ممکن است هنگامی که امروز صبح از خواب بیدار شده اید متوجه شده باشید که صندوق پستی و اینباکس ایمیل شما پر از ایمیل های سازمانی و کسب و کار باشد که به شما اطلاع داده اند در حال به روز رسانی خط مشی و  سیاست حریم خصوصی ( privacy policy ) هستند.

دلیل این است که امروزه  GDPR در حال اجرا بوده و اگر یک کسب و کار در این زمینه تسلیم نباشد باید منتظر جریمه های سنگین را داشته باشد. اما اهمیت GDPR برای چیست؟ چرا در دنیای امروز GDPR  اینقدر ضروری است. در این مقاله به توضیحی جامع در زمینه GDPR  و موارد استفاده از آن می پردازیم. با خواندن این مقاله در زمینه GDPR  دیگر بی نیاز از هر منبعی در از این زمینه خواهید بود. پس با [نت شهر](https://www.netshahr.com/)همراه شوید.

**GDPR چیست و چرا ضروری است؟**

 The General Data Protection Regulation یا به فارسی "مقررات حفاظت کلی اطلاعات" (GDPR) یک چهارچوب قانونی است که کسب و کارها و شرکت های اروپایی را مستلزم می کند تا از اطلاعات شخصی و حریم خصوصی شهروندان اتحادیه اروپا (EU) برای انجام معاملات در کشورهای عضو اتحادیه اروپا محافظت کند. قانون GDPR همه شرکت هایی را که اطلاعات مربوط به شهروندان اتحادیه اروپا را در اختیار دارند، مخصوصا بانک ها، شرکت های بیمه و دیگر شرکت های مالی را پوشش می دهد و این التزام را برای آن ها به ارمغان می آورد.

**دستورالعمل حفاظت از داده ها در سال 1995**

 در آوریل 2016، پارلمان اروپا GDPR را به تصویب رساند، و آن را جایگزین رهنمودهای حفاظت از داده های قدیمی خود نمود که در سال 1995 به اجرا گذاشته شده بود. مورد قبلی یک دستورالعمل بود اما GDPR یک قانون است. بر خلاف یک قانون، یک دستورالعمل اجازه می داد تا هر یک از بیست و هشت عضو اتحادیه اروپا قانون را بر اساس نیازهای خود و شهروندان تغییر داده و اجرایی کنند ، در حالی که یک قانون قابل تغییر نبوده و اتخاذ کامل آن باید صورت پذیرد. در همین راستا GDPR باید توسط تمامی 28 کشور اتحادیه اروپا به همین صورت قبول شود.

 مشکلی که این دستورالعمل داشت این است که دیگر به عصر دیجیتال امروز مربوط نیست. مقررات آن نتوانستند در مورد نحوه ذخیره، جمع آوری و انتقال داده های امروزی - عصر دیجیتال - پاسخگو باشند. همانند بسیاری از مقررات و مقررات در سراسر اتحادیه اروپا و ایالات متحده، این مقررات نمی توانستند با سرعت پیشرفت های تکنولوژیکی روبرو شوند.

**مشخصات کلی GDPR**

متن کامل GDPR شامل 99 مقاله است که حقوق افراد و تعهدات مربوط به شرکت هایی را که تحت این مقررات قرار دارند، مشخص می کند. همچنین مقررات GDPR  ملزم می کند که هرگونه اطلاعات شخصی صادر شده در خارج از اتحادیه اروپا نیز محافظت و تنظیم شود. به عبارت دیگر، اگر هر گونه اطلاعات شهروند اروپایی دستکاری شود، بهتر است که شما  GDPR را مسئول بدانید. به عنوان مثال، یک شرکت هواپیمایی ایالات متحده خدماتی را به کسی که در انگلیس است می فروشد، هرچند این شرکت در ایالات متحده واقع شده است اما همچنان مورد نیاز است که با GDPR مطابق با داده های اروپایی را بپذیرد.

 GDPR یک استاندارد بسیار بالا است و نیاز شرکت هایی است که مبالغ هنگفتی از پول را صرف می کنند تا اطمینان حاصل شود که آنها قابل اطمینان هستند. بر طبق وب سایت GDPR اتحادیه اروپا، این قانون برای "هماهنگ کردن" قوانین حریم خصوصی داده ها در سراسر اروپا طراحی شده است و حفاظت و حقوق بیشتری را برای افراد فراهم می کند.

