ПРОМЕНИ В УРЕДБАТА НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ С РЕГЛАМЕНТ (ЕС) 2016/679 (ОРЗД/GDPR), ПРИЛОЖИМИ ОТ 25 МАЙ 2018Г.

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 – ОРЗД/GDPR) - новите изисквания и санкции в областта на защитата на лични данни, свързаните с тях проблеми и техните правни и технически решения

Настоящото изложение има за цел да систематизира и обобщи основните положения, застъпени в GDPR, отнасящи се до:

- понятието лични данни и какъв тип информация включва то;
- правата на лицата, чиито лични данни биват събирани и обработвани;
- правата и задълженията на администраторите на лични данни, съответно – на обработващите лични данни;
- правни и технически решения, които да осигурят съвместимост с изискванията, предвидени в Регламента;
- установените санкции във връзка с нарушаване или неизпълнение разпоредбите на Регламента и стъпките, които следва да бъдат предприети с оглед избягването им.

GDPR е публикуван в Официален вестник на Европейския съюз на 4 май 2016 г. **Регламентът влиза в сила <u>на 25 май 2018 г.</u>**, като същият има пряко и непосредствено приложение, което означава, че за да се прилагат предвидените в него правила, съответно – да бъдат налагани предвидените санкции не е нужен какъвто и да е нормативен акт на вътрешното право на държавите-членки. Съобразяването на изискванията на GDPR в дейността на администраторите на лични данни и на обработващите лични данни ще бъде свързано с големите промени и изпълнение на значително завишените изисквания, които същият предвижда, т.е. казано накратко – **до 25.05.2018 г. всяко лице, което попада в обхвата на GDPR следва да е съобразило изискванията на същия, като в противен случай би могло да понесе санкция в размер до 20 милиона евро или до 4% от общия си годишен оборот.**

Макар на пръв поглед реформата в европейскоправния режим на защитата на личните данни да е стряскаща за бизнеса, мащабните цели, които тя си поставя са, от една страна – осигуряване на по-сериозна защита на личните данни на гражданите в условията на автоматизация и дигитализация, и от друга – осигуряване на благоприятна трансевропейска бизнес среда за малките и средни предприятия, които занапред ще съобразяват поведението си с единните законодателни решения, а не с 28 вътрешни правни системи.

ТЕРИТОРИАЛЕН И МАТЕРИАЛЕН ОБХВАТ НА GDPR

Кой ще бъде засегнат от новите изисквания?

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

GDPR значително разширява териториалния обхват на приложимост на правилата на правото на Европейския съюз в областта на защитата на личните данни. Регламентът ще засегне не само **организации, ситуирани в държавите – членки на Европейския съюз**, но и такива, **чиито седалища се намират в трети страни**, но същите в дейността си обработват лични данни на граждани на страни-членки на Европейския съюз. Последните ще са длъжни да прилагат правилата на Регламента, когато дейностите по обработване на данни от тях са свързани с предлагането на стоки и услуги на физически лица, намиращи се на територията на Европейския съюз (като наличието на задължение за плащане от субекта е ирелевантно) или с наблюдението на тяхното поведение, в случаите, в които това поведение се проявява в рамките на съюза.

При изследване на обхвата на Регламента първият важен въпрос, който следва да бъде обсъден е какво всъщност попада в понятието лични данни. Чл. 4, §1 от Регламента гласи: „лични данни" означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;"

По същество, при определяне на понятието, разлика с досегашната уредба няма.

Следващият изключително важен отговор, който следва да бъде даден е кога, т.е. по отношение на какви действия, извършвани в ежедневната работа на дружествата, възниква задължението за съблюдаване на изискванията на Регламента, или иначе казано - кога едно лице „обработва" лични данни.

Най-общо казано - с тези изисквания ще бъдат засегнати всички видове структури, които имат досег до лични данни, включително на работници и служители, клиенти, партньори-физически лица, пациенти и др. В обхвата на Регламента попадат както частните фирми, така и държавните органи, нестопанските и неправителствените организации, които имат един или повече служители.

