ПРИВЕЖДАНЕ В СЪОТВЕТСТВИЕ С GDPR – СТЪПКА ПО СТЪПКА

КОМЕНТАРИ - ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Привеждане в съответствие с GDPR – стъпка по стъпка

Десислава Кръстева, адвокат,
съдружник в Адвокатско дружество „Димитров, Петров и Ко.“ и старши правен експерт във Фондация „Право и интернет“

Актуално към 07. 05. 2018 г.

Времето от 04. 05. 2016 г., когато бе публикуван в Официален вестник на ЕС *Регламент 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***) (**GDPR**/ Регламента), до 25. 05. 2018 г. датата, от която същият ще започне да се прилага, неусетно изтече.

След броени дни всички негови правила и изисквания ще започнат да се прилагат едновременно, пряко и по еднакъв начин Регламентът във всички държави-членки на ЕС.

Този „гратисен“ период бе предоставен от европейския законодател на всички публични и частноправни организации, за да приведат дейността си в съответствие с изискванията на GDPR.

В рамките на изминалите 2 (две) години темата за защитата на личните данни и конкретно за изискванията на Регламента добиваше все по-голяма популярност и актуалност, достигайки в последните няколко месеца до изключителни нива на напрежение, тревога и объркване сред всички сектори от бизнеса и дори сред публичните органи.

Някои организации твърде късно и дори едва сега предприемат първите си действия в посока съобразяване с GDPR, а не липсват и такива, които все още изчакват приемането на национално законодателство, появата на официални разяснения относно изискванията или дори отлагане действието на Регламента.

Безспорно всяка организация е срещнала или тепърва ще среща редица затруднения в процеса по привеждането си в съответствие с изискванията на Регламента – от липсата на ресурси при микро, малки и средни предприятия и start-ups до необятните и разнопосочни информационни масиви, изградени в мултинационалните бизнес гиганти, от непознаването и неразбирането на новите правила до осъзнаването на дълбочината и степента, в която Регламентът в действителност изисква да се промени всяка дейност по обработване на лични данни.

Настоящата статия:

- ще се спре на **ключовите стъпки**, през които трябва да премине:

- ***всяка една организация*** (независимо от мащабите си) и дори

- ***самостоятелно практикуващи физически лица*** (счетоводители, одитори и др. под.), за да са в съответствие с Регламента, като

- същевременно **даде препоръки**, които да улеснят дори най-малкия бизнес да започне (ако все още не е) и да реализира успешно този процес.

Имаме малка фирма. Засягат ли ни GDPR?

GDPR ще се прилага към дейността на всеки администратор и на всеки обработващ лични данни, независимо от мащаба на дейността им. Това означава, **че в приложното поле на GDPR** попадат и:

- ***най-малките организации и бизнеси***, както и
- ***самостоятелно практикуващи физически лица.***

Основните изисквания на Регламента и особено **основните му принципи**, дефинирани в чл. 5 (повече информация може да се види в материала „**GDPR - основни принципи при защита на личните данни**“ от февруарския брой на списанието за 2018 г.), са **задължителни за всички администратори.**

Предварителна подготовка

Преди да преминем по същество към привеждането на дейността ни в съответствие с изискванията на Регламента има определени подготвителни действия:

1. Формиране на **вътрешен екип**;
2. Запознаване с **основните изисквания на Регламента** най-малко на екипа по т. 1; и
3. Избор на **подход**:

- изцяло със ***собствени ресурси*** или
- с помощта на ***външни консултанти***.

Формирането на вътрешен екип, който да отговаря за защитата на личните данни, в рамките на самата организация е задължителна предпоставка не само за привеждането в съответствие, а и за последващото спазване на изискванията на Регламента.

Този екип трябва да обхваща **ключовите фигури във вашата организация**, които в съвкупност да имат ***поглед върху всички основни ваши дейности*** (наемане на персонал; отношения със служители; финансови и счетоводни дейности; продажби/отношения с клиент; информационно и технологично обезпечаване и т.н.).