 پیش از اینکه اینترنت بوجود آید، اروپا برای مدت طولانی مدلی ارائه کرده بود که چگونه اطلاعات ما باید محافظت و تنظیم شود. دلیل آن این است که نگرانی عمومی نسبت به حفظ حریم خصوصی در حوزه کسب و کار تحت سلطه قرار گرفته، و برای حصول اطمینان از اینکه قوانین سختگیرانه درباره نحوه استفاده از اطلاعات شخصی شهروندان از شرکت ها وجود دارد همیشه به عنوان یک عامل مهم تلقی شده و در نظر گرفته شده است.

دو روز پیش، دولت انگلیس قانون جدید حفاظت از داده ها را ایجاد کرد و آن را تصویب کرد و جایگزین قانون قبلی شد که در سال 1998 به قانون بازگردانده شده بود. این قانون در حال اجرا 353 صفحه بوده و پر از مقررات پیچیده است که عمدتا شامل همه مقررات GDPR است، اما تفاوت آن این است که کشورها نمی توانند و قادر به انتخاب بخش هایی از GDPR نیستند که می توانست بر اساس نیازهای شهروندانشان آن را تغییر دهند.

 پس از چند ماه یادگیری در مورد نقض داده ها از شرکت هایی مانند فیس بوک و Equifax، این امر می تواند ضروری تر از چیزی باشد که فکر می کنید. حتی مارک زوکربرگ در سخنرانی خود در جلسه کنگره در کاپیتول هیل، بر این باور بود که GDPR یک گام بسیار مثبت برای اینترنت است.

**چه داده هایی تحت GDPR محافظت می شود؟**

 با تصویب GDPR امروز، باید دو حامی حقوق اصلی باید برجسته شود. اول، حق پاک شدن یا حق فراموش شدن. اگر شما نمی خواهید داده هایتان خارج شود، پس شما حق دارید که برای حذف یا پاک کردن آن درخواست دهید. دوم، حق انتقال. هنگامی که به مقررات "انتخاب / در حالت اختیاری" اعمال می شود، اعلان ها برای کاربران باید بسیار روشن و دقیق بسته به شرایط آن باشد.



GDPR  دارای شرایطی واضح و قوانینی توجیهی است. بر طبق GDPR، نوع داده های زیر مورد توجه و پوشش قرار می گیرد:

 (1) اطلاعات قابل شناسایی شخصی، از جمله نام ها، آدرس ها، تاریخ تولد، شماره های تأمین اجتماعی

 (2) داده های مبتنی بر وب، از جمله مکان کاربر، آدرس IP، کوکی ها و برچسب های RFID

 (3) بهداشت (HIPAA) و داده های ژنتیکی

 (4) داده های بیومتریک

 (5) اطلاعات نژادی و / یا قومی

 (6) نظرات سیاسی

 (7) جهت گیری های جنسی و جنسیتی

**چه معیارهایی در GDPR باید برآورده شوند؟**

 همانطور که قبلا نیز ذکر شد، الزامات GDPR شامل مجموعا 99 مقاله است. هر شرکتی که اطلاعات شخصی خود را در مورد شهروندان اتحادیه اروپا در کشورهای عضو اتحادیه اروپا ذخیره و یا پردازش می کند، باید با GDPR همخوانی داشته باشد، حتی اگر آنها حضور تجاری در اتحادیه اروپا نداشته باشند.



 شرکت هایی در معرض GDPR هستند که:

 (1) در حال کسب و کار در یک کشور عضو اتحادیه اروپا هستند؛

 (2) حتی اگر در اتحادیه اروپا وجود نداشته باشد، این شرکت همچنان اطلاعات شخصی افراد ساکن اروپا را پردازش می کند؛

 (3) بیش از 250 کارمند دارند

 (4)  کمتر از 250 کارمند دارند، اگر پردازش داده ها این شرکت بر حقوق و آزادی های افراد و کاربران خود تاثیر بگذارد

**چگونه می دانید که آماده هستید؟**

 افراد و کسب و کار ها تقریبا دو سال زمان داشته اند تا از سازگار و چگونگی رعایت این قوانین و حصول اطمینان از آن را درک کنند، بنابراین نباید بهانه ای برای عدم رعایت نکردن وجود داشته باشد. اما، بیایید واقع بین باشیم، تعداد زیادی از شرکت ها به سختی یک قانون را اجرایی می کنند. امروزه تلاش بر این است که همه این تلاش ها به مصرف کنندگان جهان  منتقل شود.