В тази връзка, следва да се посочи, че GDPR определя материалния си обхват доста общо. В чл. 2, §1 е казано: *„Настоящият регламент се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват регистър с лични данни".*

На първо място, за точното тълкуване на цитираната разпоредба следва да бъде обяснено какво влага европейският законодател в понятието „обработване" на лични данни. Чл. 4, т.2 дава следните примери *„събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване"* /посочени в английския текст на регламента като: *„collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise*

гр. София, бул. „Витоша" № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

making available, alignment or combination, restriction, erasure or destruction“/. Това изброяване, обаче не покрива всички случаи, при които следва да бъде прието, че е налице обработване на лични данни. Такова ще се приеме, че има и във всеки друг случай, при който се извършват „операции“ с лични данни с автоматични или други средства.
От разпоредбата на чл. 2, §1 GDPR следва, че той се прилага във всеки случай, когато е налице обработване на лични данни с автоматични средства. Когато обработването се извършва чрез други, различни от автоматичните средства, правилата на Регламента ще намерят приложение, когато обработваните лични данни са част от регистър или са предназначени да бъдат включени в такъв. Поредният въпрос, който възниква, е какво стои зад понятието „регистър“. Съгласно легалното определение „регистър с лични данни“ („filing system“) е „всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип“. Регистърът може да бъде както автоматизиран (например компютърна база данни), така и на хартиен носител (например ведомости за заплати или други систематизирани служебни документи, които работодателят е длъжен да съхранява).
В заключение, следва да бъде направен извод за изключителна широта на приложното поле на GDPR, както в териториално отношение, така и по отношение на дейностите, които ще бъдат предмет на регулация от Регламента.

ОСНОВНИ ЦЕЛИ НА GDPR

Какво наложи извършването на реформа на Европейската правна рамка на защитата на личните данни?

Основна цел на новото законодателство, въведено с **GDPR** е да бъде осигурена и гарантирана **по-добра и ефективна защита на неприкосновеността на личния живот**, като същевременно, съобразявайки динамиката на влиянието на технологиите в съвременното общество, ще се открият нови възможности за развитие на трансевропейска стопанска дейност . Европейската комисия сочи, че единното законодателство в областта на защитата на лични данни ще спести на бизнеса 2,3 милиарда годишно .
Както бе посочено, основна цел на GDPR е именно осигуряване на ефективна защита на „субектите“, както Регламентът нарича гражданите, чиито лични данни биват обработвани. Защитата на личните данни е едно от основните права, гарантирано с Хартата на основните права на Европейския съюз и Договора за функциониране на ЕС. Освен това Комисията взе предвид и че субектите на лични данни са неограничен кръг от лица, поради което Регламентът урежда значително завишени критерии по отношение на това как същите ще бъдат получавани и обработвани, като се предвиждат и значително завишени санкции за субектите, на които се възлага съблюдаване на посочените изискванията.

ОСНОВНИ ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Глава II от GDPR урежда основните принципи, при които следва да бъде извършвано обработването на лични данни. Посочването на същите е важно, предвид свободата за

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

интерпретация, която Регламентът дава при изследване на понятието за „достатъчно" гаранции за прилагане на подходящи технически и организационни мерки.
В чл. 5 се изреждат принципите за обработване на лични данни по следния ред:

► ***Законосъобразност, добросъвестност и прозрачност***

Законосъобразността на обработването Регламентът най-общо определя като наличие на поне едно от посочените в чл. 6 условия за допустимост на обработването (съгласие на субекта, законово или договорно задължение, за изпълнението на което е необходимо обработването на лични данни, защита на жизненоважни интереси на субекта или обществен интерес или с оглед защита на легитимни интереси на администратора). С оглед на този принцип обработването следва да се осъществява само в случай, че субектът, носител на данните, е дал изричното си писмено съгласие за обработването на личните му данни и то по отношение на една или повече конкретни цели, или обработването да произтича от нормативен акт. Тук следва да се вметне, че съгласието за обработване на лични данни задължително
- следва да бъде дадено по недвусмислен начин,
- да е конкретно за определено посочени цели и
- субектът на личните данни да е дал по изричен начин информираното си съгласие по отношение на всяка отделна дейност по обработване на предоставените данни.

