**GDPR یا قوانین عمومی حمایت از داده‌ها**

**GDPR چیست؟**

GDPR مخفف General data protection regulation می‌باشد، GDPR در واقع قوانینی برای ایجاد کنترل بیشتر بر روی اطلاعات شخصی مردم در اتحادیه اروپا توسط شورای اروپا و پارلمان اروپا به تصویب رسیده است. هدف این مقرره این است که مقررات قانونی را برای کسب و کارها ساده‌تر کند تا از این طریق هم شهرویندادن و هم کسب و کارها در اتحادیه اروپا از عصر دیجیتال بهره لازم را ببرند.

این مقره تمام شرکت‌هایی را که با اطلاعات شخصی کاربران اتحادیه اروپا در ارتباط هستند شامل می‌شود و تضمین کننده حفاظت از اطلاعات کاربران آن‌ها است حتی اگر آن شرکت ها خارج از اتحادیه اروپا باشند ولی با اطلاعات مردم این منطقه در ارتباط باشند مشمول این مقرره خواهند بود.

حال ذیل این مقرره نه تنها شرکت‌ها موظف هستند از اطلاعات شخصی افراد که به صورت قانونی و با شرایط دقیق و سختی جمع‌آوری می‌کنند، حمایت کنند بلکه کسانی که این اطلاعات را جمع‌آوری و مدیریت می‌کنند موظف و متعهد هستند که در برابر هر نوع سو استفاده و بهره‌برداری از آن حفاظت کنند در غیر این صورت با جرایم سنگینی روبه‌رو می‌شوند.

**اهداف GDPR**

بعضی از سازمان‌ها از اطلاعاتی که جمع آوری شده است به شکل نامناسبی استفاده می‌کنند. بدون اجازه کاربر به پردازش اطلاعات سازمان می‌پردازند تا اطلاعات بیشتری درباره کاربر بدست آورند. بسیاری از اطلاعات محرمانه کاربر نیز به دلیل هک شدن سازمان‌ها به سرقت می‌روند.

این امر باعث شده است که بسیاری از کاربران اعتماد خود را به توانایی سازمان‌ها در حفظ مناسب داده‌ها از دست دهند. GDPR برای بازگرداندن اعتماد مشتری و کنترل بیشتر افراد بر داده‌های خود ایجاد شده است. این قوانین همچنین سازمان‌ها را برای محافظت از داده‌ها پاسخگو می‌سازد.

GDPR مجموعه ای از قوانین استاندارد را برای مشاغل و سازمان‌هایی که داده‌های به دست آمده از شهروندان اتحادیه اروپا به دست می‌آورند، فراهم می‌کند. این امر باعث می‌شود که سازمان‌ها به تعهدات خود پایبند باشند، زیرا آن‌ها اجازه مقابله با مقررات مختلف بسیاری از کشورهای اتحادیه اروپا را ندارند.

**چه کسانی باید به GDPR عمل کنند؟**

کلیه سازمان‌های اتحادیه اروپا باید از قوانین مندرج در GDPR پیروی کنند. این شامل مشاغل، خیریه‌ها و سازمان‌های دولتی است. سازمان‌هایی که در خارج از اتحادیه اروپا ساکن هستند اما با اطلاعات شهروندان اتحادیه اروپا کار می‌کنند نیز باید قوانین GDPR را رعایت کنند. هر سازمانی که خدمات که داده‌های شهروندان اتحادیه اروپا را اداره می‌کند باید این استانداردها را رعایت کنند. این شامل ارائه‌دهندگان ذخیره‌سازی Cloud، شرکت‎های بازاریابی ایمیل، شرکت‌های تحلیلی و غیره می‌شود.

**اصطلاحات مهم GDPR**

* **اطلاعات شخصی**

GDPR برای محافظت از اطلاعات شخصی افراد ساکن در اتحادیه اروپا طراحی شده است. OECD داده‌های شخصی را به عنوان هر گونه اطلاعات مربوط به یک فرد مشخص یا قابل شناسایی تعریف می‌کند. اطلاعات شخصی شامل نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است.

GDPR نگران اطلاعات ناشناس  که نمی‌توانند به شخصی مرتبط شوند نیست بلکه برای محافظت از اطلاعاتی که می‌توانند به یک فرد مرتبط باشند طراحی شده است. اما اگر راهی برای اتصال داده های ناشناس با فرد یا پردازش آن وجود داشته باشد، تحت پوشش GDPR قرار می‌گیرد.

* **GDPR از سه اصطلاح برای توصیف بازیکنان اصلی درگیر در هنگام دستیابی به داده‌ها استفاده می‌کند:**

**موضوع داده:** فردی است که داده‌هایش جمع آوری، پردازش، ذخیره یا به اشتراک گذاشته می‌شود. آن‌ها معمولاً مشتری، کارمند، پیمانکار یا عضو عمومی هستند که به سادگی به یک وب سایت مراجعه کرده و از آن‌ها خواسته شده است که اطلاعات شخصی خود را ارائه دهند.

