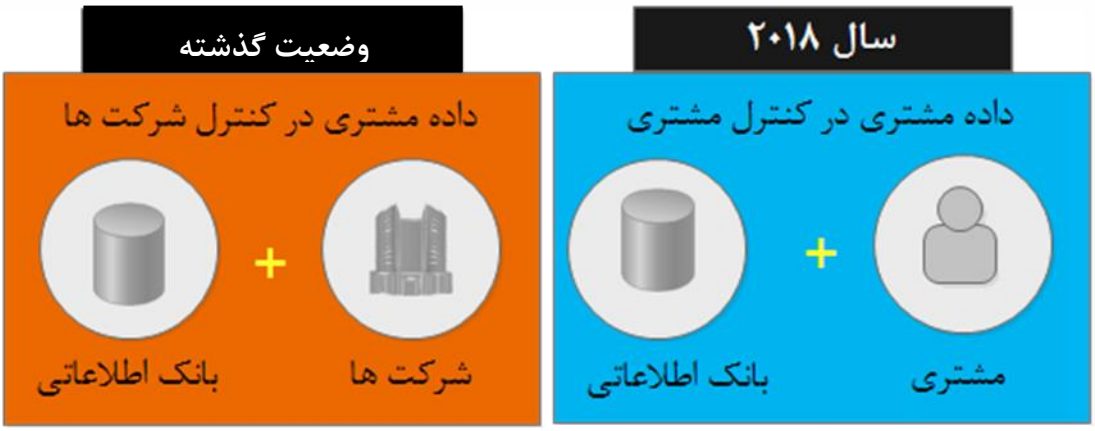
"مقررات حفاظت از داده‌های عمومی اتحادیه‌ی اروپا"

شرکت سرمایه گذاری گروه صنایع بهشهر ایران

۱. مقدمه

داده ها به سرعت در حال تبدیل شدن به شاهرگ حیاتی اقتصاد جهانی هستند . در عصر کلان داده ها و هوش مصنوعی ، داده می تواند هم به عنوان یک فرصت و هم به عنوان یک تهدید مطرح گردد . با توجه به این که داده ارایه دهنده نوع جدیدی از دارایی اقتصادی است ، می توان با مدیریت صحیح ، منسجم ، هدفمند ، یکپارچه و بکارگیری یک تفکر راهبردی آن را به یک مزیت رقابتی تبدیل کرد . عدم مدیریت مناسب داده خصوصا در مواردی نظیر حفظ حریم خصوصی و حفاظت از داده های محرمانه و حساس مشتریان ، می تواند به شهرت و اعتبار یک سازمان آسیب برساند و استمرار کسب و کار یک بنگاه اقتصادی را با چالش جدی مواجه نماید . داشتن داده دلیلی بر موفقیت نمی باشد ، مهم شیوه جمع آوری ، ذخیره سازی ، آماده سازی ، استخراج ، عملیات ، بهره برداری ، پالایش ، تولید و توزیع داده است که می تواند مسیر سیستم های بالادستی ، میانی و پایین دستی موجود در یک سازمان را برای استفاده و ایجاد ارزش هموار نماید.

علی رغم ، پیامدهای شدید مخاطرات امنیت داده ، تا همین اواخر ، جریمه نقض مقررات حفاظت از داده ها ، محدود بود و در عمل اقدامات اجرایی قابل ملاحظه ای انجام نمی شد . با معرفی قانون عمومی حفاظت از داده یا همان GDPR (برگرفته شده از General Data Protection Regulation) شاهد یک تحول بنیادین در روش های حفاظت داده مشتریان خواهیم بود و پیامد آن برای شرکت های ناسازگار با GDPR و ناقض داده ، جرایم و مجازات های سنگین خواهد بود ، که درادامه به آن اشاره خواهیم نمود.



