Адвокатско дружество "Горанова & Христова-Аличкова"

www.gaplaw.eu
гр. София 1309
ул. "Царибродска" №94
ет. 3, офис 5
office@gaplaw.eu

януари 2018 г.

На вниманието на

Управител

Ръководен мениджмънт

ИНФОРМАЦИОННО ПИСМО ПО ПРИЛАГАНЕ НА РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ФИЗИЧЕСКИ ЛИЦА

Уважаеми Дами и Господа,

Във връзка с предстоящото започване на прякото прилагане от 25.05.2018 г. на РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО - **Общ регламент относно защитата на данните** (наричан по – долу за краткост „*Регламент*"), бихме искали да обърнем внимание върху някои от по-съществените задължения за администраторите и обработващите лични данни, които произтичат от неговото приложение. Изложеното не изчерпва действията, които новият Регламент изисква да бъдат предприети или редовно предприемани за осигуряване на законосъобразната обработка на лични данни след 25.05.2018 г., за което екипът ни е готов да Ви окаже индивидуално, навременно, компетентно и детайлно допълнително съдействие.

Важно е да се отбележи, че поради особено голямата значимост на Регламента, размерът на предвидените санкции за нарушения е изключително завишен и е един от най-високите в българската административно-наказателна практика – съгласно Регламента санкциите се определят в порядък до 10 или 20 млн. евро или 2% / 4% от оборота за предходната финансова година (която от двете суми е по-висока), като за всяко нарушение се налага отделна санкция, но има ограничение на максималния размер на кумулираните санкции. Все още няма яснота за това какъв ще бъде подходът на българската Комисия по защита на личните данни в хода на проверките за изпълнение на задълженията по Регламента и дали ще приеме методика и критерии за налагане на конкретен размер на санкциите. Независимо от това е ясно, че материята е от изключителна важност и очакваме, че изпълнението на Регламента ще се следи, за разлика от формалния подход на българската администрация до момента, когато изпълнението на задълженията на администратора да се регистрира в КЗЛД и да осигури писмено съгласие на служителите си за обработка на лични данни общо взето изчерпваше на практика неговите активности по отношение изпълнението на Закона за защита на личните данни.

НОВА УРЕДБА В РЕГЛАМЕНТА ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ. АНАЛИЗ

Регламентът е акт, който се прилага пряко и непосредствено на територията на всяка държава членка на ЕС без да е необходимо неговите разпоредби да бъдат допълнително възпроизведени в друг вътрешен акт, т.е. не е необходимо да се чака приемането на нов български закон за личните данни или друг подобен акт, както и ако не бъде приет такъв това не освобождава администраторите от задълженията им, произтичащи от регламента. Регламентът започва да се прилага от **25.05.2018 г.**, което означава, че всеки, който във връзка със своята дейност събира, обработва и съхранява лични данни на физически лица на територията на ЕС, следва до тази дата да отговаря на въведените с него нови изисквания.

С новия Регламент се въвеждат редица промени в законодателството във връзка със защитата на личните данни, които администраторите на лични данни събират, съхраняват или по друг начин обработват лични данни, предоставени им от физически лица, наричани в Регламента „субекти на

www.gaplaw.eu
гр. София 1309
ул. "Царибродска" №94
ет. 3, офис 5
office@gaplaw.eu

данни". Разширяват се правата на т. нар. субекти на данните и се увеличават задълженията към администраторите на личните данни. Нововъведенията са най – общо следните:

