ЗАЩИТА НА ЛИЧНИТЕ ДАННИ :
БРЕМЕ ИЛИ ВЪЗМОЖНОСТ ЗА ВАШИЯ БИЗНЕС?

Модерните технологии, IT иновациите, използването на клауд/облачни услуги, internet of things, директният маркетинг и проследяване на поведението на потребителите в по-малка или в по-голяма степен са част от бизнес стратегията на повечето компании и доставчици на услуги. С цел да се предостави по-добра услуга, да се предложи по-интуитивно и бързо обслужване и да се отгатнат предпочитанията на клиента, компаниите разчитат на събирането и обработването на все по-голям обем от лични данни на физически лица. Тук е мястото да направим уточнение и да дефинираме понятието „лични данни“. Това е информация, съдържаща **не само име, адрес, телефон и имейл на физическото лице, но и неговото поведение, движение в пространството, справки за реализирани покупки, използвани услуги, клиентски предпочитания, също така за здравословното и финансовото му състояние, политически възгледи, видеозаписи на лицето, и редица други**.

Именно поради широко разпространеното и често нерегламентирано и прекомерно събиране, обработване и споделяне на лични данни за физически лица Европейският съюз и Европейската комисия приеха Регламент (ЕС) 2016/679, по-известен с абревиатурата GDPR. Регламентът предвижда редица новости във връзка с режима на защита на лични данни, правата на физическите лица и дължимата отчетност и отговорността на лицата, събиращи и обработващи лични данни.

Някои от новите изисквания са:

- завишени и по-стриктно прилагани **изисквания за прозрачност, добросъвестност, законосъобразност и отчетност** при обработването на лични данни;
- засилено право на физическите лица- субекти на личните данни да бъдат информирани по всяко време за всички аспекти, действия и рискове, свързани с обработването на личните им данни; относно това кой и с каква цел събира и обработва данните им;
- за определени компании: задължение да се назначи **независимо длъжностно лице** по защита на данните, както и за извършване на нарочни **оценки на въздействието върху защитата на лични данни** на съществуващи и нови дейности, процеси, проекти и услуги, които се предлагат на клиенти;
- задължение за въвеждане на разнородни **организационни, технически и правни мерки и механизми, за да се гарантира спазването на регламента**: нови софтуерни решения и системи, разработване на правилници за поведение и вътрешни инструкции и правила,

въвеждане на ограничен достъп до бази данни (на електронен и хартиен носител), съдържащи лични данни, нови мерки за сигурност, криптиране и анонимизиране на личните данни, въвеждане на изрични срокове за изтриване на информацията, и др.

- □ задължение компаниите да работят и обменят лични данни единствено и само с други дружества, които са въвели и спазват изискванията на GDPR, в противен случай – риск от значителни имуществени санкции.

Спазването на всички тези задължения и нови изисквания е скрепено с възможността за налагане на стряскащи административни санкции в размер на 20 млн. евро или 4 % от глобалния оборот на цялата икономическата група (която сума е по-голяма), към която принадлежи българското дружество, а не просто на самото дружество. С други думи вие може да сте обект на санкции както поради порочните практики, които сами налагате, но и като част от бизнес-групата, към която принадлежите.

NB! Често пренебрегвана последица, в случай че Вашият бизнес не спазва Регламента, е загубата на настоящи и потенциални проекти и бизнес партньори, намалена конкурентоспособност и приходи. Големите и средни предприятия, които могат да понесат значителни имуществени санкции и репутационни рискове, бързат да въведат GDPR и няма да рискуват да работят с подизпълнители и съконтрахенти, които все още не са сторили това. На тяхно място те ще търсят предприятия и партньори, които могат да докажат, че са положили усилия и са въвели мерки, за да спазват новите изисквания. Както бе посочено по-горе, сключването на договори с дружества, които не отговарят на изискванията на GDPR, е основание за налагане на санкции в значителни размери и сериозен стимул за преоценка на изградените партньорства и мрежи.

