مرکز ماهر

معرفی GDPR و نقش آن در صیانت از حریم خصوصی کاربران شبکه‌های اجتماعی

فهرست مطالب

فصل ۱ مقدمه

اتحادیه اروپا به منظور صیانت از حریم خصوصی افراد و محافظت از داده‌های شخصی آن‌ها، قانونی موسوم به GDPR[1] تصویب کرد که همه شرکت‌های ارائه‌دهنده خدمات به کاربران که با داده‌های شخصی افراد سروکار دارند را ملزم به رعایت آن می‌کند. حوزه فراگیر و گسترده این قانون و ضمانت‌های اجرایی مستحکم آن از یک طرف و جرائم سنگینی که در صورت تخلف از آن‌ها به شرکت‌ها تحمیل می‌گردد باعث شد سازگاری با این قانون به شکل جدی در دستور کار بسیاری از شرکت‌ها به خصوص شرکت‌های حوزه فناوری اطلاعات و ارائه دهنده سرویس‌های شبکه اجتماعی قرار گیرد. به همین دلیل شرکت‌های مطرح در حوزه خدمات شبکه اجتماعی فرایند آماده‌سازی خود جهت سازگاری با نیازها و خواسته‌های GDPR را آغاز کردند.

اگر چه این قانون در اتحادیه اروپا وضع شده است اما حوزه سرزمینی آن محدود اعضای اتحادیه اروپا نیست و دایره شمول آن شرکت‌ها و سازمان‌هایی که در این اتحادیه مستقر نیستند را نیز می‌تواند در برگیرد. همچنین ماهیت این قانون و دید جامع و فراگیر آن در ارتباط با حریم خصوصی افراد و محافظت از داده‌ها، باعث شده است که مطالعه آن از منظر نیازهای امنیتی بسیار مهم باشد. نیازهای موجود در این قانون کاملا متناسب با دغدغه‌های شرکت‌ها و ارائه دهندگان سرویس‌های شبکه اجتماعی داخلی و سایر فعالان حوزه فناوری اطلاعات است. به دلیل اهمیت این مسئله، در این گزارش تلاش می‌کنیم تا نقش GDPR در صیانت از حریم خصوصی افراد را مورد ارزیابی قرار دهیم. به همین دلیل ابتدا به معرفی GDPR و ساختار آن و اهرم‌های قانونی و حفاظتی آن می‌پردازیم و اثرات آن بر روی تجارت را مورد بررسی قرار می‌دهیم. سپس تلاش می‌کنیم با ارائه یک چارچوب سطح بالا، اقداماتی را که شرکت‌های برای سازگاری با GDPR باید انجام دهند را به شکل منسجم و ساختاریافته ارائه کنیم؛ و در پایان اقداماتی که برخی از شرکت‌های مطرح حوزه خدمات شبکه‌های اجتماعی در راستای تبعیت از GDPR انجام داده‌اند را مورد بررسی قرار می‌دهیم.

۱-۱ GDPR چیست؟

شبکه‌های اجتماعی پدیده فراگیر عصر حاضر هستند که فرایند تعامل افراد با یکدیگر را تسهیل می‌کنند. در این میان حجم زیادی از داده‌ها که نشان دهنده علایق، دیدگاه‌ها و نظرات افراد است در بستر شبکه‌های اجتماعی مانند Facebook یا Twitter تا پیام‌رسان‌هایی مانند WhatsApp یا Telegram به اشتراک گذاشته می‌شود. اکثر شبکه‌های اجتماعی از شماره موبایل یا آدرس ایمیل برای ثبت‌نام کاربران استفاده می‌کنند. پروفایل شخصی افراد در این شبکه‌ها به همراه مطالبی که توسط کاربر در این شبکه‌ها منتشر می‌شود و پاسخ‌هایی که از سوی کاربر در پاسخ به یک مطلب گذاشته می‌شود می‌تواند مورد تحلیل قرار گیرد تا جایی که ویژگی‌های شخصیتی افراد را می‌توان از طریق مطالبی که مورد پسند او قرار گرفته است تا حد بسیار دقیقی مشخص کرد.

این قابلیت‌هایی که در نتیجه تحلیل داده‌های شبکه اجتماعی وجود دارد به طور بالقوه حریم خصوصی را در خطر قرار می‌دهد به نحوی که در آخرین رسوایی در این زمینه، شرکت Cambridge Analytica توانست به اطلاعات ۵۰ میلیون نفر از کاربران Facebook دست یابد و از این اطلاعات جهت هدایت کمپین‌های انتخاباتی آمریکا و تاثیرگذاری بر روی آن استفاده کند. مسئله این‌گونه آغاز شد که در سال ۲۰۱۴ یک پژوهشگر به نام Aleksandr Kogan یک App موبایلی که در واقع نوعی مسابقه در مورد شخصیت افراد بود را برای Facebook توسعه داد. ۲۷۰،۰۰۰ نفر این App را نصب کرده‌اند و در آن زمان Kogan مانند سایر توسعه‌دهندگان می‌توانست به داده‌های دوستان آن افراد دسترسی پیدا کند. هنگام درخواست برای

[1] General Data Protection Regulation

این اطلاعات، داده‌ها در یک بانک اطلاعاتی خصوصی ذخیره شد به جای اینکه بلافاصله حذف گردند. این بانک اطلاعاتی که حاوی داده‌های ۵۰ میلیون کاربر بود در اختیار موسسه Cambridge Analytic قرار گرفت و بر اساس این داده ۳۰ میلیون پروفایل روانشانی رای‌دهندگان ایجاد شد. این مسئله همان چیزی است که آن را نقض[2] می‌نامیم.

با توجه به تهدیدات موجود در ارتباط با نقض حریم خصوصی توسط اطلاعات موجود در شبکه‌های اجتماعی و سایر سیستم‌هایی که با داده‌های شخصی افراد سروکار دارند، اتحادیه اروپا تلاش‌های خود را برای ایجاد بستر قانونی جهت محافظت از داده‌ها و حریم خصوصی افراد شروع کرد تا اینکه درنهایت قانون جامع و فراگیری موسوم به GDPR در اتحادیه اروپا وضع و تصویب شد تا محافظت از داده‌های شهروندان اتحادیه اروپا را ارتقاء دهد و چارچوبی جهت استفاده تجاری از داده‌های شخصی افراد در سرتاسر اتحادیه اروپا مشخص نماید و جایگزین قوانین محافظتی قبلی شود. GDPR از داده‌های شخصی افراد، که شامل همه کسانی که به طور فیزیکی در اتحادیه اروپا ساکن هستند حتی اگر شهروند اتحادیه اروپا نباشند، محافظت می‌کند. با توجه به حوزه‌ای که برای آن تعریف شده و در برگیرنده پایش رفتار افراد نیز می‌باشد، دایره شمول و حوزه قابل اعمال آن بسیار گسترده است و به طور مشخص شامل همه وب‌سایت‌ها و برنامه‌هایی که فعالیت کاربران خود در فضای دیجیتال را رصد می‌کنند می‌شود. تعریف GDPR از حوزه داده‌ها شخصی نیز تا حد زیادی وسیع و گسترده است. اتحادیه اروپا در ارتباط با حفاظت از حریم خصوصی افراد به شدت قاطع و محکم عمل می‌کند و امروز با وضع این قانون جامع مسیر جدیدی را برای محافظت از حقوق افراد شروع کرده است و با وضع جریمه‌های مالی سنگین تا سرحد ۴ درصد سود کل یک شرکت، که می‌تواند به راحتی شرکت‌ها را در بازار با چالش مواجه کند، از اجرای این قوانین پشتیبانی می‌کند.

با توجه به ماهیت شبکه‌های اجتماعی، آن‌ها به طور قطع تحت حوزه قوانین GDPR قرار می‌گیرند. در GDPR دو مفهوم بسیار مهم تعریف شده تحت عنوان کنترل‌کننده داده و پردازشگر داده و مجموعه‌ای از وظایف و نیازمندی‌ها برای آن‌ها تعریف شده است. شرکتی که داده‌ها را جمع‌آوری می‌کند و کنترل داده‌ها در دست او است یک کنترل کننده داده است. به عبارت دیگر کنترل کننده تصمیم می‌گیرد که داده‌های شخصی افراد چرا و با چه هدفی پردازش می‌شود. پردازشگر داده شرکتی است که داده‌ها را از طرف کنترل کننده داده مورد پردازش قرار می‌دهد.