Препоръчително е **участниците в този екип да са на по-ръководни позиции**, т.е. екипът да се състои от хората, които взимат важните управленски решения относно дейността на организацията.

В по-малки организации би било съвсем уместно и дори препоръчително **част от този екип да е самият управител на организацията**.

В **изключително малки организации** пък вместо цял екип, би могъл да бъде определен **един отговорник**.

Това не е задължение, което ви е предписано от самия Регламент, а практическа необходимост, защото спазването на изискванията е възможно единствено при добро и пълно познаване на същинската дейност на организацията.

Този **екип или отговорник** за защитата на личните данни в организацията ***не трябва да се бърка*** с фигурата на **Длъжностно лице по защита на личните данни**, за която ще спомена по-долу.

Така формираният екип или определеният отговорник за защитата на личните данни е необходимо да имат добри познания и разбиране относно изискванията на Регламента.

Ако планирате да ползвате съдействието на външни консултанти, е важно да знаете, че за успешното ви привеждане в съответствие с изискванията на Регламента ще е невъзможно, ако формираният вътрешен екип не им окаже адекватно съдействие и не им предостави пълна и достоверна информация за дейностите на организацията.

Стъпка 1 – Инвентаризация

Независимо как ще бъде наречена тази стъпка – инвентаризация, каталогизация, data mapping и т.н., това е **първата задължителна стъпка**, през която е нужно да се премине, за да сме сигурни, че спазваме изискванията на Регламента.

Най-сигурният начин да не спазваме изискванията на Регламента е, ако изобщо не осъзнаваме, че обработваме лични данни или ако не знаем пълния обхват на извършваното от нас обработване на лични данни.

В рамките на **тази стъпка** трябва ***да се идентифицират всички дейности*** в организацията ни, които са ***свързани с обработване на лични данни***.

Най-общо казано това са **всички дейности**, при които по някакъв начин:

- събираме,
- използваме,
- създаваме,
- променяме,
- пазим,
- заличаваме *или*
- извършваме каквото и да е друго действие, свързано с **информация, отнасяща се до физически лица**.

В съвременния високотехнологичен свят дори една малка организация би могло да се окаже, че борави с внушителен обем данни.

За да улесните процеса по инвентаризация, **разделете дейностите по обработване** на **основни процеси** като:

- отношения със служители,
- отношения с кандидати за работа,
- отношения с ползватели на уебсайт,
- отношения с клиенти,
- отношения с доставчици,
- видеонаблюдение и т. н.

Обичайно тези основни процеси ***съдържат множество подпроцеси по обработване*** на данните със свои собствени специфики, *например*, **в отношенията със служителите** или т. нар. управление на човешки ресурси се включват подпроцеси като:

1. сключване, изменение и прекратяване на договорите;
2. пенсионна, здравна и социално-осигурителна дейност;
3. управление на изпълнението на работата и оценка на представянето;
4. контрол на достъпа до помещенията;
5. контрол на достъпа до информационните системи и оборудването и други подобни. Преди да пристъпите по същество към инвентаризацията е необходимо да имате максимално пълен списък от

процеси и под-процеси. Ако в хода на самата инвентаризация, установите, че съставеният списък е непълен допълнете го и включете в инвентаризацията и новите процеси.

Знайте, че **дори и да използвате външен консултант** успешната реализация на тази стъпка е ***невъзможна без адекватно и активно участие от ваша страна***, от страна на вашия вътрешен екип.

Опитните консултанти могат въз основа на натрупаните познания да предполагат за наличието на определени често срещани в организациите дейности по обработване на данните и могат да ви насочват с конкретни въпроси.

Единствено вие, обаче, познавате в дълбочина и пълнота спецификата на собствените си дейности и практики.

Затова именно е изключително важно отговорният екип в организацията да има добри познания относно Регламента – за да може да набележи в пълнота всички дейности по обработване на данни.