1. **Отпада общото задължение за уведомяване на надзорния орган за обработване на данни, конкретно при нас Комисия за защита на личните данни** (задължението отпада след 25.05.2018 г., до тогава подлежи на изпълнение на основание законовата норма на чл. 17 от Закона за защита на личните данни (ЗЗЛД)).
2. **Определението за лични данни** се разширява в сравнение с това, което е въведено със ЗЗЛД, а именно то гласи, че това е „***всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано***", независимо дали то се идентифицира пряко или непряко с име, местоположение, поведение в онлайн пространството (т.нар. „бисквитки") или по други начини и признаци. **Следва да се прилага и съобразява дефиницията, дадена в Регламента!**
3. **Относно съгласието на субекта на данните** – Регламентът поставя повишени изисквания за съгласието на субекта на данните, което следва да е свободно дадено, конкретно, информирано и недвусмислено за обработване на свързани с него лични данни, например чрез писмена декларация, включително по електронен път. Регламентът съдържа много специфично разбиране кога е налице съгласие, кога се приема, че то е дадено свободно и кога не, кога е информирано, допустимо и необходимо ли е администраторът да изисква „съгласие" на субекта на данните като условие за сключване на договор с него или предоставяне на услуга, и др., на които въпроси бихме могли да отговорим конкретно при запитвания от Вас и след като съобразим естеството на дейността Ви, на конкретния договор или услуга, за да се прецени дали конкретният подход не е в противоречие с новия Регламент.

   Когато обработването се извършва въз основа на съгласието на субекта на данните, **администраторът следва да може да докаже, че субектът на данните е дал съгласието си за конкретната операция по обработване.** По-специално, в случай на писмена декларация конкретно, точно и ясно трябва да е описано по недвусмислен начин, че субектът на данни е информиран с каква цел се събират личните му данни, какви точно данни се събират, за какъв период от време, т.е. в каква степен и за какво дава съгласието си.

   Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни следва да бъде информиран за правото да го оттегли. Оттеглянето на съгласие трябва да бъде също толкова лесно, колкото и даването му, като администраторът е длъжен да осигури възможността оттеглянето да бъде извършено по същия начин, по който е дадено съгласието, т.е. да не му се създават неоснователни затруднения.

   Регламентът съдържа специфични изисквания при даването на съгласие за обработване на „специални категории лични данни" и лични данни на деца.

   Съгласие, което е дадено в нарушение на изискванията на Регламента следва да се счита за не обвързващо и съответно не би могло да осигури надлежно правно основание за обработване на лични данни.
4. **Права на субектите на данни** – Регламентът запазва и разширява правата на субектите на данните. Посочваме ги в това писмо, тъй като правата на субекта на данни кореспондират с **насрещните задължения на администраторите на данни** да ги осигурят и да могат при проверка да докажат, че са ги осигурили, напр. като публикуват съответните формуляри на интернет страницата си или изрично уведомяват субекта на данни за тези му права, както и за механизма за упражняването им, включително с данни за контакт със самия администратор и то на лесен и разбираем език.

www.gaplaw.eu
гр. София 1309
ул. "Цариградска" №94
ет. 3, офис 5
office@gaplaw.eu

4.1. Право на достъп – Субектът на данни има право да получи от администратора потвърждение дали негови лични данни се обработват и ако това е така да получи достъп до (копие от) обработваните лични данни. Това включва и предоставянето на допълнителна информация, чието съдържание е сходно с това на предварителната информация, което администраторът е следвало да представи на субекта преди започването на обработването на лични данни. Правото на достъп позволява на субектите на данни да проверяват коректността на данните и законосъобразността на тяхното обработване. То е и предпоставка за упражняване на другите права на субекта на данни;

4.2. Правото на коригиране - Субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването субектът на данните има право непълните му лични данни да бъдат попълнени или актуализирани;

4.3. Право на възражение - Субектът на данните има право да възрази срещу обработване на личните му данни. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват други, законови основания за обработването**. Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възражение срещу обработване на лични данни, отнасящо се до него за този вид маркетинг**, което включва и профилиране, доколкото то е свързано с директния маркетинг. Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява;

4.4. Право на изтриване (право „да бъдеш забравен“) - Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни, когато обработването им вече не е необходимо, съгласието за обработката им е оттеглено/подадено е възражение или данните са обработвани незаконосъобразно.