**# 1 - برنامه پاسخگویی رویداد خرابی داده**

 بزرگترین نشانه آمادگی این است که برنامه ریزی داده یا طرح واکنش رویداد توسط شرکت ها اجرایی شود. در حالیکه اکثر شرکت ها نوعی برنامه ریزی را در دست دارند، باید آنها را بررسی، اصلاح و به روزرسانی موده تا اطمینان کامل از اجرایی شدن GDPR را داشته باشد.

 این تنها نیمی از نبرد است. بهتر است زمانی که یک حادثه رخ می دهد، آمادگی آن را داشته باشید. تست این طرح ها ضروری است، در غیر این صورت، اگر شما واقعا آن را ایده آل می دانید، چگونه می دانید؟ GDPR مستلزم آن است که شرکت ها در عرض 72 ساعت یا 3 روز گزارش نقض کنند. چقدر تیم پاسخگویی داده قادر به اجرای طرح و به حداقل رساندن هر گونه آسیب خواهد شد تا چه حد یک شرکت جریمه و یا جریمه خواهد شد.

**# 2- استخدام یک مامور امنیت اطلاعات (DPO)**

 GDPR شرکت ها را ملزم می کند که یک افسر حفاظت از اطلاعات (DPO) منصوب و استخدام کنند. با این حال، آن را نشانی از اینکه آیا آن را به واقع باید یک موقعیت گسسته باشد، بنابراین احتمالا، یک شرکت می تواند یک افسر که قبلا نقش مشابه را به این موقعیت، به نام آن را نشان می دهد تا زمانی که آنها می توانند محافظت از اطلاعات شخصی خود را نشان می دهد (PII)، بدون تضاد منافع. GDPR اجازه می دهد تا DPO برای چندین سازمان کار کند، حمایت از «DPO مجازی» را به عنوان یک گزینه ارائه دهد.

**# 3- ایجاد یک رکورد یا ثبت خطرهای احتمالی و مطابقت پیشرفت ها**

 در حالی که زمان برای شرکت ها در حال گذر است و زمان زیادی باقی نمانده استشرکت ها بهتر است که در طول دو سال گذشته پیشرفت های خود را بهبود ببخشند و نشان دهندۀ شناسایی تمام خطرات و اقدامات آن در تلاش برای به حداقل رساندن یا رفع این خطرات است. این ثبت یا ضبط فعالیت های پردازش ("RoPA") در ماده 30 GDPR مورد نیاز بوده و بر موجودیت برنامه های خطرناک و برنامه هایی که ممکن است عامل ریسک باشند تمرکز می کند.

 با این حال، سوال دیگری از نظر  ورود به سیستم و نحوه نگهداری آن مطرح می شود. ترس از دستکاری، تغییر، و تقلب هنوز جزو مسائل مورد توجه قرار گرفته است. در عصر بلاک چین blockchain، داشتن یک ورودی ذخیره شده که در blockchain ذخیره  شده و نمی تواند دستکاری شده یا تغییر کند، می تواند برای شرکت هایی که به سمت جلو حرکت می کنند بسیار سودمند باشد.



**چگونه GDPR بر شرکت های رسانه ای اجتماعی اثر می گذارد؟**

 شاید ذهن شما در اولین نگاه فقط به فیس بوک برود و این که چگونه GDPR، شبکه های اجتماعی را تحت تاثیر قرار می دهد. همانطور که در سخنرانی کنگره مارک زوکربرگ در کنگره کاپیتول هیل دو ماه پیش شاهد بودیم، بسیاری از شرکت های رسانه های اجتماعی و شبکه های آنلاین سیاست های حریم خصوصی و شرایط خدمات خود را بر اساس GDPR بروز رسانی کرده اند.