با بررسی شبکه‌های اجتماعی حال حاضر دنیا می‌توان به راحتی به این نتیجه رسید که این شرکت‌های ارائه دهنده سرویس‌های شبکه اجتماعی هم‌زمان می‌توانند نقش کنترل‌کننده داده و پردازشگر داده را ایفا کنند. به عنوان مثال در اکثر سرویس‌های Facebook، این شرکت در نقش کنترل‌کننده داده ایفای وظیفه می‌کند. با این وجود، هنگام همکاری تجاری با طرف‌های ثالث، در نقش پردازشگر داده ظاهر می‌شود. به عنوان مثال وقتی شبکه اجتماعی Facebook داده‌ها را از طرف صاحبان آگهی پردازش می‌کند این مسئله باید در چارچوب یک مبانی قانونی باشد. کنترل‌کننده‌های داده ملزم به انجام اقداماتی در راستای سازگاری با قوانین GDPR هستند که مشخص می‌کند که داده‌ها چگونه جمع‌آوری می‌شوند و چگونه مورد استفاده قرار می‌گیرند و برای چه مدتی این داده‌ها حفظ می‌شوند. همچنین آن‌ها باید این اطمینان را حاصل کنند که پردازشگرهای داده، داده‌ها را به شکل امن و قانونی مورد پردازش قرار می‌دهند. همچنین پردازشگرهای داده نیز طبق قوانین GDPR ملزم هستند که داده‌ها را به شکل امن و قانونی پردازش کنند.

[2] Breach.

۲-۱ ساختار و برخی از مواد قانونی سند GDPR

مقررات عمومی حفاظت از اطلاعات[3]، قانون حفاظت داده در سطح اتحادیه اروپا است که جایگزین دستورالعمل حفاظت از اطلاعات اتحادیه اروپا[4]» شد که در سال ۱۹۹۵ تدوین شده بود. قانون فوق، برای هماهنگی قوانین حفظ حریم خصوصی در سراسر اروپا و با هدف محافظت و توانمندسازی حریم خصوصی داده شهروندان اتحادیه اروپا و تحول در شیوه برخورد سازمان‌ها با رویکرد حریم خصوصی داده‌ها در سراسر اتحادیه اروپا ایجادشده است. GDPR ماحصل چندین سال مذاکره است. اولین پیشنهاد در سال ۲۰۱۲ ارائه گردید و نسخه نهایی آن در ۱۴ آوریل ۲۰۱۶ توسط پارلمان اتحادیه اروپا تصویب گردید و تمامی اعضاء اتحادیه اروپا و بنگاه‌های اقتصادی مرتبط با هر یک از کشورهای اتحادیه ملزم بودند که تا ۲۵ مه ۲۰۱۸ خود را با قوانین و دستورالعمل‌های آن منطبق نمایند. این سند در ۱۱ فصل و ۹۹ ماده ارائه شده است. در این بخش، ۳ فصل اول این سند را شرح می‌دهیم و برای مطالعه جزئیات این سند و سایر فصل‌ها می‌توانید به سایت مرجع[5] این قانون مراجعه کنید.

۱-۲-۱ فصل اول: مقررات عمومی[6]

این فصل شامل ۴ ماده است که در آن ابتدا موضوع سند GDPR و اهداف آن شرح داده‌شده است. سپس به بررسی محدوده قوانین[7] GDPR در ارتباط با داده‌های شخصی افراد و همچنین مواردی که خارج از دایره شمول این قوانین است پرداخته است. در ماده ۳ حوزه و قلمرو سرزمینی[8] اعمال این قوانین در ارتباط با شهروندان اتحادیه اروپا شرح داده‌شده است و در نهایت مفاهیم به کار رفته در سند GDPR تعریف شده است.

۲-۲-۱ فصل دوم: اصول

این فصل شامل مواد ۵ تا ۱۱ است. در ابتدا، اصول مرتبط با پردازش داده‌های شخصی مورد شرح و بررسی قرار گرفته است که این اصول را می‌توانید در جدول ۱ مشاهده کنید. در ماده ۶، شرایط و موارد قانونی پردازش داده‌ها مورد شرح و بررسی قرار گرفته است. سپس شرایطی که برای اخذ رضایت و موافقت مشتری یا کاربر باید رعایت شود شرح داده‌شده است و در ادامه، شرایط قابل اعمال به فرایند اخذ رضایت و موافقت کودکان در ارتباط با سرویس‌های جامعه اطلاعاتی[9] مورد بررسی قرار گرفته است. ماده ۹ به مسئله پردازش داده‌های شخصی افراد، که در طبقه‌بندی داده‌های شخصی در دسته ویژه و خاص قرار گرفته است، می‌پردازد. داده‌های قومی نژادی، عقاید سیاسی، باورهای دینی و فلسفی، اطلاعات ژنتیکی و بیومتریک در این دسته قرار می‌گیرند. ماده ۱۰ در ارتباط با پردازش داده‌ها و اطلاعات مرتبط با محکومیت‌ها و جرائم قضائی است. در صورتیکه اهدافی که کنترل‌کننده به خاطر آن اطلاعات شخصی افراد را پردازش می‌کند، نیازمندی شناسایی فرد نباشد، کنترل کننده مجاز نیست که اطلاعات اضافی مورد پردازش قرار دهد که در راستای شناسایی فرد باشد. این مسائل در ماده ۱۱ مورد بررسی قرار گرفته است.

---

[3] General Data Protection Regulation (GDPR)
[4] 95/46/EC
[5] https://www.eugdpr.org/
[6] General provisions
[7] Material Scope
[8] Territorial Scope
[9] Information society services

جدول ۱ - اصول مرتبط با پردازش داده

اصول	شرح
پردازش منصفانه، قانونی و شفاف	داده‌های شخصی باید به صورت قانونی، منصفانه و به شیوه‌ای شفاف مورد پردازش قرار گیرد.
محدودیت هدف	داده‌های شخصی می‌بایست صرفا برای اهداف مشخص، صریح و قانونی جمع‌آوری شوند و نباید پردازش‌های مغایر با این اهداف روی آن صورت گیرد.
به حداقل رساندن اطلاعات در حد ضرورت	داده‌های شخصی باید در حد ضرورت و کفایت، مرتبط و محدود به اهداف تعیین شده برای پردازش آن‌ها باشد
دقت و صحت	داده‌های شخصی باید دقیق و صحیح باشند و در صورت نیاز به‌روز شوند و در صورت نادرست بودن اطلاعات، باید بدون تاخیر اصلاح گردند.
دوره نگهداری مشخص	داده‌ها باید به شیوه‌ای نگهداری شوند که در صورتیکه نگهداری آن‌ها برای اهداف، ضرورت نداشته باشد این مسئله مشخص شود.
امنیت داده	امنیت در پردازش داده‌های شخصی باید به‌گونه‌ای صورت پذیرد که از آن‌ها در برابر پردازش‌های غیرمجاز یا غیرقانونی، از دست دادن تصادفی، تخریب و یا آسیب تصادفی محافظت کند
پاسخگویی	کنترل‌کننده داده مسئولیت انطباق با این اصول را بر عهده دارد و باید بتواند سازگاری با این اصول را اثبات کند.

۱-۲-۳ فصل سوم: حقوق افراد

این فصل شامل ۱۲ ماده است که در آن ابتدا به مسئله شفافیت اطلاعات، ارتباطات و شرایطی که لازمه حمایت و پشتیبانی از حقوق افراد است، می‌پردازد. هنگام جمع‌آوری اطلاعات شخصی از داده‌های افراد، آن‌ها باید نسبت به این مسئله آگاه شوند و اطلاعات لازم در این زمینه در اختیار آن‌ها قرار گیرد. همچنین در صورت عدم به دست آوردن اطلاعات شخصی از داده‌های افراد، آن‌ها باید نسبت به این مسئله آگاه شوند و اطلاعات لازم در این زمینه باید در اختیار آن‌ها قرار گیرد. این موارد در مواد ۱۲ و ۱۳ مورد شرح و بررسی قرار گرفته است. در مواد ۱۵ تا ۱۸، به بررسی حقوق افراد در ارتباط با دسترسی به داده‌ها، اصلاح اطلاعات ناقص یا نادرست، حذف اطلاعات مرتبط با آن‌ها و همچنین حق آن‌ها در محدودسازی پردازش داده‌های شخصی و شرایط آن می‌پردازد. همچنین در ماده ۱۹ به تعهد کنترل‌کننده داده مبنی بر اطلاع‌رسانی در زمینه موارد مرتبط با حقوق مصرح در مواد ۱۶ تا ۱۸ می‌پردازد. بر اساس ماده ۲۰، افراد حق دارند که خواستار دریافت و انتقال داده‌های خود به شکل قابل حمل، ساختارمند و در فرمت‌های قابل خواندن توسط ماشین[10] باشند. این ماده به شرح و بررسی این مسئله می‌پردازد. ماده ۲۱، حق افراد در مخالفت با زمینه‌ها و مواردی که مرتبط با آن‌هاست را به رسمیت شناخته شده است و ماده ۲۲ به بررسی حق افراد در ارتباط با فرایندهای تصمیم‌گیری اتوماتیک بر اساس داده‌های آن‌ها می‌پردازد. در پایان شرایط و محدودیت‌ها قانونی موجود اتحادیه و اعضای آن در ارتباط با مواد ۱۲ تا ۲۲ و همچنین مواد ۵ و ۳۴ را مورد شرح و بررسی قرار می‌دهد.