В тази връзка администраторът на лични данни, който по някаква причина ги е разпространил и направил достъпни на трети лица, има задължение да уведоми всички, разполагащи с данните да изтрият всякакви връзки между тези лични данни, техни копия или реплики;

4.5. Право на ограничаване на обработването – Субектът на данните има право да изиска от администратора ограничаване на обработването в определените в Регламента хипотези, а администраторът е длъжен да му осигури такава възможност;

4.6. Право на преносимост на данните – Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратора, в структуриран, широко използван и пригоден за машинно четене формат и има правото да ги прехвърли на друг администратор, без да търпи негативни последици от това. Правото на преносимост се осъществява, доколкото обработването се извършва с автоматизирани средства на основание на дадено от субекта на данните съгласие. Когато това е технически възможно, правото на преносимост се осъществява чрез прехвърляне на данните директно от един администратор на друг.

Субектите на данни имат право на защита по съдебен или административен ред, в случай че правата им са нарушени.

5. <u>Промени, свързани с отговорността и задълженията на администраторите на лични данни -</u> Регламентът предвижда засилване на отговорността и задълженията на администраторите на лични данни:

5.1. Личните данни следва да бъдат **обработвани** по начин, който гарантира подходящо **ниво на сигурност, включително защита** срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки и тяхното документиране. Според Регламента може да се приеме за

www.gaplaw.eu
гр. София 1309
ул. "Царибродска" №94
ет. 3, офис 5
office@gaplaw.eu

подходяща някоя от следните мерки или техни комбинации, като във всеки конкретен случай следва да се подхожда и преценява индивидуално:

а) псевдонимизация и криптиране;

б) свеждане на данните до минимум;

в) ограничаване на броя на лицата, които имат достъп на данните;

г) гарантиране на постоянна поверителност; цялостност, наличност и устойчивост на системите и услугите за обработване;

д) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на инцидент, както и редовно изпитване и оценка на предприетите мерки.

5.2. Задължение за уведомяване на КЗЛД за нарушение на сигурността на личните данни, както и на лицето, чиито данни са засегнати - В случай на нарушение на сигурността на личните данни администраторът незабавно, но не по-късно от 72 часа след като е разбрал за него, уведомява КЗЛД и субекта на данните. **Субектът на данните може да не се уведомява,** когато се приема, че за него не съществува вероятност нарушението на сигурността на личните данни да породи риск - например когато администраторът е направил личните данни технически „неразбираеми", например чрез криптиране. Уведомлението до надзорния орган има **задължително необходимо съдържание**. Независимо от задълженията за уведомяване, администраторът е длъжен да документира всяко нарушение на сигурността на личните данни, включително обстоятелствата във връзка с нарушението, последиците от него и предприетите мерки.

5.3. Администраторът на лични данни следва да предвиди ред и условия за улесняване на упражняването на правата на субектите на данни съгласно Регламента, включително механизми за искане, и ако е приложимо — безплатно получаване **на достъп до, коригиране или изтриване на лични данни и упражняване на правото на възражение**. Администраторът има задължение да предостави и средства за подаване на искания по електронен път, особено когато личните данни се обработват електронно. Администраторът е длъжен да отговоря на исканията на субекта на данни без ненужно забавяне и най-късно в рамките на един месец, както и да посочи причините ако не възнамерява да се съобрази с тези искания.

Администраторът следва да информира субекта на данни дали е задължен да предостави личните данни и за последствията, в случай че не ги предостави на трети лица, например банки (за превод на трудово възнаграждение), Служби по трудова медицина, съдебни и съдебно – изпълнителни органи, полицейски органи и други.