**کنترل کننده داده:** سازمانی است که داده‌ها را بر اساس یک موضوع جمع آوری می‌کند. آن‌ها وظیفه دارند امنیت اطلاعات سوژه را حفظ کنند.

**پردازنده داده:**نهادی است که داده‌ها را در هر نقطه اداره می‌کند. این می‌تواند یک شرکت شخص ثالث باشد که تجزیه و تحلیل آماری را بر روی داده‌های کاربر یا یک سرویس ذخیره سازی داده مبتنی بر ابر انجام می‌دهد. سرویس‌های وب مانند MailChimp ،Google Analytics ،Shopify و Dropbox به عنوان پردازنده داده در نظر گرفته می‌شوند.

کنترلر داده پردازنده‌های داده را به طور مناسب و مطابق قوانینی که در GDPR برای کنترل داده‌های کاربر وجود دارد، انتخاب می‌کند. اگر کنترل کننده داده پردازنده داده‌ای را انتخاب کند که داده‌های کاربر را ایمن نگه ندارد، باید پاسخگو باشد.

**اصول اساسی GDPR چیست؟**

GDPR در قالب چندین اصل راهنما طراحی شده است. آنها شامل موارد زیر هستند:

**اصول محافظت از داده‌ها**

اطلاعات شخصی که توسط یک سازمان جمع آوری می‌شود باید با دقت محافظت و رسیدگی شود. کلیه داده‌ها باید به صورت قانونی، منصفانه و شفاف پردازش شوند، برای یک هدف خاص و قانونی جمع آوری شده باشد، محدود به آنچه برای یک هدف خاص لازم است، باشد، با دقت حفظ شود و به روز باشد، فقط تا زمانی که لازم است، ذخیره شود و ایمنی و محرمانه بودن آن با استفاده از فناوری‌های مناسب حفظ شود

GDPR مشخص می‌کند که سازمان‌ها باید فرایندهای مؤثری را برای حفاظت از داده‌ها توسعه دهند. این شامل استفاده از فن آوری‌های مناسب، آموزش کارمندان و ایجاد روش‌های دقیق برای محافظت از داده‌ها است.

**پردازش قانونی**

سازمان‌ها باید قبل از جمع آوری، ذخیره یا پردازش اطلاعات شخص مجوز را از فرد دریافت کنند. آن‌ها فقط می‌توانند داده های شخصی را پردازش کنند که از شخصی که داده هایش دریافت می شود مجوز داشته باشند، از داده‌ها برای محافظت از منافع فرد استفاده کنند، از داده‌ها برای منافع عمومی استفاده کنند، برای انجام یک قرارداد از داده ها استفاده کنند و تنها برای برآورده کردن منافع قانونی سازمان استفاده از اطلاعات استفاده کنند.

**گزارش نقض داده‌ها**

GDPR از سازمان‌ها می خواهد تا نسبت به نقض داده‌هایی که دارند، شفاف‌تر عمل کنند. کلیه نقض داده‌ها باید ظرف 72 ساعت از کشف به سازمان حفاظت از داده‌ها گزارش شود. همچنین اگر خطرات زیادی برای حقوق و آزادی‌های کاربر وجود داشته باشد، این سازمان باید در صورت عدم تأثیر داده‌های آن‌ها به کاربران اطلاع دهد.

**آماده سازی برای GDPR**

GDPR از تاریخ 25 مه 2018 قابل اجرا شد. پس از این تاریخ، هر مشاغل یا سازمانی که با اطلاعات شخصی شهروندان اتحادیه اروپا سر و کار دارد، باید این مقررات جدید را رعایت کند در غیر این صورت با جریمه‌های جدی روبرو می‌شود.

لازم به ذکر است، دفتر اطلاعات (ICO) یک راهنمای جامع برای GDPR و یک راهنمای 12 مرحله‌ای برای آماده سازی سازمان برای GDPR ایجاد کرده است. هر دو این منابع بسیار مفید هستند و به سازمان کمک می‌کنند تا برای تغییرات آماده شود.

**جمع بندی**:  هر چند که این مقرره برای کاربران اتحادیه اروپا و شرکت‌هایی که با اطلاعات مردم اروپا دسترسی دارند طراحی شده است با این حال به جهت کامل بودن و جامع بودن آن می‌توان از آن برای تمام کسب و کارهایی که به اطلاعات شخصی همه افراد دسترسی دارند به کار برد. این امر برای کشور ما هم ضروری است و تمامی کسب و کارها باید این موضوع را بدانند که حفظ حریم خصوصی کاربران و شفاف سازی همه امور در این زمینه به سازمان‌ها و افراد می‌تواند باعث اعتماد هر چه بیشتر کاربران به سازمان‌ها و خدماتشان شود.

منبع: [GDPR](https://gdpr.eu/)

لطفا جهت مشاوره در [انتخاب محصول امنیتی مناسب](https://softyab.com/product-category/security/antivirus/) خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های**[**اجتماعی**](https://www.instagram.com/softyab)**خودتان به اشتراک بگذارید.**