Във връзка с посочените изисквания, администраторите и обработващите лични данни вероятно ще срещнат значителни затруднения както в технически, така и в организационен план (включително във връзка с изискването за документално и/или по електронен начин отчитане на всяко действие). Въвеждането на посочените технически и организационни мерки е от значителна важност и поради обстоятелството, че при евентуален спор, администраторът е този, който ще носи доказателствената тежест относно факта на дадено надлежно съгласие за обработване на лични данни. На следващо място принципът за законосъобразност ще бъде спазен, когато обработването на личните данни представлява предаване в рамките на група предприятия за вътрешни административни цели, както и в случаите на гарантиране на мрежовата и информационната сигурност.
Принципът на **прозрачност** пък изисква цялата информация относно обработването на лични данни да бъде предоставяна на субекта лесно и в разбираема за него форма /в този смисъл е и съображение 60 от Регламента/.
Добросъвестността в обработването на лични данни на лицата следва да се тълкува в смисъл, че обработването не следва да надхвърля целите, относно които същото е необходимо или да води до противоправни резултати.

► ***Ограничение на целите***

Посоченият принцип следва да бъде тълкуван в смисъл, че конкретните цели, за които се обработват лични данни, следва да бъдат ясни и законни и определени към момента на събирането на личните данни. Той изисква от задължените лица /администраторите и обработващите лични данни/ да събират и обработват лични данни за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, който да е несъвместим с тези цели. Във връзка с този принцип и в случай, че предоставените лични данни се използват за други цели, които дори да са тясно свързани с първоначално заложените, то

гр. София, бул. „Витоша" № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

лицето задължително трябва да бъде информирано за другите цели и му се даде възможност да възрази.

Във връзка с гореизложеното следва да се обърне внимание на случаите, в които администраторът или обработващият лични данни обработва личните данни за други цели, които не съвпадат с тези, за които лицето е предоставило първоначално данните си и е дало информираното си съгласие или обработването не е свързано с овластяване по силата на изрична правна норма. В посочените случаи администраторът или обработващият личните данни следва да направи обоснована конкретна преценка дали обработването е съвместимо с първоначалната цел, за която са били събрани личните данни, Считаме че и това задължение би могло да доведе до поява на затруднения, които ще следва да бъдат разрешавани чрез консултации, в някои случаи чрез участието и на специалисти в конкретната област, за да не се стигне до незаконосъобразно обработване на лични данни за цели, които не са съвместими с първоначално приетите от лицето, предоставило данните, а впоследствие - и до налагането на санкции във връзка с това обработване.

► ***Свеждане до минимум***

Под това понятие всъщност GDPR има предвид, че събираните и обработвани лични данни следва да бъдат релевантни (свързани) и ограничени единствено до необходимото за целите, за които се обработват. Отделно от това, до обработване на лични данни следва да се стига единствено в случаите, в които целта не може да бъде постигната с други средства и то единствено за срок, който не надвишава необходимостта.

► ***Точност***

Принципът на „точност“ на личните данни е свързан със задължението на администраторите и обработващите лични данни да поддържат последните в актуален вид, с оглед на което ще следва да се предвидят подходящи и своевременни организационни мерки, които да гарантират коригиране, допълване или изтриване на неточни лични данни.

► ***Ограничение на съхранението***

Чл. 6, б. „д“ от Регламента обяснява смисъла на посочения принцип като забрана за съхранение, съответно задължение, към администраторите да съхраняват данните във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни. В тази връзка следва да се подчертае, че личните данни могат да се съхраняват и за по-дълги срокове, доколкото те биват обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в Общия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните.

В тази връзка е важно да се вземат предвид нормативно установените срокове за съхранение, като по отношение на всяка сфера на дейност е необходимо конкретно задължените лица освен да проучат и установят нормативно определените срокове, да следят за бъдещо изменение на същите, за да не се стигне до налагането на санкции за неправомерно обработване на лични данни.