5.4. Длъжностно лице по защита на данните – Считаме за важно администраторите да обърнат специално внимание на фигурата на длъжностно лице по защита на данните, включително:

- кога назначаването му е задължително и кога е въпрос на преценка на администратора – напр. задължително е когато администраторът извършва т.нар. мащабна обработка на данни (преценява се според дейността му за всеки конкретен случай), като за „мащабна" за целите на Регламента се счита например обработката на данни, извършвана от банки, застрахователни дружества, болници и др., а като „не мащабна" би могла да се приеме дейността на лекар на индивидуална практика, самостоятелно зает адвокат и т.н. – необходима е преценка за всеки конкретен случай;
- възможно ли е няколко дружества да ползват едно и също лице по защита на данните;
- ако работодателят реши да назначи свой служител за такова длъжностно лице по защита на данните какви специфични, допълнителни изисквания към трудовите му функции (напр. длъжностна характеристика, йерархична зависимост) трябва да се предвидят, има ли и каква допълнителна защита срещу уволнение на тези лица, каква отговорност носят, данните за

www.gaplaw.eu
гр. София 1309
ул. "Царибродска" №94
ет. 3, офис 5
office@gaplaw.eu

контакт на това лице на кои други лица следва да се съобщават и как да се документира това съобщаване и др.

Длъжностното лице по защита на данните може да е служител на дружеството или външно лице (физическо или юридическо), ангажирано по договор за услуга. Това лице следва да притежава необходимите познания на нормативната уредба в областта, както и умения, за да заема такава позиция, респективно за да извършва такава дейност (няма изисквания за специфично образование).

5.5. Администратор на лични данни и обработващ лични данни: Не винаги администраторът и обработващият лични данни са едно и също лице, като администратора има право да възлага тази дейност на други лица с договор. В случай, че администраторът използва трето лице - обработващ лични данни, което събира от негово име лични данни, следва да се увери, че обработващият е актуализирал документите и процедурите си във връзка с възложеното му предоставяне или събиране на информация за субектите на данни. Обработващият лични данни е задължен да спазва всички установени правила и норми за защита на личните данни, като администраторът и носи солидарна отговорност за причинени вреди заедно с обработващия, както и за неоторизиран достъп до лични данни. За това е важно в договорите с обработващите лични данни ясно и детайлно да се посочат правата, задълженията и отговорностите и на двете страни. Едно от основните задължения на администраторите и обработващите лични данни е да бъдат в състояние да докажат, че дейностите по обработването, включително ефективността на предприетите мерки, са в съответствие с Регламента, като се вземат предвид естеството, обхвата, контекста и целите на обработването от една страна, както и риска за правата и свободите на субектите на данни, от друга. Принципът на отчетност, залегнал в Регламента изисква във всички случаи, администраторът и обработващият лични данни да поддържат документация за дейностите по обработване, за които са отговорни. Тази документация при поискване следва да бъде предоставяна на КЗЛД.

5.6. Транфер на лични данни между различни държави – Регламентът разширява териториалният обхват на европейските правила за защита на личните данни и те ще важат и за администратори, които не са установени в ЕС, но обработват лични данни на физически лица, които се намират в ЕС. Регламентът въвежда задължение за дружества, намиращи се извън ЕС, които системно, а не случайно, обработват данни на субекти на ЕС и дейностите по обработването са свързани с предлагане на стоки и услуги, да посочат **свой представител на територията на ЕС**. Центровете за данни (вкл. call center) и доставчиците на „облачни" услуги, които съхраняват лични данни на физически лица от ЕС са част от случаите, свързани с такива дейности.

6. КАКВО Е ПРЕПОРЪЧИТЕЛНО ДА НАПРАВИ АДМИНИСТРАТОРЪТ ДО 25.05.2018 г., ЗА ДА ПРИВЕДЕ ДЕЙНОСТТА СИ В СЪОТВЕТСТВИЕ С ПРОМЕНИТЕ?