[10] Machine-readable

۱-۳ اثرات GDPR بر روی تجارت

دادها می‌توانند مرزهای اتحادیه اروپا را درنوردند با این وجود GDPR از اطلاعات شهروندان اتحادیه اروپا محافظت می‌کند و مهم نیست سازمانی که داده‌های شهروندان اروپایی را نگهداری می‌کند در کجا قرار داشته باشد. GDPR با این پیش‌زمینه عمل می‌کند که امروزه جمع‌آوری و پردازش داده‌ها موتور اصلی بسیاری از کسب‌وکارهای تجاری است. بر این اساس، برای سازگاری و انطباق یک شرکت یا سازمان با GDPR، نه‌تنها داده‌های مشتریان باید با دقت مدیریت شوند بلکه باید این امکان برای آن‌ها فراهم باشد تا بتوانند آن را کنترل، پایش و بررسی کنند و حتی در صورت نیاز، هر زمان که خواستند داده‌های مرتبط با خود را حذف کنند. شرکت‌هایی که می‌خواهند با GDPR سازگار باشند، باید فرایندهایی را پیاده‌سازی کنند تا این اطمینان حاصل شود که هنگام اداره کردن داده‌های افراد، آن‌ها تحت محافظت قرار گرفته‌اند.رمزنگاری[11]، ناشناس‌سازی[12] و مستعارسازی[13] تکنیک‌هایی هستند که معمولا در این مسیر از آن استفاده می‌شود.

ناشناس‌سازی شامل مجموعه اقداماتی نظیر رمز کردن داده‌ها و یا حذف داده‌های شخصی قابل شناسایی از میان اطلاعات است که باعث می‌شود فردی که توسط این اطلاعات توصیف می‌شود، ناشناس باقی بماند. در مستعارسازی، فیلدهای قابل شناسایی افراد در میان داده‌ها را با اطلاعات ساختگی و مستعار، جایگزین می‌کنیم. همچنین در این فرایند پس از حذف داده‌های قابل شناسایی، مولفه‌های داده می‌توانند از هم جدا شوند و به هر مولفه یک شناسه ساختگی مجزا تخصیص یابد. به عنوان مثال ممکن است شناسه‌ای که سیستم به کاربر برای اطلاعات مکانی‌اش اختصاص می‌دهد با شناسه‌ای که به او در ارتباط با اطلاعات مرورگرش، تخصیص می‌دهد متفاوت باشد. این دو فقره اطلاعات، با دو شناسه مختلف برای یک کاربر، تنها زمانی می‌توانند یکپارچه شوند که مولفه اطلاعاتی دیگری (مثلا تاریخ تولد) آن‌ها را به هم پیوند دهد. به همین دلیل، GDPR مستعارسازی را به ناشناس‌سازی ترجیح می‌دهد زیرا مستعارسازی نوع ارتقاء یافته ناشناس‌سازی است.

براساس GDPR، شرکت‌ها باید اهرم‌ها و ابزارهای حفاظتی در اختیار کاربران قرار دهد تا از حقوق خود محافظت کنند. شاکله اصلی این مسئله این است که فرایندها و ارتباطات باید به شکل شفاف، دقیق و براساس اخذ صریح رضایت کاربر صورت پذیرد.

۱-۴ اهرم‌های قانونی و حفاظتی GDPR

قلمرو قضائی و حقوقی GDPR بسیار گسترده[14] است. GDPR در ارتباط با همه شرکت‌هایی که داده‌های شخصی شهروند اتحادیه اروپا را پردازش می‌کنند، قابل اعمال است و مهم نیست که شهروند اتحادیه اروپا در کجا ساکن باشد. وضع جرائم سنگین یکی از اهرم‌هایی است شرکت‌ها را ملزم به تحقق نیازمندی‌های مطرح شده در این سند قانونی کرده است. نقض قوانین می‌تواند جرائمی به میزان ۲۰ میلیون یور تا ۴ درصد از سود سالانه شرکت را به آن‌ها تحمیل کند. علاوه بر این، در فضای رقابتی موجود، سازگاری و انطباق با GDPR برای شرکت‌ها یک مزیت تجاری از منظر کاربران به حساب می‌آید. وجود این قوانین کمک می‌کند که هنگام ایجاد یک سیستم دغدغه حریم خصوصی را از همان ابتدا در طراحی لحاظ کنیم تا اینکه پس از ایجاد سیستم در جهت رفع تهدیدات و مخاطرات در این حوزه باشیم.

[11] encryption
[12] Anonymization
[13] Pseudonymization
[14] Broad jurisdication

برای حفاظت از داده‌های شخصی هنگام پردازش آن‌ها، GDPR شرکت‌ها را ملزم به اخذ رضایت از افراد[15] به شکل ساده و سر راست کرده است. رضایت باید به شکل ساده، قابل فهم و با اهدافی مشخص به شکل واضح از کاربر اخذ گردد و این امکان برای کاربر باشد تا رضایت خود را پس بگیرد. از آنجایی که کودکان در معرض آسیب‌پذیری بیشتری قرار دارند و نسبت به مخاطرات موجود آگاهی کمتری دارند، GDPR شامل رهنمودهایی است که شامل کسب رضایت و مجوز والدین برای کودکان تا سن ۱۶ سال می‌باشد. هرگونه نقض داده که احتمالا منجر به ایجاد مخاطره برای حقوق و آزادی‌های افراد می‌شود باید در عرض حداکثر ۷۲ ساعت پس از کشف گزارش شود. پردازش‌گران داده به محض اطلاع یافتن از نقض داده، باید مشتریان خود را در اسرع وقت نسبت به این مسئله مطلع سازند. مشتری این حق را دارد که یک نسخه از اطلاعاتی که از او در اختیار شرکت یا سازمان است را داشته باشد و همچنین از نحوه استفاده آن‌ها مطلع باشد. همچنین این حق را دارد که خواستار حذف این اطلاعات شود و یا خواهان انتقال آن به یک سرویس‌دهنده[16] دیگر شود.

۵-۱ اقدامات اولیه در ارتباط با GDPR

برای سازگاری و انطباق یک سازمان با GDPR، آمادگی و برنامه‌ریزی اولیه نقش کلیدی در موفقیت دارد. بر همین اساس یک سازمان نیازمند تعامل نزدیک و یکپارچه واحدهای IT و واحدهای تجاری خود است. استخدام یک کارشناس مسئول محافظت از داده[17]، می‌تواند به تسهیل این فرایند کمک کند. قبل ورود به فاز جدی و عملیاتی، نیازمند بررسی و ارزیابی وضعیت فعلی سیستم امنیتی هستیم تا با استفاده از این اطلاعات، ریسک‌ها و شکاف‌های موجود بین وضعیت فعلی و وضعیت مطلوب از منظر نیازمندی‌های مطرح شده در GDPR مشخص شود. علاوه بر این آموزش کارمندان نقش مهمی در تسهیل فرایند سازگاری ایفا می‌کند زیرا به یکسان‌سازی دید کارمندان نسبت به ماهیت موضوع کمک می‌کند و انتظارات موجود از آن‌ها را مشخص می‌نماید. حفاظت از حریم خصوصی بدون استفاده از ابزارهای مناسب برای این مسئله، ممکن نیست. به همین دلیل ابزارهای لازم جهت اطمینان از حفظ حریم خصوصی افراد باید ایجاد شود. همچنین در صورت نیاز می‌توان از سرویس‌ها و خدمات شرکت‌های ثالث در این زمینه کمک گرفت.