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

► ***Цялостност и поверителност***

Принципът на цялостност и поверителност изисква от администраторите и обработващите лични данни да осигурят „подходящи“ технически и организационни мерки, така че обработваните лични данни да бъдат защитени от злоупотреба, унищожаване, загуба и т.н. В тази връзка следва да се отбележи, че много малко са предприятията и организациите, които разполагат с технически решения за осигуряване на сигурност срещу незаконосъобразно обработване или изгубване и унищожаване на личните данни, а дори и някои от задължените лица да имат такива, то с предстоящата правна уредба, въведена с Регламента, защитата значително се увеличава, с оглед на което следва да бъдат взети сериозни мерки както от техническо и организационно, така и от юридическо естество във връзка с новите изискванията.

► ***Отчетност***

Макар посоченият принцип, по своето наименование да звучи формално, всъщност той възлага в тежест на администратора и обработващия лични данни да докаже точното спазване на принципите на обработването и задълженията, възложени му с Регламента. От тук следва, че предприятието, обработващо лични данни, следва да е приело вътрешни писмени правила, които да уреждат реда и процедурите по обработване, използване и съхранение на лични данни в съответствие с разпоредбите на Регламента.

Както става ясно, адресатите на горепосочените задължения – администраторите и обработващите лични данни, са тези, които носят юридическата отговорност за спазването на всички изброени принципи, като освен това същите следва по всяко едно време да бъдат в състояние да докажат спазването им и съобразяването с новите правила, въведени с Регламента. С оглед на гореизложеното, за задължените лица следва период, в който да предприемат подходящите технически и организационни мерки във връзка със спазването на изискванията, както и надлежно документиране, за да може лесно да се доказва спазването им при осъществяване на проверки от контролиращите органи.

ОСНОВНИ ПОЛОЖЕНИЯ НА GDPR

ПРАВА НА ФИЗИЧЕСКИТЕ ЛИЦА, СУБЕКТИ НА ЛИЧНИ ДАННИ

Във връзка с посочената по-горе цел на Общия Регламент за защита на личните данни, както и практическото приложение на изброените принципи, е необходимо да бъдат посочени конкретните права, които лицата имат, както и необходимостта от осигуряването на гаранции за защита на тези права.

Субектът на данни (физическото лице, за което се отнасят данните) има право на:

► **Информираност** - всеки субект има право да получи по ясен, недвусмислен начин, на прост и разбираем език информация относно правата си, като за част от информацията GDPR дори поставя изискване същата да бъде предоставена отделно от всяка друга. Дори и от най-повърхностния анализ на приложимите разпоредби става ясно, че посоченото право на физическите лица всъщност възлага значителни задължения върху администратора на лични данни. Последният ще е длъжен да изготвя и поддържа значителен набор от документи,

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

съдържащи посочената информация, както и сериозна организация, която да осигурява своевременното предоставяне на тази информация на субектите. В тази връзка, ще следва да отпаднат досегашните практики за прикрито посочване на целите на обработването и правата на физическите лица в различни договори или формулирането на дълги, сложни и изпълнени с правни термини изречения;

► **Достъп до собствените лични данни** - субектите на лични данни имат право, при поискване, да получат копие от личните данни, които биват обработвани, както и допълнителна информация във връзка с обработването. От анализа на разпоредбата на чл. 15, §3 става ясно, че първоначално посочената информация се предоставя на субектите безплатно, а едва при изискване на допълнителни копия администраторът има възможност да наложи разумна такса.

► **Коригиране** (в случай, че обработваните лични данни са неточни или непълни);

► **Изтриване на личните данни** (т.нар. право на субекта „да бъде забравен“);

► **Ограничаване на обработването** от страна на администратора или обработващия лични данни;

► **Преносимост на личните данни** между отделните администратори;

► **Възражение спрямо обработването** на негови лични данни. Тук отново следва да бъде посочено, че в производството по разглеждане на възражението от страна на субекта, в тежест на администратора ще бъде да докаже наличието на легитимно основание за обработването;

► Субектът на данни има **право и да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране**, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен;

► **Право на защита по съдебен или административен ред**, в случай, че правата на субекта на данни са били нарушени. Във връзка с това право са предвидени и определени средства за защита.