- ✓ با توجه به تعریف کمیسیون اروپا اطلاعات شخصی هر گونه اطلاعات مربوط به یک فرد است خواه مربوط به زندگی خصوصی فرد باشد و خواه مربوط به زندگی حرفه‌ای و یا عمومی وی و آن می‌تواند هر چیزی مثل نام، عکس، آدرس ایمیل، اطلاعات بانکی، پست در وبسایت های شبکه‌های اجتماعی، اطلاعات پزشکی و یا آدرس IP یک کامپیوتر باشد.

از دیگر مزایای مهم مقررات حفاظت از داده های عمومی این است که مجموعه‌ای واحد از قوانین به تمام کشورهای عضو اتحادیه‌ی اروپا اعمال خواهد شد. هر دولت عضو یک "اداره‌ی نظارتی مستقل" برای شنیدن و بررسی شکایات، مجازات کردن جرائم اداری و غیره ایجاد خواهد کرد. این اداره در هر کشور عضو با دیگر ادارات نظارتی همکاری خواهد داشت و کمک‌های متقابلی ارائه خواهند کرد و عملیات‌های مشترکی را سازماندهی خواهند نمود.

۲. GDPR چیست؟

مقررات حفاظت داده های عمومی یا GDPR (برگرفته شده از General Data Protection Regulation) ، قانون حفاظت داده در سطح اتحادیه اروپا است که جایگزین دستورالعمل "حفاظت از اطلاعات اتحادیه اروپا" تدوین شده در سال ۱۹۹۵ شده است . 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 سازمان ها با رویکرد حریم خصوصی داده ها در سراسر اتحادیه اروپا ایجاد شده است .

۳. مقررات عمومی حفاظت از داده‌ها

شهروندان اطلاعات بیشتری در مورد این که چگونه اطلاعات و داده‌هایشان پردازش می‌شود خواهند داشت.همچنین آن‌ها حق دارند که چنانچه اطلاعاتشان هک یا افشاء گردد در اسرع وقت مطلع شوند. حق "مورد فراموشی قرار گرفتن" روشن و تقویت خواهد شد. در حال حاضر در اتحادیه‌ی اروپا، افراد تحت شرایط خاصی حق دارند که از موتورهای جستجو درخواست نمایند لینک‌هایی را که حاوی اطلاعات شخصی در خصوص آن‌ها باشد را حذف نمایند. بین این حق و حق آزادی بیان باید به درستی ارتباط برقرار شود و تعادل وجود داشته باشد.

سایر مقررات عمومی حفاظت از داده ها به شرح ذیل می باشد:

۳-۱-.برخورد با سازمان هایی که سازگار با GDPR نباشند.

جریمه های بالقوه تحت GDPR بسیار بالاتر از قوانین حفاظت از داده های موجود در کشورهای عضو اتحادیه اروپا می باشد. به عنوان مثال، تحت قانون حفاظت از اطلاعات در انگلستان، بزرگترین جریمه یک شرکت غیر سازگار در انگلستان ۵۰۰۰۰۰ پوند است . جرایم فوق در خصوص عدم سازگاری با GDPR تغییر می کند : حداکثر جریمه از ماه مه ۲۰۱۸ می تواند تا ۲۰ میلیون یورو یا ۴ درصد از گردش مالی جهانی (global turnover) باشد (هر کدام که بیشتر باشد) . این به وضوح نشان دهنده یک جهش بزرگ و چالش برانگیز است و می تواند یک تهدید جدی برای بنگاه های کسب و کار را به دنبال داشته باشد . بدیهی است که این موضوع دارای تاثیری مستقیمی بر روی استراتژی مدیریت ریسک خواهد داشت.

۳-۲-دامنه تغییرات

الزامات چشمگیر زیادی در GDPR وجود دارد ، اما تمرکز بیش تر و مهم ترین تغییرات بر روی شفافیت و حقوق بسیار گسترده برای افراد می باشد. یکی از بزرگترین تغییرات GDPR دامنه وسیعی از قوانین است که هر شرکتی که داده های شخصی اتحادیه اروپا را پردازش می کند را شامل می شود (اعم از شرکت های اتحادیه اروپا و یا شرکت های دره سیلیکون و یا سیلیکون فین انگلیس) . به طور خلاصه، اگر کارمندان ، پیمانکاران ، مشتریان یا تامین کنندگان شما شهروندان یا ساکنان اتحادیه اروپا هستند و شما داده های آنها را پردازش می کنید ، تقریبا قطعا باید سازگار با GDPR باشد و یا پذیرای عواقب آن باشید.