[15] Data subject
[16] Service provider
[17] Data Protection Officer (DPO)

فصل ۲ ارائه یک چارچوب برای سازگاری و تطبیق با GDPR

قوانین GDPR شرکت‌ها را در معرض نیازمندی‌های جدید، ورای رویه‌های امنیتی فعلی، قرار می‌دهد. برای اینکه مشخص کنید آیا شرکت شما تحت تاثیر قانون GDPR قرار می‌گیرد یا نه، پاسخگویی به سه سوال زیر می‌تواند مفید باشد:

۱. آیا شرکت شما کالا یا خدماتی را به افراد ارائه می‌کند؟
۲. آیا شرکت شما رفتار افراد را پایش می‌کند؟
۳. آیا شرکت شما کارمندانی در اتحادیه اروپا دارد؟

مثبت بودن پاسخ به هر یک از این سوال‌ها نشان می‌دهد که احتمالا GDPR در مورد شرکت شما مصداق دارد. اما رسیدن به یک دید جامع و کلی در مورد اینکه آیا یک شرکت درگیر هر یک از این فعالیت‌ها است نیازمند اطلاعات دقیق از واحدهای مختلف آن شرکت است. برای این منظور نیازمند ارزیابی واحدها کلیدی نظیر، مهندسی، منابع انسانی، امنیت اطلاعات، حقوقی، بازاریابی، تدارکات، مدیریت محصولات و واحد توسعه وب‌سایت‌ها و دیگر بسترهای آنلاین هستیم. در صورتیکه هر یک از این بخش‌ها با داده‌های شخصی افراد از هر نوعی سر و کار داشته باشند، آنگاه تحقیقات بیشتری در آن زمینه باید انجام شود تا مشخص شود که آیا قوانین GDPR در آن بخش باید اعمال شود یا نه. بر همین اساس TrustArc[18] یک چارچوب سطح بالا جهت حرکت به سمت انطباق و سازگاری با قوانین GDPR ارائه کرده است. بر اساس این چارچوب، علیرغم پیچیدگی و نیازمندی‌های جدید ایجادشده، انطباق با قوانین GDPR را می‌توان از طریق یک نقشه راه در ۵ فاز به سرانجام رساند. در شکل ۱، نمای کلی چارچوب پیشنهادی TrustArc را مشاهده می‌کنید.

ساخت برنامه و تیم	ارزیابی ریسک‌ها و ایجاد خودآگاهی	طراحی، پیاده‌سازی و کنترل‌های عملیاتی	مدیریت، حفظ و ارتقاء کنترل‌ها	نشان دادن انطباق با قوانین به شکل مداوم
شناسایی ذینفعان	ارزیابی فهرست داده‌ها و تحلیل جریان داده	اخذ و مدیریت رضایت و موافقت	ارزیابی اثرات بر حریم خصوصی	ارزیابی و حسابرسی میزان موثر بودن
تخصیص منابع و بودجه	ارزیابی ریسک‌ها و شکاف‌های موجود	انتقال داده‌ها و مدیریت شرکت‌های ثالث	ضرورت داده، دوره نگهداری و حذف	گزارش‌دهی داخلی و خارجی
انتخاب مسئول حفاظت از داده‌ها	توسعه سیاست‌ها، روال‌ها و فرایندها	حقوق محافظت از داده‌های شخصی افراد	یکپارچگی داده و کیفیت آن	اعلان‌های امنیتی و مکانیسم حل اختلاف
تعریف برنامه، اهداف و ماموریت‌ها	گفتگو در زمینه انتظارات و آموزش	حفاظت‌های فیزیکی، فنی و مدیریتی	تعیین نحوه مواجهه به هنگام وقوع نقض داده	اخذ گواهینامه

شکل ۱- چارچوب سطح بالا جهت سازگاری با GDPR

همه این فازها حول سه محور افراد، فرایندها و تکنولوژی (ابزارها و پلتفرم‌ها) شکل می‌گیرد. افراد دخیل در این مسئله باید مسئولیت‌پذیر و دارای دانش ضروری برای انجام یک ارزیابی کامل باشند. باید این اطمینان حاصل شود که افراد درگیر در این

[18] https://www.trustarc.com/

مسئله آموزش‌های لازم در مورد فرایند و تکنولوژی را دیده‌اند. فرایند باید دارای یک گردش‌کار جهت جمع‌آوری اطلاعات و شناسایی شکاف‌های موجود در ارتباط با نیازمندی‌ها باشد. برای این منظور می‌توان از رویه‌های کاری و قالب‌های نظیر پرسشنامه و یا چک‌لیست استفاده کرد. پلتفرم‌های مدیریت حریم خصوصی داده‌ها[19] به همراه قابلیت‌های درونی آن نظیر اکتشاف داده[20]، فهرست داده‌ها[21]، قالب‌های ارزیابی اثرات روی حریم خصوصی، چرخه‌های کاری[22] و گزارش‌دهی، امکان مشارکت اعضای تیم و هدایت فرایندها را فراهم می‌کند. همچنین می‌تواند به عنوان یک مخزن متمرکز برای نشان دادن سازگاری و انطباق با قوانین مورد استفاده قرار گیرد و فرایند حسابرسی دوره‌ای و انعکاس تغییرات فضای کسب‌وکار را تسهیل کند.

۲ ۱ فاز یک: ایجاد اجماع و ساخت یک تیم

ابتدا باید با ذینفعان مختلف صحبت کنید تا مشخص شود که آیا ضرورتی برای اعمال GDPR در سازمان یا شرکت وجود دارد یا نه. ذینفعان کلیدی را می‌توانید از میان افرادی که در واحدهای مهندسی، منابع انسانی[23]، امنیت اطلاعات[24]، حقوقی[25]، بازاریابی[26]، تدارکات[27]، مدیریت محصول[28] و توسعه وب مشغول[29] به فعالیت هستند، شناسایی کنید. با کمک این ذینفعان می‌توانید درک سطح بالایی از وضعیت سازگاری خود با قوانین پیدا کنید. برای این منظور باید رویه‌های فعلی خود را با لیست جامعی از نیازمندی‌ها که شامل حوزه‌های زیر است مقایسه کنید.

۱. **جمع‌آوری و محدودسازی اهداف:** آیا اجازه جمع‌آوری داده‌ها را دارید و آیا داده‌ها فقط در محدوده اهداف خود مورد استفاده قرار می‌گیرند؟
۲. **نقض داده‌ها و آمادگی برای پاسخ‌گویی:** آیا آمادگی اداره کردن و پاسخگویی به بروز نقض داده، بر اساس نیازمندی‌های GDPR را دارید؟
۳. **کیفیت داده‌ها:** چه شاخص‌ها و معیارهایی برای اطمینان از ارتباط، صحت، کامل بودن و به هنگام بودن اطلاعات شخصی نگهداری شده وجود دارد؟
۴. **حقوق افراد:** یکی از تغییرات کلیدی در GDPR، توسعه حقوق افراد مانند حق دسترسی، اصلاح، محدودسازی پردازش، پاک کردن و غیره است که بر اساس آن باید سیاست‌های موجود، فرایندها و روال‌ها مورد بازبینی قرار گیرند.
۵. **مدیریت حریم خصوصی:** فرایند ساخت، نظارت و نمایش رویه‌های کاری مناسب برای مدیریت حریم خصوصی در سازمان چگونه است؟
۶. **امنیت از منظر حریم خصوصی:** چه شاخص‌ها و روال‌های فنی باید طراحی شود تا از داده‌های شخصی افراد سازمان محافظت کند؟

---

[19] Data privacy
[20] Data discovery
[21] Data inventory
[22] Workflows
[23] Human resources
[24] Information security
[25] Legal
[26] Marketing
[27] Procurement
[28] Product management
[29] Website development

۷. **شفافیت:** چگونه روندهای اداره داده‌ها را برای صاحبان آن داده[30] آشکار می‌سازد؟

در ارتباط با بخش‌هایی که هسته اصلی فعالیت کنترل کننده یا پردازشگر داده شامل پایش منظم و دوره‌ای داده‌های افراد در مقیاس وسیع است و یا پردازش‌هایی در مقیاس وسیع بر روی یک دسته خاص از اطلاعات شخصی افراد (مثل نژاد، عقاید سیاسی و ...) صورت می‌گیرد، باید یک افسر حفاظت از داده[31] یا DPO انتخاب شود. DPO می‌تواند یک کارمند و یا یک طرف ثالث، که سرویس‌های مشاوره‌ای و یا حقوقی را ارائه می‌کند، باشد. در هر صورت DPO باید گزارش‌های خود را به بالاترین سطح مدیریتی ارائه کند و در نهایت استقلال عمل نماید.