Целта е **в края на тази стъпка** да имаме **пълна картина** на текущото състояние на **дейностите по обработване на лични данни**, които се извършват в организацията и по-конкретно:

1. *Какви лични данни обработваме*?

Всяка информация, която може да доведе ***пряко*** или ***косвено*** **до идентифицирането** на определено **физическо лице**, представлява **лични данни**.

Преценката дали са налице лични данни е необходимо винаги да се извършва въз основа на обработваната от администратора информация в нейната съвкупност.

Не бързайте да изключвате информация, която считате за анонимна на този етап.

2. За кого се отнасят?

Данните, които почти всяка организация обработва, се отнасят до различни типове физически лица:

1. **персонал** (по трудови и граждански договори), кандидати за работа;

2. **контрагенти**, клиенти доставчици, търговски партньори, подизпълнители, наемодатели, наематели и др. под., ако са:

- ***физически лица*** или
- ***техните представители***, ако са юридически лица;

3. посетители на офисите/ помещенията при контрол на достъпа, видеонаблюдение и друг подобни и т. н., и т.н.

3. За какви цели обработваме данните? За какво са ни нужни?

Вероятно събирате, обработвате и съхранявате лични данни за най-разнообразни цели:

- управлението на човешките ресурси,
- изпълнението на трудовите договор,
- за счетоводни цели,
- за обслужване на клиентите,
- за планиране на дейността на организацията,
- за маркетингови цели, и т.н.

Положете усилия да **опишете всички цели**, за които са ви нужни или биха могли да ви потрябват данните, с които разполагате.

4. От къде получаваме данните? Кой е техния източник?

Дали събирате данните:

- **директно** от самите физически лица, за които те се отнасят (например, CV-та, изпратени ви от кандидати за работа), *или*
- ***се генерират в процеса на ползване на определена услуга*** *или*
- при реализиране на **някакви конкретни договорни отношения** (информация за направени заявки, за дължими и платени възнаграждения от клиенти и др. под.), *или*
- ги **получавате от други лица** (напр. ваши клиенти ви предоставят данни за свои служители или клиенти и ви възлагат да ги обработвате от тяхно име), *или дори*

- ги събирате от **публично достъпни източници** (вкл. Интернет) и т. н.

Не изключвайте от вашата инвентаризация ***данни, които събирате от публично достъпни източници.*** Това, че определени данни са публично достъпни, изобщо не означава, че по отношение на тях не се прилагат изискванията на Регламента.

5. Къде обработваме данните?

6. На кого предоставяме данните извън нашата организация?

7. Предоставяме ли данните на лица, които са в други държави и особено в държави извън ЕС?

Отговорите на всички гореизброени въпроси, наред с тези за източниците на данни по т. 4, ще помогнат да бъдат идентифицирани извършваните от организацията обмени/трансфери на данни.

8. С какви средства обработваме данните?

9. В какви срокове пазим данните?

Детайлното и добре структурирано описание на изброената по-горе информация, ще спомогне за по-бързото и ***ефективно изпълнение на следващите стъпки***, затова му отделете нужното време и внимание.

Не на последно място, в рамките на тази дейност съберете **и систематизирайте и всички вътрешни правила, документи и процедури, типови договори, модели на декларации за съгласие и др. под., които се отнасят до обработването на лични данни** и използвате/прилагате към момента, включително информацията, която фигурира в текущата ви регистрация като администратори в Комисията за защита на личните данни (КЗЛД).

Знайте, че **Регламентът не променя концепцията за защита на личните данни**, която е бе ***заложена в досегашния Закон за защита на личните данни***, а единствено я **надгражда**.

Това означава, че колкото повече усилия сте инвестирали в спазването на стария режим по защита на личните данни и колкото по-голяма степен на съответствие са дейностите ви с него, толкова по-лесно и бързо ще се приведете в съответствие и с новите изисквания.

