (Doctoral dissertation).

Fahey, E., & Terpan, F. (2023). The future of the EU-US privacy shield. In *The Routledge Handbook of Transatlantic Relations* (pp. 221-236). Routledge.

Fakeyede, O. G., Okeleke, P. A., Hassan, A. O., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science*, *11*(11).

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process?. *Review of Accounting Studies*, *27*(3), 938-985.

Framework, B. E. (2015). The National Institute of Standards and Technology (NIST).

Geradin, D., Bania, K., & Karanikioti, T. (2022). The interplay between the Digital Markets Act and the General Data Protection Regulation. *Available at SSRN 4203907*.

Gilman, M. E. (2020). Five privacy principles (from the GDPR) the United States should adopt to advance economic justice. *Ariz. St. LJ*, *52*, 368.

Gobeo, A., Fowler, C., & Buchanan, W. J. (2022). *GDPR and Cyber Security for Business Information Systems*. River Publishers.

Goshadze, K. (2020). The Data Protection Officer (DPO)-Ensuring Greater Data Protection Compliance. *Law & World*, *14*, 41.

Hijmans, H., & Raab, C. D. (2018). Ethical Dimensions of the GDPR. *Commentary on the General Data Protection Regulation, Cheltenham: Edward Elgar (2018, Forthcoming)*.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

I. G. P. Team (2025). EU general data protection regulation (GDPR): an implementation and compliance guide. Packt Publishing Ltd.

Kasirzadeh, A., & Clifford, D. (2021, July). Fairness and data protection impact assessments. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 146-153).

King, D. (2019). Data classification: A means to an end. *Journal of Data Protection & Privacy*, *2*(4), 324-330.

Knoke, F., & Nwankwo, I. (2022). Managing Data Protection Compliance through Maturity Models: A Primer. *Eur. Data Prot. L. Rev.*, *8*, 536.

La Torre, M., Botes, V. L., Dumay, J., & Odendaal, E. (2021). Protecting a new Achilles heel: the role of auditors within the practice of data protection. *Managerial Auditing Journal*, *36*(2), 218-239.

Lachaud, E. (2020). ISO/IEC 27701 standard: Threats and opportunities for GDPR certification. *Eur. Data Prot. L. Rev.*, *6*, 194.

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices. *Administrative Sciences*, *14*(10), 238.

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, *146*, 106868.

Mahmodi Parchini, M. , Riazi, L. and Pour Ebrahimi, A. (2025). Comparison of Personal Data Protection Laws: Unique General Regulations under the

European Union's General Data Protection Regulation (GDPR) and United States Laws. *News Science Quarterly (NS)*, *13*(4), 204-224. (In Persian)

Nannini, L., Bonel, E., Bassi, D., & Maggini, M. J. (2024). Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act. *AI and Ethics*, 1-29.

Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. In *The ethics of information technologies* (pp. 141-178). Routledge.

Pandit, H. J. (2023). Making sense of Solid for data governance and GDPR. *Information*, *14*(2), 114.

Regulation, G. D. P. (2019). *GDPR. 2019*.

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: a global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences*, *6*(1), 73-88.

Rhahla, M., Allegue, S., & Abdellatif, T. (2021). Guidelines for GDPR compliance in Big Data systems. *Journal of Information Security and Applications*, *61*, 102896.

Rosenberger, A., Shvartzshnaider, Y., & Sanfilippo, M. (2021). Digital Contact Tracing in the EU: Data Subject Rights and Conflicting Privacy Governance. *Proceedings of the Association for Information Science and Technology*, *58*(1), 819-821.

Saltarella, M., Desolda, G., & Lanzilotti, R. (2021, July). Privacy design strategies and the GDPR: A systematic literature review. In *International Conference on Human-Computer Interaction* (pp. 241-257). Cham: Springer International Publishing.

Sargiotis, D. (2024). Data Governance Frameworks: Models and Best Practices. In *Data Governance: A Guide* (pp. 165-195). Cham: Springer Nature Switzerland.

Sayankar, V. N. (2013). A Review on Information Systems Audit. *Research Journal of Engineering and Technology*, *4*(3), 103-106.

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An analysis of economic impact on IoT industry under GDPR. *Mobile Information Systems*, *2018*(1), 6792028.

Sharifi Kia, M. A. and Shabani Jahromi, F. (2022). The Condition of Considering the Data Personal in Cyberspace Comparative Review of European General Data Protection Regulation and Iranian law. *Private Law*, *19*(1), 221-245. (In Persian)

Sim, J., Kim, B., Jeon, K., Joo, M., Lim, J., Lee, J., & Choo, K. K. R. (2023). Technical requirements and approaches in personal data control. ACM Computing Surveys, 55(9), 1-30.

Sovrano, F., Sapienza, S., Palmirani, M., & Vitali, F. (2022). Metrics, explainability and the European AI act proposal. *J*, *5*(1), 126-138.

Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, *91*, 101469.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5-8.

Trakman, L., Walters, R., & Zeller, B. (2020). Digital consent and data protection law–Europe and Asia-Pacific experience. *Information & Communications Technology Law*, *29*(2), 218-249.

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*(1), 83-106.

Zakerhosseini, S. (2020). Review the performance of the audit process based on auditors' knowledge of information technology. *Journal of Accounting and Management Vision*, *3*(33), 73-98. (In Persian)

Zhou, L., Wub, Y., Wang, H., Yao, Y., Wangd, Y., & Jiao, Z. (2024, October). Information Protection Impact Assessment in China. In Proceedings of the 4th International Conference on Management Science and Software Engineering (ICMSSE 2024) (Vol. 244, p. 88). Springer Nature.

Zichichi, M., Ferretti, S., D'Angelo, G., & Rodríguez-Doncel, V. (2022). Data governance through a multi-DLT architecture in view of the GDPR. Cluster Computing, 25(6), 4515-4542.