۲ ۲ فاز دوم: ارزیابی ریسک‌ها و ایجاد خودآگاهی

برای اینکه نسبت به شناسایی همه ریسک‌ها و برنامه‌ریزی بر اساس اولویت آن‌ها اطمینان حاصل کنیم لازم است که یک فهم درست از چرخه زندگی[32] داده‌ها در سازمان داشته باشیم. این پروژه نیازمند سطح بالایی از مشارکت‌های بین بخشی و درون سازمانی است. به فرایند مستندسازی چرخه زندگی داده‌ها، تحلیل داده‌های موجود[33] و یا نگاشت داده‌ها[34] گفته می‌شود.

۲-۲-۱ تحلیل داده‌های موجود و نگاشت داده‌ها

فرایند جمع‌آوری، مستندسازی چرخه زندگی داده‌ها و تحلیل آن‌ها شامل گام‌های زیر است.

۱. اطلاعات لازم در زمینه جمع‌آوری، ذخیره‌سازی، انتقال، پردازش و حذف داده‌ها را از ذینفعان اصلی به دست آورید. جزئیات این اطلاعات باید شامل موارد زیر باشد.
   a. داده‌هایی که جمع‌آوری می‌کنند
   b. نحوه استفاده از داده‌ها
   c. محلی که داده‌ها در آن ذخیره می‌شود
   d. نحوه جریان داده‌ها در داخل و یا خارج سازمان
   e. کسانی که به داده‌ها دسترسی دارند
   f. نوع حفاظتی که از آن‌ها در هر مرحله صورت می‌گیرد.
۲. این اطلاعات را در قالب لیستی از داده و نمودارهای بصری مستندسازی کنید.
۳. ریسک‌های موجود در ارتباط با GDPR و سایر نیازمندی‌ها را تحلیل کنید.

در شکل ۲ یک دسته‌بندی معمول از داده‌ها نشان داده‌شده است.

[30] Data subjects
[31] Data Protection Officer
[32] Lifecycle
[33] Data inventory analysis
[34] Data mapping

داده‌های شخصی قابل شناسایی - غیر حساس	داده‌های شخصی قابل شناسایی - حساس	دسته‌های خاص داده
• محل کار • تلفن تماس محل کار • اطلاعاتی که به صورت عمومی در دسترس است	• اطلاعات قومی و نژادی • گرایش‌های سیاسی، باورهای مذهبی و فلسفی افراد • داده‌های مرتبط با وضعیت سلامتی و یا گرایشات جنسی افراد	• اطلاعات مالی و پرداخت‌ها • اطلاعات بیومتریک، ژنتیک و مرتبط با سلامت • اطلاعات شخصی کودکان

شکل ۲- دسته‌بندی داده‌ها

۲-۲-۲ ارزیابی شکاف‌های موجود و مشخص کردن سطح لازم برای تلاش[35]

با استفاده از نتایج تحلیلی به دست آمده در مرحله قبل می‌توان به شکاف‌های موجود را ارزیابی کرد و با توسعه ماتریس سطح تلاش (LOE)، فرایند اولویت‌بندی گام‌های بعدی را تسهیل کرد. ستون‌های این ماتریس میزان تلاش لازم را نشان می‌دهد و سطرهای آن بیان‌کننده میزان ریسک است.

۲-۲-۳ توسعه سیاست‌ها، روال‌ها و فرایندها

بر اساس نتایج ارزیابی شکاف‌های موجود و میزان تلاش لازم جهت اداره و رفع آن‌ها، وظایف و کارهای لازم، به بخش‌های مختلف عملیاتی تخصیص می‌یابد و برنامه زمانی اتمام آن‌ها مشخص می‌شود. ریسک‌های سطح بالا، اولویت بالاتری دارند و در نتیجه برنامه زمان‌بندی اجرای کارهای مرتبط با رفع ریسک‌های موجود بر این اساس صورت می‌گیرد. همچنین در صورتی که رفع یک ریسک نیازمند سطح بالاتری از تلاش باشد، بهتر است اداره کردن آن را زودتر شروع کنیم. سیاست‌ها، روال‌ها و فرایندهایی که در این زمینه تعریف می‌شود نقش حیاتی در سازگاری با انتظارات GDPR دارد. مستند کردن انتظارات از افراد و طرف‌های درگیر در این مسئله و توصیف دقیق اینکه آن‌ها چگونه باید در برنامه روزانه خود به این انتظارات جامه عمل بپوشانند یکی از اساسی‌ترین مولفه‌های دستیابی به سازگاری و انطباق با GDPR است. به موازات این مولفه، آموزش افراد درگیر نقش کلیدی در موفقیت آن‌ها در نیل به خواسته‌ها دارد. نکته مهم دیگری که باید به آن توجه کرد این است که اداره کردن داده‌ها بر اساس نیازهای مطرح شده در GDPR به تنهایی کافی نیست بلکه باید بتوانیم این سازگاری و انطباق را نشان دهیم.

۲-۲-۴ تعامل و تبادل نظر

رسیدن به اجماع نقش حیاتی در موفقیت برنامه‌های مرتبط با امنیت در سطح یک سازمان دارد به خصوص اگر این برنامه با پیچیدگی‌هایی نظیر آنچه که در GDPR مطرح است مواجه باشد. در این مرحله است که اصول بنیادی رهبری و تصمیم‌گیری نقش خود را ایفا می‌کند. این فرایند را می‌توان با توسعه یک توصیف روایی از نیازها و نظرات موافقین و مخالفین سرمایه‌گذاری روی آن، شروع کرد و از سایر استراتژی‌های تعامل و گفتگو استفاده کرد تا در نهایت به یک روایت متقاعد کننده در مورد تلاش‌های لازم جهت سازگاری و انطباق با GDPR دست پیدا کرد.

[35] Level Of Effort (LOE)

۲-۲-۵ به اشتراک‌گذاری دلایل با ذینفعان اصلی

جلسات برنامه‌ریزی باید به صورت مداوم و با حضور همه ذینفعان مرتبط برگزار شود و تلاش کنید تا با به اشتراک‌گذاری و ارائه اطلاعات و مستندات جمع‌آوری‌شده، این فرایند را تسهیل کنید. نکته کلیدی در این بحث این است که به طور صریح و مشخص اهداف چنین جلساتی باید به صورت شفاف بیان شود. برخی از این اهداف عبارت‌اند از:

۱. برنامه GDPR، ساختار تیم، نقش‌ها و مسئولیت‌ها باید به شکل رسمی مشخص شود
۲. برنامه GDPR به عنوان یک طرح اولویت‌دار مطرح و به رسمیت شناخته شود.
۳. بر روی اهداف کوتاه‌مدت میان‌مدت و بلندمدت GDPR توافق شود
۴. اهداف قابل سنجش، شاخص‌های موفقیت قابل ارزیابی و نقاط عطف پروژه مشخص و تعیین گردد.
۵. بر اساس سطح تلاش مورد نیاز، بودجه و منابع مورد نیاز تخصیص یابد.

جلسات برنامه‌ریزی به شکل دوره‌ای و مداوم باید در نظر گرفته شود تا در صورت نیاز به اصلاح آن، همچنان ضرب‌آهنگ پیوسته پیاده‌سازی نیازمندی‌ها و پیشرفت پروژه حفظ شود. این یک باور اشتباه است که تصور کنیم می‌توان به یکباره، یک برنامه جامع و کامل برای این پروژه در نظر گرفت که هیچ‌گاه تغییر نمی‌کند. بنابراین برنامه‌ریزی و مرور و بازبینی مداوم برنامه، یک فرایند دائمی در طول پروژه است.