Стъпка 2 – Анализ

В рамките на **първата стъпка** (инвентаризацията) се предполага, че е събрана в ***пълната*** **информация за** ***всички*** **дейности по обработване.**

Сега е време да се направи **анализ на всяка една от тях** и да се прецени дали тя отговаря на изискванията на Регламента.

Това по своята същина е един **правен анализ** и затова извършването му изисква добро познаване и разбиране на нормативната уредба. Ако във вашия екип нямате с нужното образование, познания и опит, е препоръчително да потърсите експертна помощ.

В рамките на този анализ ще е необходимо да бъдат дадени **отговори най-малкото на следните въпроси:**

1. ***Необходими ли са ви всички данни, които обработвате, за набелязаните от вас цели*** (принцип за свеждане на данните до минимум)?

Ако в рамките на инвентаризацията сте установили, че обработвате или пазите **данни**, ***без да можете да формулирате конкретни цели***, за които те са ви нужни, то най-вероятно **трябва да преустановите тяхното обработване**. Недопустимо е да бъдат обработвани лични данни без конкретна и предварително определена цел.

Затова по отношение на такива данни е безпредметно да се извършва какъвто и да е допълнителен анализ за съответствието на обработването им с Регламента, защото **обработването им трябва да бъде преустановено** (т.е. данните по надлежен начин ще трябва да бъдат заличени и да не бъдат събирани в бъдеще).

2. ***Възможно ли е целите, за които обработвате личните данни, да бъдат постигнати с по-малко данни*****?**

Ако отговорът на този въпрос е положителен, то **всички данни, без които реално можете да постигнете преследваните цели**, също следва ***да не бъдат повече събирани и обработвани***, а събраните до този момент данни **–** да бъдат заличени по надлежен начин.

3. На какво правно основание се обработва данните:

- ***законово задължение;***
- ***сключване и/или изпълнение на договор, по който физическото лице е страна;***
- ***легитимен интерес, който има преимущество пред правата и интересите на физическите лица, чиито данни обработвате;***
- ***съгласие или др.?***

Това е особено важен въпрос.

За законосъобразното обработване на личните данни е необходимо задължително да разполагате **най-малко с едно** от правните основания по **чл. 6** от Регламента.

Преценката трябва да е много внимателна и е силно препоръчително да се извърши с помощта на квалифициран юрист, за да сте сигурни, че действително е налице валидно правно основание за обработване на данните.

Например, много често в организациите след прекратяване на едно трудово правоотношение цялата документация и информация натрупана за бившият служител се запазва с нагласата, че ще се съхранява 50 г. и че е налице законово задължение за това.

В действителност, обаче, законовото задължение за пазене за срок от 50 г. се прилага само за ограничен кръг от документи (ведомости, трудов договор, непоискана трудова книжка и др.), а не за всякакви други данни и документи натрупани в трудовото досие.

За тях въпросното законово задължение не се прилага, а по-скоро е налице друго основание (напр. легитимен интерес за защита при възникнали последващи претенции) и съответно ще могат да се пазят за друг и то много по-кратък срок.

Внимание! Особено внимателно подхождайте към използването на основанието **„съгласие“**.

В никакъв случай **не комбинирайте** това основание с основанието:

- „законово задължение“ или с

- „договорно основание“.

Това са самостоятелни основания и няма необходимост, не трябва да събирате съгласие за обработване, което се основава на някое от тях.

Не изисквайте и не събирайте съгласие, ако разполагате с друго правно основание.

Например, изключително погрешна практика, криеща рискове от възникване на спорове, е да се изискват съгласия от служителите за обработването на данните им в контекста на задължителните пенсионни, здравни и социално-осигурителни дейности, защото при искането на съгласие на физическото лице трябва да му се даде възможност и да откаже да го даде, както и да може по всяко време да го оттегли.