• На първо място се гарантира правото на гражданите за подаване на **жалба до надзорен орган.**

• Тази защита се засилва и с правото на ефективна **съдебна защита срещу решенията на надзорните органи**. Освен това субектът на данните има право на ефективна съдебна защита срещу администратор или обработващ лични данни, като тук задължително следва да се подчертае, че посочената съдебна защита предоставя **правото на субектите на лични данни да претендират заплащането на обезщетение от администратора или обработващия данни за всички материални или нематериални вреди**, които същият е претърпял в резултат на нарушение на регламента. Последното е във връзка и с посочените вече в началото на статията административни наказания, които се изразяват във възможността за налагане на глоби или имуществени санкции в предвидените размери.

Мерките, които влизат в сила от 25 май 2018 година, са предимно свързани с актуализиране на досега действащите правила, като обхватът им значително се разширява. Въвеждат се еднакви правила по отношение на нивото на поверителност при събирането и съхранението на личните данни. Освен това прилагането на новите завишени правила и задължения имат за цел създаването на различни и нови възможности за съхранението и обработката на личните данни, а по този начин ще се осигури и сигурността в цифровия единен пазар -

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

ключова цел на стратегията за цифров единен пазар, което неминуемо ще има за последица и повишаване на доверието на лицата, които предоставят личните си данни за една или друга нужда на администраторите или обработващите лични данни. Регламентът предвижда да бъдат уеднаквени правилата за електронните съобщения както за бизнеса, така и за гражданите.

ЗНАЧИТЕЛНО ЗАВИШАВАНЕ НА САНКЦИИТЕ

Регламентът предвижда значително по-големи санкции при неспазването на изискванията му в сравнение със сега установените в българския Закон за защита на личните данни. С GDPR е предвидена възможност за налагане на глоби или имуществени санкции, според вида на нарушението, в размер до 20 000 000 евро или 4% от общия годишен световен оборот за предходната финансова година на предприятие - която от двете суми е по-висока, включително при нарушаване на основните принципи за обработване на лични данни, предвидени в Регламента. Разбира се, посочените санкции са предвидени за случаите на обработване на значителни по количество лични данни, както и изключително груби нарушения да задълженията, установени в регламента.

Въпреки това, **следва да бъде взета предвид значителната вероятност относно това, предвид новите моменти в уредбата и цялостната идея зад реформата, под удара на санкциите да попаднат и организации, които обработват лични данни и в по-малък мащаб.**

НОВИТЕ ИЗИСКВАНИЯ СЪГЛАСНО GDPR

Общият регламент за защита на личните данни (ОРЗД/GDPR) въвежда редица задължения за администраторите и обработващите лични данни, някои от които са изцяло нови и непознати в досега действащата правна уредба, поради което най-късно до 25 май 2018г. всички задължени субекти е необходимо да изградят вътрешни правила и да се снабдят с необходимите документи и технически решения за съобразяване с новите изисквания.

На първо място, следва да бъде посочено, че обработването на личните данни следва да бъде извършвано при съответствие с принципите за защита на личните данни, установени в Регламента и посочени по-горе в настоящата статия, като е необходимо съответният администратор или обработващ данните да е в състояние да докаже това – т.нар. **отчетност.** В тази връзка следва да се има предвид, че именно при нарушаване на основните принципи при обработване на личните данни, Регламентът предвижда посочените по-горе в настоящата статия санкции, а именно – до 20 000 000 евро или 4 % от общия годишен световен оборот за предходната финансова година на предприятие - която от двете суми е по-висока.

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Едно от най-важните нови задължения, произтичащи от Общия Регламент за защита на личните данни, е това по определяне на длъжностно лице по защита на личните данни в изрично посочените от Регламента случаи, както и поддържане на регистър на дейностите по обработване, за които същото ще носи отговорност. Длъжностното лице може да е служител на администратор на лични данни или да бъде външно за организацията на администратора