۲-۲-۶ آموزش

پس از اینکه همگان نسبت به اهمیت و فوریت مسئله آگاهی پیدا کردند، با استفاده از آموزش به ذینفعان کمک می‌کنیم تا نسبت به تغییرات مورد نیاز در سازمان درک درستی پیدا کنند. به عنوان مثال برخی از موضوعاتی که به عنوان شروع فرایند آموزش می‌تواند مورد استفاده قرار گیرد عبارت‌اند از:

۱. مرور کلی GDPR و دلایل اهمیت آن
۲. شرح اثرات GDPR بر روی سازمان یا شرکت
۳. بحث و گفتگو در مورد فعالیت شرکت در ارتباط با GDPR و برنامه زمانی آن
۴. توضیح در مورد نحوه مشارکت ذینفعان در انجام این فعالیت‌ها

پس از آماده‌سازی برنامه و کسب موافقت و حمایت سازمان، می‌توان اقدامات لازم برای عملیاتی کردن پروژه را شروع کرد که شامل طیف گسترده‌ای از ایده‌ها و برنامه‌ها از قبیل، جذب نیروی جدید، آموزش پرسنل قبلی، بنیان نهادن فرایندهای جدید و استفاده از تکنولوژی‌های جدید می‌شود.

۲-۳ فاز سوم: طراحی، پیاده‌سازی و کنترل‌های عملیاتی

در این فاز به طراحی و پیاده‌سازی مکانیسم‌هایی جهت اخذ رضایت و مدیریت آن در ارتباط با پردازش‌داده‌های شخصی افراد می‌پردازیم و استانداردهای لازم جهت حفاظت از داده‌ها در تبادلات بین‌المللی را مشخص می‌کنیم. همچنین بر مبنای حقوق افراد در ارتباط با محافظت از داده‌های شخصی، اقدامات فیزیکی، فنی و مدیریتی لازم را انجام می‌دهیم.

۲-۳-۱ مکانیسم‌های اخذ رضایت و مدیریت آن

نیازمندی‌های مرتبط با رضایت و موافقت تحت GDPR بسیار جدی هستند و برای شرایط مختلف تعریف شده‌اند. برای پردازش داده‌های افراد، اخذ موافقت آگاهانه کاربر و یا تائید آشکار آن در قالب یک عمل، به شکل شفاف مشخص و غیر مبهم، مسئله‌ای ضروری است. به عنوان مثلا کاربر باید تیک مربوط به موافقت را بزند و انتخاب پیش‌فرض آن از سوی سیستم کافی

نیست. موافقتی که برای یک پردازش خاص روی‌داده‌ها اخذ می‌شود، خاص همان عمل است و کاربر باید بتواند در هر زمان، موافقت خود را از آن عمل پس بگیرد. در مورد پردازش داده‌های خاص مثل اطلاعات ژنتیکی اخذ رضایت باید به شکل صریح[36] صورت گیرد. همچنین در مورد داده‌های مربوط به کودکان (زیر ۱۶ سال)، اخذ رضایت و موافقت والدین آن‌ها به شکل صریح، الزامی است و تلاش لازم جهت اعتبارسنجی فرایند اخذ موافقت والدین کودک به شکل صحیح و کامل، ضروری است.

۲-۳-۲ محقق کردن شروط لازم جهت تبادل بین‌المللی داده و استانداردهای محافظت از داده

GDPR اجازه انتقال داده‌ها به کشورهای غیر عضو اتحادیه را در صورت فراهم کردن روش‌های حفاظت از داده‌ها را می‌دهد. بر اساس ماده ۴۶، روش‌های حفاظتی مناسب شامل BCRs[37]، MCCs[38] یا SCCs[39] و مستندات قانونی الزام‌آور و قابل‌اجرای نهادهای عمومی دولتی است.

۲-۳-۳ حقوق افراد در ارتباط با محافظت از داده‌های شخصی

GDPR در سطوح مختلفی از حقوق افراد نظیر حق اطلاع‌رسانی[40]، حق دسترسی[41]، حق اصلاح اطلاعات[42]، حق محدود کردن پردازش[43]، حق اعتراض[44]، حق پاک کردن[45]، حق درخواست داده به شکل قابل حمل[46] محافظت می‌کند. در ادامه برخی از این حقوق را شرح می‌دهیم. پردازش‌ها و قابلیت‌های تکنولوژیکی که در یک سازمان به کار گرفته می‌شود باید در جهت صیانت از این حقوق و برآورده کردن آن باشد و امکان دریافت و تحقق درخواست‌هایی که در راستای این حقوق هستند، باید وجود داشته باشد.

حق اطلاع‌رسانی

وقتی داده‌های شخصی افراد را پردازش می‌کنید، نیازمند اطلاع‌رسانی به کاربران هنگام جمع‌آوری داده‌ها هستید و این مسئله باید در قالب یک اعلان صریح مرتبط با حریم خصوصی باشد. این اعلان باید حداقل شامل اطلاعات زیر باشد:

- چرا داده شخصی فرد را پردازش می‌کنید.
- این فرایند برای چه مدتی خواهد بود
- طرف‌های دیگری که این اطلاعات با آن‌ها به اشتراک گذاشته می‌شود چه کسانی هستند
- لینک ارجاع به صفحه کامل سیاست‌های حریم خصوصی

حق دسترسی

اگر کاربری خواهان دسترسی به داده‌های شخصی خود باشد، هویت کاربر باید تائید شود.

---

[36] Explicit
[37] Binding Corporate Rules (BCRs)
[38] Model Contract Clauses (MCCs)
[39] Standard Contractual Clauses (SCCs)
[40] Right to information
[41] Right to access
[42] Right to rectification
[43] Right to restrict Processing
[44] Right to object
[45] Right to Erasure
[46] Right to Data portability

حق اصلاح اطلاعات

کاربران این حق را دارند که در صورت مواجه با اطلاعات ناصحیح، خواستار اصلاح فوری آن شوند. همچنین آن‌ها باید بتوانند اطلاعات ناقص را تکمیل کنند.

حق پاک‌کردن

کاربران این حق را دارند که خواهان حذف داده‌های شخصی خود شوند و این خواسته باید در اسرع وقت محقق شود و پس از حذف کامل اطلاعات، این مسئله باید به اطلاع و تائید او برسد.

حق درخواست داده به شکل قابل حمل

کاربر این حق را دارد تا یک کپی از اطلاعات شخصی‌اش را به شکل قابل حمل و قابل خواندن توسط ماشین در قالب فرمت‌های عمومی دریافت کند. این اطلاعات باید پس از اطمینان یافتن از هویت کاربر در اختیار او قرار گرفته و تائیدیه آن دریافت شود.

حق اعتراض

کاربر این حق را دارد تا نسبت به پردازش داده‌های شخصی‌اش اعتراض کند و در این شرایط کنترل‌کننده داده حق پردازش این اطلاعات را ندارد مگر اینکه نشان دهد که این مسئله بر مبنای قانونی است که این حق کاربر را خنثی[47] می‌کند.

حق پس‌گرفتن رضایت و موافقت

این حق، درشرایطی که پردازش داده‌های شخصی بر مبنای رضایت و موافقت کاربر باشد قابل اعمال است. در این شرایط اگر مکانیسمی برای اخذ رضایت و موافقت کاربر برای پردازش داده‌ها وجود دارد، مکانیسم بازپس‌گیری این موافقت نیز باید ایجاد شود.

۲-۳-۴ حفاظت‌های فیزیکی، فنی و مدیریتی

رعایت حریم خصوصی بدون تامین امنیت امکان‌پذیر نیست. به همین دلیل نیازمند اقدامات فیزیکی، فنی و مدیریتی هستیم که این اطمینان را ایجاد کند که داده‌ها امن هستند. GDPR به استاندارد خاص امنیتی ارجاع نمی‌دهد با این وجود این وظیفه سازمان‌ها است که حفاظت‌های امنیتی را مورد ارزیابی قرار داده و خلاءهای موجود را بپوشانند.

۲ ۴ فاز چهارم: مدیریت، حفظ و ارتقاء کنترل‌ها

بر اساس ماده ۳۵، هر نوع پردازش داده‌ای که دارای ریسک بالا است را باید بررسی کرد و اثرات آن بر روی حریم خصوصی و محافظت از داده‌ها را مورد ارزیابی قرار داد که اصطلاحا به این فرایند DPIA[48] گفته می‌شود. این ارزیابی باید شامل موارد زیر باشد:

۱. یک توصیف سیستماتیک از عملیات پردازشی و اهداف آن
۲. ارزیابی میزان ضرورت آن

[47] Override
[48] Data Protection Impact Assessment

۳. ارزیابی ریسک‌های مرتبط با آن
۴. اقداماتی که برای رفع این ریسک‌ها باید انجام شود.

