



ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

GDPR

مقدمه

شما ممکن است درباره قانونی جدید به نام General Data Protection Regulation (GDPR) یا مقررات حفاظت از اطلاعات عمومی شنیده باشید. این قانون توسط اتحادیه اروپا توسعه داده شد و در تاریخ 25 مه 2018 به اجرا در می آید. این قانون به هر سازمانی بدون توجه به جایی که آن سازمان در جهان واقع است و با اطلاعات شخصی ساکنین در اتحادیه اروپا (EU) سر و کار دارند اعمال می شود. GDPR سازمانها را ملزم به حفظ حریم خصوصی و امنیت اطلاعات شخصی ساکنین اتحادیه اروپا میکند. برای اطمینان از انطباق با GDPR، اصول کلیدی آن باید دانسته و اجرا شود.

مردم حق دارند که حریم خصوصی داشته باشند. سازمانها باید با محدود کردن جمع آوری و پردازش اطلاعات شخصی شهروندان و با محافظت از آن داده ها، به حریم خصوصی آنها احترام بگذارند. تعهدات مربوط به حریم خصوصی به اطلاعاتی مربوط میشود که به تنهایی یا با ترکیب با سایر اطلاعات می تواند فردی را که در اتحادیه اروپا زندگی می کند قابل شناسایی کند. این اطلاعات می تواند مواردی مانند آدرس، شماره گذرنامه، شماره مجوز رانندگی، جزئیات مالی، بیومتریک، عضویت اتحادیه، تاریخ پزشکی، اطلاعات مکان یا اطلاعات مربوط به گرایش جنسی، مذهبی یا سیاسی فرد باشد. این مقرر به یک «شخص» یعنی یک فرد زنده اعمال میشود. در اینجا برخی از قواعد اصلی GDPR که باید دنبال شود، آمده است:

اطلاعات شخصی افراد باید به صورت قانونی، منصفانه و به صورت شفاف مورد پردازش قرار گیرد.

به مردم باید گفته شود که چه اطلاعاتی و برای چه هدفی جمع آوری میشود.

اطلاعات شخصی باید برای اهداف مشخص، صریح و قانونی جمع آوری شود. این نباید به دلایلی دیگر باشد که با این اهداف تضاد دارد.

داده های شخصی باید تا زمانی نگهداری و پردازش شوند که برای این منظور و موارد لازم باشند و نه مدت بیشتر.

اطلاعات شخصی باید به روز و دقیق نگه داشته شوند.





افراد حق دریافت کپی از داده های خود را دارند یا می توانند درخواست کنند که اطلاعات شخصی آنها دیگر مورد استفاده قرار نگیرند و یا در برخی موارد به طور کامل حذف شوند.



سازمانها باید اقدامات امنیتی مناسب را برای محافظت از اطلاعات شخصی در برابر نابودی، از بین بردن، تغییر، یا افشای تصادفی یا غیر قانونی اجرا کنند.



علاوه بر این، سازمانها باید اطمینان حاصل کنند که تمام کارمندانی که به اطلاعات شخصی دسترسی دارند، به خوبی در نحوه محافظت از این داده ها آموزش دیده اند.

اقدامات حفاظتی که برای حفظ اطلاعات شخصی در نظر گرفته شده است، باید یک سطح حفاظت مناسب با محتوای حساس داده ها را تضمین کنند. هرچه احتمال اتفاق ناگوار در خصوص داده ها بیشتر می شود، باید تلاش و هزینه اقدامات برای محافظت از داده ها نیز افزایش یابد. این اقدامات باید به طور منظم بررسی و به روز شود. سوابق مستند شده درباره تصمیمات گرفته شده و اقدامات انجام شده برای حریم خصوصی و امنیت آنها به اثبات مطابقت سازمان با الزامات کمک خواهد کرد. علاوه بر این، سازمان ها از لحاظ قانونی مجبورند اقدامات لازم و بررسی های قانونی را برای محافظت از اطلاعات شخصی در هنگام انتقال آن به اشخاص ثالث خارجی و به ویژه کسانی که خارج از اتحادیه اروپا هستند، بکار گیرند. در نهایت، در زمان بروز رخنه به اطلاعات شخصی، سازمان ها باید ظرف 72 ساعت پس از مطلع شدن از این اتفاق، آن را گزارش کنند. کوتاهی سازمان ها برای تطبیق با GDPR می تواند جریمه تا 4 درصد از درآمد جهانی خود را منجر شود، و اینگونه GDPR یکی از مقرراتی است که میتواند خیلی گران تمام شود.

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاوره، آموزش و تست نفوذ، اطلاعات بیشتر در: www.safenet-co.net



سر دبیر مهمان

براون هونن مدیر عامل شرکت BH Consulting است که یک شرکت مستقل امنیت اطلاعات و امنیت اطلاعات در ایرلند، دوبلین است. براون به عنوان مشاور ویژه برای مرکز اطلاعات جرایم سایبری یورپول (Europol (EC3) بوده است، همچنین بنیانگذار اولین CERT ایرلند است و در هیئت مشورتی چندین شرکت امنیتی نوآور قرار دارد. برایان را در www.linkedin.com/in/brianhonan یا [Twitterbrianhonan](https://twitter.com/Twitterbrianhonan) دنبال کنید.

منابع

مروری بر GDPR برای اشخاص و سازمانها:

<http://gdprandyou.ie>

مقررات GDPR:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679>

بایگانی ترجمه های وای در ماههای قبل:

<https://www.sans.org/u/D88>

OUCH! توسط برنامه «زندگی امن» موسسه SANS تحت مجوز Creative Commons BY-NC-ND 4.0 منتشر و توزیع شده است. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. برای اطلاعات بیشتر، لطفاً با www.sans.org/security-awareness/ouch-newsletter تماس بگیرید. هیأت تحریریه: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | ترجمه شده توسط: سعید میرجلیلی، مجید هدایتی