В този смисъл спазването и въвеждането на конкретни мерки за привеждане дейността на компанията в съответствие с изискванията на GDPR може да изглежда като бреме за бизнеса, изискващо сериозни финансови, човешки и организационни ресурси. Такъв едностранчив поглед към GDPR обаче е контрапродуктивен и игнорира предимствата, които новите правила могат да имат за Вашия бизнес. Освен отслабване на конкурентите Ви, GDPR може да допринесе за развитието на компанията Ви в други насоки като например засилване на доверието на клиенти и партньори към вас, подобряване на репутацията, усъвършенстване на системите за сигурност и повишаване мотивацията на служителите.

- ✓ Повишаване на конкурентоспособността: неизбежно голяма част от компаниите, които използват подизпълнители и доставчици на стоки и услуги, ще бъдат принудени да заменят досегашните си с такива, които са въвели изискванията на Регламента за защита на личните данни. В този смисъл спазването на новите правила Ви гарантира сигурно предимство сред Вашите конкуренти и Ви отваря нови врати и възможности за бизнес.
- ✓ Създаване на доверие: доверието на клиенти и партньори е ключов фактор за успеха на всеки бизнес. В дигиталната ера, в която живеем, доверието е неразривно свързано със сигурността на данните, които клиенти и партньори предоставят. Спазването на GDPR създава възможност за всяка компания да увери своите настоящи и бъдещи клиенти, че полага усилия за защитата на личните им данни.
- ✓ Сигурност и прозрачност: въвеждането на организационните и техническите изисквания на GDPR ще допринесе за по-лесно и прозрачно управление на процесите във Вашата организация и по-добра защита на търговските Ви тайни и бази данни.
- ✓ Подобряване на корпоративната култура и мотивацията на служители чрез въвеждането и спазването на ясни правила за обработка на личните им данни, отчетност и сигурност на информацията им.

Макар датата на влизане в сила на Общия регламент за защита на личните данни да е съвсем близо, все още не е късно да се предприемат необходими мерки, за да може всеки да се възползва от бизнес предимствата, които Регламентът предлага. По данни на КЗЛД, проучванията показват, че около 80% от компаниите в България не са подготвени да реагират на въвеждането на Общия регламент за защита на данните[1].

Как да постигнете съответствие с новите изисквания:

Не съществува единна формула или алгоритъм от действия, които да Ви гарантират, че при прилагането им, ще отговорите автоматично на изискванията на Регламента и ще се предпазите от имуществени санкции. Действията по привеждане на дейността Ви в съответствие с изискванията в областта на защитата на лични данни зависят до голяма степен от вида и начина, по който обработване лични данни, от законодателството, което регулира Вашата дейност, от вътрешната организация и работни процеси, както и от редица други индивидуални характеристики и особености. **Във всеки случай обаче водещо е да можете да демонстрирате, че сте положи необходимите и разумно очаквани усилия да постигнете съответствие, че сте анализирали в каква степен спазвате правилата на Регламента и сте определили мерки, които допълнително да предприемете**. Регламентът не изисква постигането на безусловна и абсолютна степен на защита на информацията, обработвана от предприятието Ви (която степен едва ли би могла да бъде постигната), но държи сметка за разумно очакваните и положените усилия и реално предприети мерки и действия за тази цел.

Националният регулатор - Комисията за защита на личните данни, е предложила списък с 10 практически стъпки за прилагане на Регламента[2], а именно:

1. Запознаване с новите нормативни изисквания в областта на защитата на личните данни - **определяне на служители или екип, които да отговарят за привеждане на дейността на дружеството или организацията в съответствие** с новите нормативни изисквания в областта на защитата на личните данни.

2. **Извършване на вътрешен анализ на дейностите по обработване на лични данни** – кой, защо и за какъв срок работи с лични данни на физически лица, предоставя ли се достъп до тях на външни лица и институции, какви мерки за сигурност се използват при този трансфер. В тази връзка често се изготвя **т.нар. GAP анализ**, чиято цел е да идентифицира всички обстоятелства и процеси по обработване на лични данни, дали това обработване е законосъобразно в светлината на новите правила и да посочи „пролуките“ *(оттам и употребата на термина GAP – от англ. език – „дупка“, „пролука“),* за отстраняването на които е необходимо да бъдат предприети допълнителни действия и мерки.

3. Преценка дали е налице задължение да се **определи Длъжностно лице по защита на данните**, съответно назначаването на такова лице. Тук е важно да отбележим, че все още на Европейско ниво липсва приет единен стандарт за обучение на такива лица.