شفافیت بدان معنی است که بنگاه های اقتصادی کسب و کار می بایست به طور شفاف مشخص کنند که قصد آنها از جمع آوری داده های شخصی و کار با آنها چیست . اگر تاکید بر رضایت شخصی برای پردازش داده افراد است ، مردم می بایست دقیقا بدانند رضایت آنها چه مواردی را شامل شده است و دامنه تایید رضایت آنها تا کجا گسترش خواهد یافت .

۳-۳- دامنه تاثیرات

مسلما ، بیش ترین تاثیر بر روی افرادی است که دارای اطلاعاتی می باشند . بدیهی است هر اندازه که میزان اطلاعات بیش تر باشد ، افراد دارای حقوق بیش تری در خصوص شیوه استفاده از داده ها و جبران خسارات احتمالی از طرف سازمان هایی خواهند بود که ناقص قانون می شوند. با این حال، GDPR همچنین بر کسب و کارهای داخل و خارج از اتحادیه اروپا تأثیر می گذارد که می بایست آنها را رعایت کند . رهبران کسب و کار می بایست به دلیل تاثیرگذاری گسترده GDPR بر فضای کسب و کار ، به سرعت و به دقت شرایط راهبردی برخورد مناسب با آن را در سازمان خود فراهم نمایند . استراتژی و سیاست های داده می بایست در سطح مدیران ارشد سازمان تدوین گردد تا اجزاء آن به عنوان بخشی از تمامی فرآیندها از مراحل اولیه تعریف محدوده یک پروژه تا عرضه نهایی خروجی های پروژه مورد توجه قرار گیرد .

بنگاه های اقتصادی کسب و کار ممکن است نیازمند بکارگیری یک متخصص حفاظت داده یا یک DPO (برگرفته شده از Data Protection Officer) و کارشناسانی باشند که وظیفه آنها نظارت و مانیتورینگ مستمر به منظور اطمینان از انطباق با قوانین باشند .

۳-۴-محدوده عملیاتی

GDPR در ۱۱ فصل سازماندهی و شامل ۹۹ بند است . یکی از مهمترین بخش های این سند ، فصل دوم و بند پنجم است که به اصول مربوط به پردازش داده های شخصی اشاره می کند . در شکل ۱ ، به این اصول اشاره شده است .

مقررات عمومی حفاظت داده اتحادیه اروپا General Data Protection Regulation (GDPR)		
ردیف	اصل	شرح
۱	پردازش منصفانه، قانونی و شفاف	داده های شخصی باید به صورت قانونی، منصفانه و به شیوه ای شفاف در رابطه با موضوع داده پردازش شوند
۲	محدودیت هدف	داده های شخصی می بایست صرفا برای اهداف مشخص، صریح و قانونی جمع آوری شوند و نباید پردازش های بیش تری که با اهداف تعیین شده مغایر باشد بر روی آنها انجام داد
۳	به حداقل رساندن اطلاعات	داده های شخصی می بایست کافی، مرتبط و محدود به موارد مرتبط با اهداف تعیین شده برای پردازش داده باشند
۴	دقت	داده های شخصی باید دقیق باشند و در صورت لزوم می بایست به روز نگهداری شوند . در صورتی که اطلاعات شخصی نادرست باشند ، می بایست بدون تاخیر حذف و یا اصلاح شوند
۵	دوره نگهداری داده ها	داده های شخصی می بایست در قالبی نگهداری شوند که بتوان عدم ضرورت نگهداری آنها جهت پردازش با توجه به اهداف تعیین شده را شناسایی کرد
۶	امنیت داده	داده های شخصی می بایست با استفاده از اقدامات فنی و سازمانی مناسب ، به گونه ای پردازش شوند که امنیت مناسب آنها شامل حفاظت در برابر پردازش های غیر مجاز یا غیر قانونی ، از دست دادن تصادفی ، تخریب و یا آسیب تصادفی تامین گردد
۷	پاسخگویی	کنترل کننده داده مسئول انطباق با اصول حفاظت داده است و می بایست قادر به اثبات آن باشد