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

лице, като следва да се подчертае, че е предвидена възможност едно такова лице да отговаря и за няколко структури. Лицето по защита на личните данни ще следва да притежава задълбочени експертни познания в областта на законодателството и практиката на защитата на личните данни. То ще бъде натоварено с консултативни функции в областта на защитата на личните данни, както и ще следва да осъществява надзор по спазването на регламента в организацията на администратора, включително повишаването на осведомеността и обучението на персонала във връзка с новите изисквания. Независимо дали лицето, което ще бъде определено за длъжностно лице по защита на личните данни, ще е част от структурата на съответния работодател, или ще бъде външно за него лице, ще следва да се изработят съответните трудови/граждански договори, както и длъжностна характеристика, включително съдържаща подробно описание на дейностите, с които същото ще се занимава, както и отговорностите му, за да се гарантира точното изпълнение на изискванията, предвидени с Регламента.

Следва да се има предвид, че определянето на такова лице ще бъде задължително единствено в изрично определените в Регламента случаи. Случаите на задължително определяне и назначаване на такова лице са следните:

- За публични органи или структури, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;
- Администратори, чиято дейност, поради своето естество, обхват и цели, изискват редовно и систематично мащабно наблюдение на субектите на данни;
- Администратори, чиито основни дейности се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

УВЕДОМЯВАНЕ НА НАДЗОРНИЯ ОРГАН И СУБЕКТА НА ДАННИ В СЛУЧАЙ НА НАРУШАВАНЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Следващо важно задължение за администраторите и обработващите лични данни е това относно уведомяване на надзорния орган и субекта на данни в случай на нарушаване на сигурността на личните данни, както и документиране на всяко нарушение на сигурността на личните данни, включително относно всички факти, свързани с нарушението, последиците от него, както и предприетите действия за справяне с нарушението. С оглед на тези изисквания задължените субекти ще следва да подготвят значителна по обем документация, за да може да изпълняват задълженията си за уведомяване своевременно и в пълнота с изискванията.

Освен това, друго задължение, при случаи с висок риск за личните данни, породен от обработването им, задължените лица ще следва да провеждат предварителни консултации с надзорния орган, за да се вземат превантивни мерки за защитата на данните, както и за превенция на евентуални спорове.

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ, СВЪРЗАНИ СЪС СИГУРНОСТТА НА ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Както вече беше споменато в началото на статията, във връзка със засилената защита, задължените лица ще следва да започнат използването на подходящи технически и

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com

организационни мерки за осигуряване в достатъчна степен на сигурността на обработваните лични данни, като Регламентът посочва като част от тях следните:

► псевдонимизация;

► криптиране;

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

► своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

► редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки;

► сътрудничество с надзорния орган за защита на личните данни при изпълнение на задълженията, произтичащи от Регламента.

Следва да се подчертае, че предвид липсата на значителна практика у българските дружества относно имплементирането, съответно – ефикасното използване на посочените както чисто технически, така и правно-организационни мерки, в началото на периода на приложение на GDPR, ще възникнат затруднения за задължените лица.

Последното ще породи и нуждата от използването както на юридически консултации, така и на услуги в областта на информационните технологии. Последните ще осигурят техническите решения, необходими за справяне с проблемите във връзка със създаването или въвеждането на специфични софтуерни решения, както и използването капацитета на IT специалистите във връзка с поддръжката и актуализацията му, и използването на адекватни технически мерки за защита на информацията. Юридически познания ще бъдат необходими при създаването, и надлежното използване на документация и вътрешни правилници на предприятията, въвеждането на адекватна вътрешноорганизационна структура, и първоначални и периодични обучения на засегнатите служители. Предоставените технически и юридически решения, взети заедно ще отговорят на нуждите на администраторите на лични данни и ще осигурят т.нар „GDPR compliance“ – или иначе казано, адекватно и пълноценно прилагане правилата на Регламента в съответствие с поставените в него многобройни условия за защита на личните данни на гражданите.

Във връзка с подбиране и изработване на подходящите технически и правно-организационни мерки, както и относно консултации по приложението на GDPR, Адвокатско дружество „Георгиева, Фитковски и Тонев“ може да предостави капацитета на екипа си.

гр. София, бул. „Витоша” № 81, ет.3 (надпартерен), ап.10 тел. 02/980 09 04; тел./факс 02/980 85 93 www.gftlaw.com