4. **Управление на риска** по отношение на защитата на личните данни – идентифициране на възможните **проблемни зони, които са свързани със завишен риск от неправомерна обработка на лични данни**, напр. сривове в системите, в които се съхраняват, осъществяване на неправомерно човешко въздействие – предоставяне на данните на трети лица, използването им по непозволен начин и за лични цели, и др. Целта на тази четвърта стъпка е, в случай че се установи съществуването на висок риск, да се набележат подходящи мерки, които адресират и намаляват този риск. При необходимост следва да се проведат и **задължителни предварителни консултации с КЗЛД**.

5. **Приемане на план за действие** – независимо дали рискът от неправомерно и незаконосъобразно обработване на личните данни е висок или нисък, всяко предприятие следва да разпише план за действие за привеждане на дейността си в съответствие с новите

[1] Информационен бюлетин на КЗЛД, брой 1 (70), януари 2018 г.
[2] https://www.cpdp.bg/index.php?p=element&aid=1110

правила. По този начин най-малкото ще бъде в състояние докаже, че е положило необходимите усилия и ще намали възможността за носене на административно-наказателна и имуществена отговорност.

6. Документиране и отчетност – Тази стъпка включва: 1) създаване и редовно актуализиране на **вътрешен регистър на дейностите** по обработване на лични данни в дружеството (не е задължително за организации с до 250 наети служители и работници на трудов или граждански договор); 2) **описване на предприетите мерки** за защита на личните данни; 3) **наличието на вътрешни правилници и актуализирани бланки и договорни** клаузи в светлината на новите правила;

7. Преглед на **правните основания за обработване на лични данни**, включително въз основа на съгласие на лицата – следва да се извърши внимателна **преценка дали администраторът на лични данни действително има легитимно основание да изисква и да обработва данните** на физически лица, както прави към настоящия момент; дали не е необходимо да ограничи обработката на данни или да престане да използва декларации за съгласие от физическото лице, понеже съгласието му не е информирано или свободно дадено, по смисъла на новия Регламент. Така например изрично се приема, че работодателят няма право да събира лични данни за своите служители на база тяхното съгласие (тъй като същото не е свободно дадено) и следва да се преустанови практиката за включването на такива клаузи или декларации при наемане на работа.

8. **Информираност на субектите на данните** и **прозрачност** на обработването – Регламентът, а и Директивата преди него, изискват преди личните данни да се съберат от лицето, на последното да бъде **предоставяна обобщена, кратка и разбираема информация** за целите и начина на обработка, за субекта, който ще обработва данните му, за какъв срок, пред кого може да подаде жалба в случай на нарушения, и др. Работодателите трябва например да информират по подходящ начин работниците си, ако извършват видеонаблюдение на работното място или на електронната им комуникация. Организациите, притежаващи лична интернет страница или мобилно приложение, следва да публикуват политиката си за защита на личните данни отново по ясен и разбираем начин, в структуриран вид с подзаглавия, картинни изображения и схеми, създаващи яснота.

9. **Практическо упражняване на права от субектите на данните** – в изпълнение на тази стъпка организациите трябва да въведат мерки (технически, организационни и др.), **за да обезпечат възможността за упражняване на правата, които Регламентът признава на физическите лица**, чиито данни се обработват. Така например всяко дружество следва да разработи вътрешна процедура, чрез която в рамките на до 1 месец при поискване от физическото лице да идентифицира всяка лична информация, която има за това лице (на сървър, свалена на мобилно устройство на свой служител, на хартиен носител или в софтуерна система), и да му я предостави в ясен и структуриран вид.

10. **Уведомяване за нарушение на сигурността на личните данни** – задължително е за всяко предприятие да приеме вътрешна процедура и план за действие в случай на нарушение на сигурността на личните данни (например пробив в системата, или изтичането на лични данни поради човешка грешка или злонамерено действие); да се определи отговорен служител, да се провежда инструктаж на персонала, и при нарушение – да се уведоми в рамките на до 72 ч. КЗЛД.

Лена Бориславова

Адвокат „Герогиев, Тодоров и Ко.“,

LLM Harvard law school