Експертите по защита на личните данни в адвокатското ни дружество биха могли да Ви бъдат полезни в следните дейности, които според нас е необходимо да извършите, за да приведете дейността си в съответствие с новите изисквания на Регламента:

6.1. Одит и ревизия на съдържанието на създадената документация – заявление, регистри, процедури, инструкции и др., преглед на договори с доставчици и партньори, със Служба по трудова медицина, рекламни агенции, агенции за подбор на персонал, маркетингови агенции, счетоводни къщи, на които възлагате да обработват възнагражденията и/или болнични листове на персонала ви и други подобни, по повод на които се събират, обработват и/или съхраняват лични данни на физически лица, включително договорите ви с IT компании, които извършват софтуерна поддръжка / внедряване на вашите програмни продукти, поддръжка на сървъри,

www.gaplaw.eu
гр. София 1309
ул. "Царибродска" №94
ет. 3, офис 5
office@gaplaw.eu

осигуряване на защити от неоторизиран достъп и др. Съвместно с IT компаниите е необходимо да проведете анализ на IT инфраструктурата и да се предприемат действия относно подобряване на защитата на софтуера, с който се обработват лични данни, респективно предприемане на мерки за невъзможност за персонализиране на тези данни при неоторизирано проникване в системата.

6.2. Редактиране на съществуващите документи с цел привеждането им в съответствие с новите изисквания, въведени с Регламента, както и приемане на нови документи - срокът за това е до **25.05.2018** г. Препоръчително е това да стане по – рано, за да може екипът, работещ по проекта, включително от страна на клиента, да има достатъчно време да реагира в отношенията си с контрагенти и други. Администраторът има задължение да изготви и поддържа: регистри на дейностите по обработване, кодекси за поведение, препоръчително е да заложи определено ниво на сигурност в основата на бъдещи внедрявания и разработки.

6.3. Определяне на длъжностно **лице по защита на данните –** когато е задължително според Регламента или по преценка на администратора.

6.4. Заключителен одит: проверка за правилна имплементация на изискванията на Регламента.

6.5. Продължаваща дейност: *Няма стандартно и универсално средство, което да направи една компания „в съответствие" с Регламента. Това винаги ще бъде предмет на конкретна оценка на конкретните процеси на компанията и идентифициране на рисковете.*

Това представляват най – общо положенията на Регламента и новите задължения за администраторите и обработващите лични данни, които той предвижда.

За да можем конкретно да Ви бъдем полезни в привеждане на Вашите документи и дейност в съответствие с Регламента, както и да дадем съвети за това дали в онлайн проектите Ви изпълнявате новите изисквания, следва да се свържете с нас, като ни изпратите имейл на адрес: office@gaplaw.eu и оставите Вашите координати, за да могат нашите експерти да се свържат с Вас или да потърсите съдействие директно от адвоката – съдружник, който отговаря за връзката с Вас.

Бихме искали да изтъкнем, че гаранция за успешно сътрудничество помежду ни при съобразяването на Вашата дейност с новите изисквания на Регламента, е да работим в екип, в тясното сътрудничество и взаимодействие с Вашите служители от различни звена (човешки ресурси, онлайн продажби и т.н.), а понякога и с Вашите партньори (трети лица, на които сте възложили обработването на данни и др.). От изключително и основно значение за нас е съвместната работа с Вашите IT специалисти, които следва да извършат одита и оценката на прилаганите от Вас технически мерки за сигурност и които единствени са компетентни да предложат конкретни технически / технологични (напр. софтуерни, хардуерни или др.) мерки за привеждане на дейността Ви от техническа гл.т. в съответствие с изискванията на Регламента.

Настоящото становище представлява предварителен кратък правен анализ на Регламента. Становището не представлява конкретен правен съвет или консултация. Такъв може да бъде даден след извършване на одит и запознаване със съществуващите документи и Вашата дейност, свързана със събиране, обработка и съхраняване на лични данни на физически лица.

С уважение,

Екипът на Адвокатско дружество **„Горанова и Христова – Аличкова"**