 پاسخ فیس بوک پس از نقض کمبریج Analytica و همچنین نگرانی های طولانی درباره جمع آوری داده های این شرکت توسط رگولاتورهای اروپا مورد بررسی دقیق قرار می گیرد. توییتر نیز به همین صورت زیر ذره بین خواهد بود اما هیچ رسوایی بزرگی هنوز آنها را در کانون توجه عمومی قرار نداده است.

**سخنگو نماینده اتحادیه اروپا**

 اگر فکر می کنید سیستم عامل های رسانه های اجتماعی از این مقررات معاف هستند، تفکرتان نیز قدیمی شده است. GDPR ملزم نموده است که شرکت های رسانه ای اجتماعی دارای یک نماینده اتحادیه اروپا باشند که بتواند برای پذیرش GDPR سازمان در اروپا پاسخگو باشد.



**پاک کردن یادداشت خصوصی**

 پس از شنیدن شهادت زوکربرگ، واضح است که کاربران باید با یک اطلاعیه امنیتی خصوصی ساده و روشن  که واقعا قابل فهم باشد ارائه شود.

**حق فراموش شدن**

 جالب خواهد بود ببینید چگونه این شرکت ها با درخواست های کاربر برای حذف اطلاعات شخصی  مقابله خواهند کرد. دیگر برای یک شرکت ایمن نیست که فرض شود مشتریان یا کاربران خود را با نگه داشتن داده های شخصی شان راضی نگه داشت، زیرا بسیاری از آن ها این موضوع را تصور نمی کنند تا زمانی که چیزی دوباره اتفاق بیفتد.

 من از وکیل اینترنتی آریزونا، آنِت بیبی پرسیدم که نظر او درباره "حق فراموش شدن"  و چگونگی تاثیر آن بر آزادی بیان ما چیست.

 وی گفت: "در اتحادیه اروپا، تحت حق نادیده گرفتن، افرادی که بازیگران بدی بودند توانستند تاریخچه و بک گراند بد خود را از انجام اشتباهات پاک کنند. با این حال، در ایالات متحده، ما آزادی بیان را به ارمغان می آوریم و این کار را با فراهم نمودن اطلاعات بیشتری برای مردم به جای آنکه آنها را پنهان کنیم به ارمغان می آوریم. مردم بر این اساس  می توانند تصمیمات آگاهانه بگیرند. من می توانم حفظ حریم خصوصی و احترام آن را درک کنم، اما من به  قانونی احترام نمی گذارم که به افراد بی پروا کمک می کند که از اشتباهات خود پنهان شوند. "



**فیس بوک و گوگل در حال حاضر با 8. 8 میلیارد دلار شکایت برای نقض قوانین GDPR دست و پنجه نرم می کنند**

 GDPR شوخی نیست  و نمی توان آن را دور زد. و امروز یک روز بزرگ برای هر کسب و کار و سازمان در جهان است. بیایید امیدوار باشیم که شرکتهایی که ما به آن ها وفادار هستیم، آن ها نیز به ما وفادار هستند.

GDPR (مقررات حفاظت کلی داده ها) در هفته گذشته در اروپا اجرایی شد. GDPR به شهروندان اتحادیه اروپا اجازه می دهد تا اطلاعات شخصی خود را بیشتر کنترل کنند، از جمله پیام هایی که از بازاریابان و صاحبان کسب و کار دریافت می کنند، و در حال حاضر در ایالات متحده آمریکا تاثیر زیادی بر آن دارد. در مورد این که چگونه رفتارهای بازاریابی کوچک و بزرگ کسب و کارهای بزرگ و بر این باورند که 4 تغییر عمده خواهد بود:

1) ایجاد فالوورها و درخواست از فالوورها برای کمک به مارک تجاری و برند خود توسط شرکت ها

2) پست ها نیاز به افزایش خلاقیت، ارزشمندی و تکنیک های بصری برای به حداکثر رساندن داغ شدن در فضای مجازی دارند

3) Micro Influencers بیشتر در تقاضا خواهند بود

4) رسانه های سنتی، تلویزیون، مجلات، روزنامه ها و رادیو نیز باید سود ببرند