С оглед принципът за отчетност е важно при **правни основания** от типа:

- съгласие или
- договор,

да разполагате и с надлежно доказателство, че същите са налице, т.е. да можете да докажете, че действително сте получили съгласие и то като съдържание то отговаря на изискванията на Регламента.

4. Оправдано ли е свързаното с извършваното обработване навлизане в личната сфера на физическите лица, спрямо целите, за които се преследват (принцип на добросъвестност)? Съответстват ли обработваните данни, на преследваните цели?

Определени дейности по обработване на лични данни могат да нарушават принципите и изискванията на Регламента, дори и да сме си осигурили правно основание, като например, съгласие, за тях, ако по **неоправдан, прекомерен начин навлизат в личната сфера на физическите лица.**

Например, изискването на прекомерно лична информация в рамките на едно интервю за работа от типа дали кандидатът планира в близките няколко години да забременее и да има деца, може да изглежда напълно резонен въпрос за един работодател, но в действителност би съставлявал нарушение на принципа за добросъвестност и за свеждане на данните до минимум. Събирането на такава информация би поставило кандидати – жени в детеродна възраст, в неравнопоставено положение спрямо другите кандидати и би накърнило правото им на труд.

5. Установени ли са конкретни срокове за обработване на данните? В случаите, когато фиксирането

на конкретни срокове е невъзможно, установени ли са обективни критерии за тяхното определяне и извършват ли се периодични прегледи за необходимостта и актуалността на данните?

Недопустимо е обработването на данни за ***неопределен и неопределяем срок***.

Пазенето на данни „завинаги“ също противоречи на изискванията на Регламента (на принципа за ограничение на съхранението).

6. Осигурена ли е възможността на физическите лица да упражняват правата, предоставени им с Регламента (право на информация, достъп, коригиране, изтриване, възражение, ограничаване на обработването, уведомяване на третите страни и преносимост) и ако да, по какъв начин?

Обърнете особено внимание на това дали и **по какъв начин са информирани физическите лица за извършаното обработване на техни лични данни** (принцип на прозрачност; право на информираност).

Осигурява ли ви използваният до сега начин за информиране надлежно доказателство, че сте изпълнили това свое задължение.

По отношение конкретно на информираността на физическите лица дори и до момента да сте ги информирали надлежно по стария режим за извършваното обработване на данни, знайте, че Регламентът въвежда допълнителни изисквания за информацията, която трябва да им бъде предоставена. Това означава, че е много вероятно да е необходимо **да актуализирате използваните до сега от вас декларации или политики за информираност** и ***да ги сведете по подходящ начин до знанието на физическите лица***, за които те се отнасят.

Проверете дали сте осигурили **практическа възможност на физическите лица да упражняват правата си**.

Преценете обективно и вашите **практически възможности да отговаряте и да обслужвате адекватно и в срок техните искания**.

Имате ли процедури за това и съответстват ли те на Регламента? ***Имате ли лице***, което да отговаря за тази дейности и достатъчно подготвено ли е то*?*

В зависимост от конкретната ви дейност, може да се окаже, че са необходими промени в начина, по който

функционират или са настроени системите и базите данни, които използвате.

Ако **основната ви дейност се реализира чрез уебсайт**, то ще е много по-удачно да осигурите в максимална степен ***адекватни функционалности в сайта***, чрез които ползвателите на уебсайта да упражняват правата си (напр. функции за коригиране на техните данни, функции за експорт и др. под.).

Относно така нашумялото напоследък право да „бъдеш забравен“, знайте, че то не е абсолютно и се прилага в ограничен набор от случаи.

Например, **нямате задължение да триете данни, които са ви необходими, за да изпълните вменено ви по закон задължение** (т.е. нямате задължение, а и реално не можете, изцяло да „забравите“ за бившите си служители дори и те да поискат това от вас).

7. По какъв начин са уредени отношенията, при които обменяте лични данни с трети лица? В какво качество, в каква роля (на администратор или на обработващ лични данни действате)?