در ماده ۲۵، اشاره شده است که فقط داده‌هایی که ضروری هستند باید مورد پردازش قرار گیرند و در صورتیکه نیازی به نگهداری و ذخیره این اطلاعات به شکل قابل شناسایی[49] نبود، باید از تکنیک‌های ناشناس‌سازی[50] و مستعارسازی[51] استفاده کرد. در ماده ۳۲، خواسته شده است که از تغییر داده‌ها در صورت عدم وجود مجوز و صلاحیت لازم، جلوگیری شود و اقدامات لازم برای اطمینان یافتن از این مسئله که داده‌ها صحیح، مرتبط، به‌روز و کامل هستند به عمل آید. همچنین در ماده ۳۳ و ۳۴ خواسته شده است که برای پاسخگویی به نقض‌های امنیتی و داده، برنامه‌ریزی لازم صورت گیرد. این مسئله نیازمند اصلاح سیاست‌های امنیتی، برنامه‌ریزی برای پاسخگویی در صورت بروز نقض و استقرار و آموزش این برنامه در سازمان است تا همان‌طور که خواسته شده است ظرف کمتر از ۷۲ ساعت، اطلاع‌رسانی در مورد بروز این نقض و اقدامات لازم جهت جلوگیری از ایجاد خطر و آسیب، صورت پذیرد. در خلال اجرای فرایند DPIA و شناسایی شکاف‌ها و اقدامات لازم، گام بعدی تلاش برای رفع این شکاف‌ها است و در این مسیر فعالیت‌های صورت گرفته را مستندسازی کنید تا در صورت بروز مشکل، امکان ردیابی آن را داشته باشید.

۳.۵ فاز پنجم: نشان دادن سازگاری و انطباق به شکل مستمر

آخرین گام در این مسیر این است که به نحوی نشان دهید که سازگاری و انطباق با GDPR به شکل مستمر برقرار است. روش‌هایی برای مرور و ارزیابی فعالیت‌هایی که در جهت سازگاری و انطباق با GDPR پایه‌گذاری کنید و نتایج آن را برای گزارش‌های داخل و خارج سازمانی نگهداری کنید تا مبنایی برای اثبات سازگاری و انطباق سازمان با نیازهای GDPR باشد.

هنگامی‌که همه مولفه‌های مورد نیاز که در بخش‌های قبل به آن اشاره شد پیاده‌سازی و اجرا شدند، آمادگی سازمان در ارتباط با GDPR مورد ارزیابی قرار می‌گیرد تا این اطمینان حاصل شود که همه شکاف‌های موجود پوشش داده‌شده است. برای داشتن یک حسابرسی و ارزیابی دقیق و استوار، بهتر است نکات زیر در نظر گرفته شود:

۱. جزئیات تفصیلی از هر نوع پردازش بر روی‌داده‌های شخصی را نگهداری کنید
۲. با زمان‌بندی انجام حسابرسی‌های دوره‌ای و DPIA مستمر، نسبت به سازگاری و انطباق با نیازمندی‌ها و سیر تکامل آن، اطمینان حاصل کنید.
۳. گزارش‌هایی که نشان دهنده آمادگی سازمان و تحقق همه نیازمندی‌های GDPR است را داشته باشید تا در بازرسی‌ها بتوانید به عنوان مبنای پاسخگویی ارائه کنید.
۴. مستندات پشتیبان فرایندهای DPIA را در یک مخازن متمرکز نگهداری کنید.

[49] Identifiable form
[50] Anonymization
[51] Pseudonymization

فصل ۳ بررسی اقدامات انجام شده توسط برخی شرکت‌های مطرح فضای مجازی در راستای سازگاری با GDPR

در این بخش نحوه تضمین سازگاری با GDPR توسط برخی از شرکت‌های مطرح، بر اساس گزارش خود آن‌ها، مورد بررسی قرار می‌گیرد و اقدامات و الزامات به کار گرفته شده جهت تبعیت از قوانین اتحادیه اروپا توسط این شرکت‌ها به شکل عملیاتی‌تر شرح داده می‌شود.

۳-۱ Facebook

بر اساس ادعای شرکت Facebook، این شرکت هم‌اکنون با قوانین محافظت از داده‌های اتحادیه اروپا که شامل GDPR نیز می‌باشد، سازگار است و فرایند آماده‌سازی این شرکت با کمک تیم محافظت از داده‌ها صورت گرفته است و توسط بزرگ‌ترین تیم چندوجهی[52] تاریخ این شرکت، پشتیبانی شده است. در تمام طول فرایند آماده‌سازی، Facebook متعهد به سه مسئله شفافیت، پاسخگویی و امکان کنترل بوده است. این شرکت تلاش کرد تا شفافیت را از طریق تعریف سیاست‌های داده‌ای و نحوه پردازش داده‌های شخصی افراد تامین کند. همچنین در این زمینه آموزش‌های لازم در ارتباط با محصولات این شرکت را به کاربران ارائه نماید. این کار از طریق اعلان‌های درون برنامه‌ای و همچنین راه‌اندازی کمپین‌هایی در این زمینه صورت پذیرفته است تا کاربران بفهمند که داده‌های آن‌ها چگونه مورد استفاده قرار می‌گیرد و آن‌ها چه گزینه‌هایی در این ارتباط در اختیار دارند. همچنین این شرکت تلاش می‌کند تا به کاربران این امکان را بدهد که بر روی نحوه استفاده از داده‌های خود کنترل داشته باشند. به همین منظور یک مرکز کنترلی جدید راه‌اندازی شد تا فرایند انجام و به‌روزرسانی تنظیمات امنیتی مرتبط را قابل فهم‌تر و ساده‌تر کند. در راستای پاسخگویی و مسئولیت‌پذیری، این شرکت اصول حریم خصوصی و نگاهش به این مسئله و دیدگاهش در مورد حفاظت از داده‌ها را شرح داده است و تیمی تخصصی در این شرکت، کمک می‌کنند تا نسبت به مستندسازی سازگاری با این اصول اطمینان حاصل شود. در کنار این اقدامات، در این شرکت جلسات دوره‌ای با حضور سازمان‌های تنظیم مقررات، کارشناسان حریم خصوصی و چهره‌های دانشگاهی برگزار می‌شود تا با دریافت فیدبک، فرایند محافظت از اطلاعات شخصی افراد ارتقاء یابد.

برای انتقال داده‌ها به بیرون از اتحادیه اروپا، نیازمندی‌های قانونی باید رعایت شود و از این منظر Facebook تحت چارچوب Privacy Shield قرار گرفته است. در قالب این چارچوب آن‌ها می‌توانند داده‌های شخصی افراد را از آگهی‌دهندگان اروپایی خود دریافت و پردازش کنند. در جایی که Facebook در نقش پردازشگر داده از طرف آگهی‌دهندگان اروپایی خود ظاهر می‌شود تلاش می‌کند تا نسبت به سازگاری با قوانین GDPR اطمینان حاصل کند. بر این اساس شرایط استفاده از خدمات در راستای انطباق با GDPR به‌روزرسانی شد. برای انتخاب شرکت‌های ثالث برای ایفای نقش پردازشگر داده از طرف Facebook، شرایط لازم در این رابطه مشخص شده است که متناسب با نیازمندی‌های این شرکت در ارتباط با سازگاری GDPR است. هنگامی که Facebook به عنوان پردازشگر داده از طرف آگهی‌دهندگان عمل می‌کند، این کار را تحت مبانی قانونی آگهی‌دهندگان به عنوان کنترل‌کننده داده انجام می‌دهد.

۳-۲ Telegram

اقدامات برخی شرکت‌ها در راستای تبعیت از GDPR حداقلی بوده که از این جمله می‌توان به پیام‌رسان تلگرام اشاره کرد. بر اساس ادعای سایت رسمی تلگرام، از آنجایی که حریم خصوصی افراد از همان ابتدا دغدغه اصلی تلگرام بوده است، برای

[52] Cross-functional

سازگاری با قوانین GDPR نیازمند تغییر جدی در فرایندها و روال خود نبوده‌اند زیرا تلگرام از داده‌های افراد برای هدف قرار دادن آن‌ها در معرض نمایش تبلیغات استفاده نمی‌کند و این اطلاعات به دیگران فروخته نمی‌شود و تلگرام جزئی از خانواده هیچ شرکتی نیست. تلگرام تنها اطلاعاتی را نگهداری می‌کند که برای ارائه کارکردهای خود در قالب خدمات غنی ابری[53] به آن نیاز دارد.