شکل ۱ : اصول حفاظت داده منطبق بر GDPR

۳-۵-دلایل پردازش داده‌ها

جز با رضایت شخص موضوع داده و تنها در یک یا دو موردی که او اجازه داده است نباید داده‌های شخصی پردازش شوند مگر حداقل یکی از مقدمات قانونی زیر فراهم باشد:

- ✓ برای منافع مشروع کنترل‌کننده داده یا یک شخص ثالث، مگر اینکه این منافع با منشور حقوق بنیادی اتحادیه اروپا در تعارض باشد. (به ویژه در مورد کودکان)
- ✓ برای اجرای وظیفه ای در خدمت عموم یا یک مرجع رسمی
- ✓ برای رعایت تکالیف قانونی کنترل‌کننده داده
- ✓ برای تحقق الزامان قراردادی با شخص موضوع داده
- ✓ برای ایفای تعهداتی که به واسطه درخواست شخص موضوع داده که در فرایند عقد قرارداد یا کنترل‌کننده داده قراردارد.
- ✓ برای حفاظت از منافع حیاتی شخص موضوع داده یا یک شخص دیگر

۴.الزامات GDPR: چگونه می توان خود را چنین قوانینی سازگار نمود؟

اگرچه این قانون در کشـور ما اعمال نمی شـود اما همانطور که قبلا نیز بیان کردیم افرادی که کسـب وکار بین المللی دارند باید از این قوانین تبعیت نمایند. به همین خاطر در این بخش از مقاله سعی می کنیم به طور خلاصه نحوه تطبیق سازمان با قوانین GDPR را با هم مرور کنیم:

اخذ رضایت و موافقت:

قوانین شما برای اخذ رضایت و موافقت افراد باید واضح و روشن باشد. این موضوع بدین معنی است که نمی توانید قوانین و شرایط خود را با زبان پیچیده بیان نمایید. این رضایت نامه باید به راحتی دریافت شود و کاربر هر زمان که خواست از آن خارج گردد.

اعلان نقض داده در زمان مقرر:

اگر مشکل امنیتی رخ داد، شما باید در عرض ۷۲ ساعت گزارشی از نقض داده را به مشتری و کنترل کننده داده ارسال کنید. ارسال نکردن چنین گزارش هایی در بازه زمانی تعیین شده به جریمه و تنبیه منجر خواهد شد.

حق دسترسی به داده ها:

اگر کاربران شـما پروفایل داده های فعلی خود را درخواسـت نمایند باید بتوانید این داده ها را با جزییات دقیق در اختیارشـان قرار دهید. این گزارش باید در برگیرنده روش های مختلفی باشد که شما از داده ها و اطلاعات افراد استفاده می کنید.

حق پاک کردن داده ها:

زمانیکه هدف اصلی یا استفاده از داده های مشتریان مشخص شد، مشتری می تواند از شما درخواست کند کل داده های او را پاک نمایید.

قابلیت انتقال داده:

این موضوع به کاربر اجازه می دهد به داده های خود دسترسی داشته باشد. آن ها باید بتوانند داده های خود را به دست آورند و دوباره از آن در محیط های متفاوت خارج از شرکت استفاده نمایند.

حریم شخصی با طراحی:

این بخش از GDPR شـرکت ها را ملزم می کند سـیسـتم های خود را قبل از آغاز هر کاری با پروتکل های امنیتی درسـتی طراحی نمایند. استفاده نکردن از چنین طراحی می تواند به جریمه شدن شرکت منجر شود.

مقامات بالقوه حفاظت از اطلاعات:

در برخی از موارد، شرکت شما ممکن است به مقامی برای محافظت از اطلاعات نیاز داشته باشد. این موضوع به اندازه شرکت و سطح فعالیت آن بستگی خواهد داشت.