تلگرام در سایت رسمی خود اعلام کرد که به همراه وکلای حقوقی خود مشغول کار بر روی سیاست‌های حریم خصوصی است و به محض آماده شدن آن را اعلام خواهد کرد. همچنین تلگرام یک ربات تلگرامی موسوم به @GDPRbot ارائه کرده است که به کاربران این امکان را می‌دهد تا یک کپی از داده‌های خود در مخازن تلگرام را دریافت کنند. در راستای اقدامات تلگرام برای تبعیت از GDPR، نسخه اندرویدی 4.8.9 این نرم‌افزار پیام‌رسان شامل به روزرسانی‌های مرتبط با GDPR می‌باشد و در اول ژوئن ۲۰۱۷ شرکت Apple اعلام کرد که نسخه 4.8.2 تلگرام برای iOS دارای ویژگی‌های مرتبط با GDPR می‌باشد.

Matomo ۳-۳

Matomo[54] یک پلتفرم تحلیلی است که امکان کنترل کامل بر روی‌داده‌های دسترسی کاربران به یک وبگاه را فراهم می‌کند. این نرم‌افزار متن‌باز است و امکان توسعه و شخصی‌سازی آن نیز وجود دارد. Matomo در گزارش که اخیرا در وبگاه خود قرار داده است تغییرات فنی صورت گرفته جهت تبعیت از GDPR را تشریح کرده است که می‌تواند دید مناسبی نسبت به اقدامات عملی در این حوزه ارائه دهد. براساس پیکربندی Matomo داده‌هایی که می‌تواند مصداق داده‌های شخصی افراد تلقی گردند عبارت‌اند از:

۱. آدرس IP
۲. کوکی‌ها[55]
۳. آدرس صفحه یا عنوان صفحه
۴. شناسه کار و اطلاعات شخصی خاص[56]
۵. شناسه سفارشات تجاری
۶. موقعیت مکانی
۷. نشست‌ها[57] و نقاط کلیک[58]

در ارتباط با هر یک از این داده‌ها، Matomo راهکارهایی به منظور حفظ حریم خصوصی کاربران ارائه کرده است که در ادامه به اختصار آن‌ها را توضیح می‌دهیم.

۱-۳-۳ آدرس IP

آدرس IP به طور غیر مستقیم می‌تواند باعث شناسایی افراد گردد. همچنین با کمک این اطلاعات می‌توان تخمین خوبی از موقعیت مکانی افراد ارائه کرد. برای حفظ حریم خصوصی کاربران Matomo این امکان را فراهم می‌کند تا بتوان آدرس IP کاربران را ناشناس کرد[59] و برای این منظور پیشنهاد Matomo این است که حداقل ۲ بایت آخر آدرس IP پوشانده[60] شود.

---

[53] Rich cloud service
[54] https://matomo.org/
[55] Cookies
[56] Custom personal data
[57] Sessions
[58] Heatmaps
[59] anonymize

با این کار دیگر قادر به روئیت آدرس کامل IP نخواهید بود. درنتیجه این احتمال وجود دارد که دو بازدیدکننده[61] متفاوت با یک دستگاه و پیکربندی نرم‌افزاری یکسان، بعد از ناشناس‌سازی آدرس IP، به عنوان یک بازدیدکننده تشخیص داده شود، هر چند احتمال این مسئله بسیار کم است.

۳-۳-۲ کوکی‌ها

علیرغم اینکه Matomo نسبت به قرار گیری کوکی‌ها تحت قوانین GDPR مطمئن نیست، با این وجود امکان غیرفعال سازی ایجاد کوکی را در اختیار کاربر قرار می‌دهد. در صورت غیرفعال شدن کوکی‌ها، Matomo از تکنیکی که موسوم به اثرانگشت[62] است استفاده می‌کند که فراداده‌ای[63] مرکب از اطلاعاتی نظیر سیستم‌عامل، مرورگر، افزونه‌های مرورگر، آدرس IP، زبان مرورگر است که از آن برای شناسایی یکتای کاربران استفاده می‌کند.

۳-۳-۳ آدرس صفحات و عناوین صفحه

آدرس صفحات به طور مشخص توسط متن رسمی GDPR مورد اشاره قرار نگرفته است با این وجود، می‌دانیم که آدرس صفحات در برخی از سیستم‌های مدیریت محتوا ممکن است همراه با شناسه‌های شخصی افراد باشد. به عنوان مثال ممکن است نام و نام خانوادگی فرد بخشی از دنباله آدرس صفحه باشد. به همین دلیل این اطلاعات باید به نحوی، ناشناس‌سازی گردد. در صورتیکه اطلاعات شخصی افراد به عنوان پارامترهایی جهت جستجو به دنباله آدرس اضافه شوند باید حذف گردند و برای پیاده‌سازی این مسئله Matomo راهکارهای مختلفی بسته به ماهیت و نوع وب‌سایت ارائه کرده است. به عنوان مثال، Matomo امکان ایجاد آدرس‌های ساختگی و یا تنظیم عناوین صفحه را فراهم می‌کند. با ناشناس‌سازی آدرس صفحات این احتمال وجود دارد که مجموعه از آدرس‌ها، در قالب یک گروه طبقه‌بندی شوند.

۳-۳-۴ شناسه کاربران و اطلاعات شخصی خاص

شناسه‌کاربر، داده‌ای است که به شما این امکان را می‌دهد تا یک کاربر را در میان سایرین شناسایی کنید. این شناسه می‌تواند آدرس ایمیل، نام‌کاربری، یک نام و یا یک عدد تصادفی باشد. همه این داده‌ها به شکل مستقیم یا غیرمستقیم یک شناسه آنلاین محسوب می‌شوند و در نتیجه در حوزه قوانین GDPR قرار می‌گیرند. یکی از راهکارهای ناشناس‌سازی شناسه کاربران استفاده از تابع درهم‌سازی است که شناسه کاربر را به یک رشته تبدیل می‌کند. راهکار دیگر، فراهم کردن امکان استفاده از قابلیت شناسه ناشناس است که Matomo آن را ارائه کرده است. با ناشناس‌سازی شناسه کاربری افراد با استفاده از تابع درهم‌سازی، امکان شناسایی یک کاربر خاص وجود ندارد. با این وجود، می‌توانیم اطلاعات دقیقی در مورد تعداد بازدید و شاخص‌های مرتبط با بازدیدکنندگان داشته باشیم، هرچند امکان ردیابی شناسه کاربری به داده شخصی فرد را نخواهیم داشت.

۳-۳-۵ شناسه سفارشات تجاری

شناسه سفارش، عددی است که به کالاها یا سرویس‌های خریداری شده توسط مشتریان ارجاع می‌دهد و بنابراین یک شناسه آنلاین محسوب می‌شود که در حوزه قوانین GDPR قرار می‌گیرد. Matomo این امکان را فراهم می‌کند تا این شناسه را نیز، مشابه شناسه کاربری، ناشناس‌سازی کرد.

---

[60] Mask
[61] Visitor
[62] Fingreprint
[63] metadata

۳-۳-۶ موقعیت مکانی

براساس آدرس IP یک بازدیدکننده، می‌توان موقعیت مکانی او را تشخیص داد و امروزه با کمک تکنولوژی این اطلاعات می‌تواند تا حد بسیاری زیادی دقیق باشد و حریم خصوصی افراد را با چالش مواجه سازد. برای غیرفعال سازی امکان ردیابی، Matomo به طور جدی توصیه می‌کند که فرایند ناشناس‌سازی آدرس IP صورت گیرد و این قابلیت را نیز فراهم کرده‌است. هر چه تعداد بیشتری از بایت‌ها پنهان شوند، پنهان‌سازی موقعیت مکانی به شکل بهتری صورت می‌گیرد. با پنهان‌سازی ۲ بایت از آدرس IP، شهر و ناحیه‌ای که بازدیدکننده در آنجا قرار دارد، دقیق نخواهد بود.

۳-۳-۷ نشست‌ها و نقاط کلیک

ذخیره اطلاعات نشست‌ها و همچنین نقاطی که کاربر در صفحه روی آن کلیک کرده است و یا ماوس را بر روی آن نگهداشته است در حوزه قوانین GDPR قرار می‌گیرد زیرا در برخی از موارد می‌توانند اطلاعات شخصی افراد را آشکار سازند. بر همین اساس Matomo، همه مقادیر وارد شده در یک فیلد از فرم را ناشناس می‌کند مگر اینکه کاربر آن فیلد را صراحتا در لیست سفید قرار دهد. خیلی از فیلدها نظیر شناسه کارت‌های اعتباری، شماره تلفن، ایمیل و ... باید ناشناس‌گرد