Необходимо е да преразгледате наличните си към момента договорни уговорки с третите страни и по-конкретно дали и какви конкретни уговорки относно обработването и защитата на личните данни са налични в тях.

Регламентът въвежда множество конкретни изисквания относно тяхното съдържание, така че **всички отношения с трети лица** (други администратори или обработващи лични данни), които са свързани със съществен обмен на лични данни, ще се нуждаят от преуреждане.

Общи формулировки от типа, че насрещната страна отговаря изцяло за защитата на личните данни, ***не ви вършат никаква работа***.

Следете **дали тези отношения са уредени писмено – *писмената форма е задължителна***. Освен това наличието на писмени уговорки в тази посока е ключово за изпълнението на принципа за отчетност.

Не третирайте служителите си на трудов договор като „обработващи лични данни“, те не са такива. Те са лица, които действат под вашето ръководство по смисъла на **чл. 29** от Регламента.

8. Проверете внимателно дали извършвате трансфери на лични данни извън ЕС и ако да, дали е налице използването на надлежен инструмент, който да осигурява адекватно ниво на защита на

трансферираните данни (Privacy Shield за САЩ, стандартни договорни клаузи и др.)?

Едни от най-често срещаните случаи на трансфери на лични данни са **използването на хостинг услуги, клауд услуги или услуги по IT поддръжка, предоставяни от лица, които са установени извън ЕС**. Използването на такива услуги не е забранено от Регламента, но е нужно да са осигурени гаранции за защитата на данните съответстващи на европейския стандарт.

Затова проверете дали и какъв инструмент използва/ предлага да се използва в отношенията ви вашия чуждестранен доставчик, и уредете отношенията си по надлежен начин. Ако доставчикът ви не желае или е неспособен да ви предложи/ да прилага подходящ инструмент за трансфер на лични данни, то е силно препоръчително да го смените с такъв, установен в ЕС или с такъв, който има възможност да ви гарантира адекватно ниво на защита на данните, съобразено с изискванията на Регламента.

9. С какви рискове е свързано извършваното от вас обработване на лични данни? По какъв начин могат да бъдат засегнати правата и интересите на физическите лица при извършваното обработване или при нарушение в тяхната сигурност (напр. неоторизиран достъп, загуба и т.н.)?

Обърнете специално внимание на дейности като:

- обработване на специални категории данни като данни, разкриващи **расов или етнически произход**, **политически възгледи, религиозни или философски убеждения** или членство в синдикални организации, **генетични данни, биометрични данни, данни за здравословното състояние** или данни за сексуалния живот или сексуалната ориентация; данни относно присъди и нарушения.
- обработване на данни за **деца** (особено за лица под 14 г.);
- обработване на **други специфични данни**, които могат да водят до по-съществени рискове – напр. **ЕГН, копия на документи за самоличност, данни за местоположение и други подобни.**

10. Какви организационни и технически мерки за защита на данните прилагате? Имате ли вътрешни правила/политики за защита на данните? Съответстват ли прилаганите от вас мерки на рисковете, с които е свързано обработването на данните? Водят ли прилаганите от вас мерки за защита до ефективно минимизиране/ ограничаване на рисковете?

Приоритети

В края на тази стъпка би следвало да разполагате най-малкото със списък на несъответствията, идентифицирани в рамките на извършения анализ. Много вероятно е този списък да е доста внушителен.

Затова е препоръчително този списък **да включва и някаква оценка** или **индикация *за риска***, с който е свързано всяко конкретно несъответствие.

По този начин ще можете да си набележите ***приоритетните мерки*** **по привеждане в съответствие** и **да си съставите план-график за тяхното реализиране**.

Знайте, че **някои от констатираните несъответствия могат да наложат съществени промени в начина, по който работи организацията ви**, в използваните от вас технологични ресурси и др. под. Това е възможно да е свързано с необходимост да се инвестират съществени за вашата организация ресурси, затова внимателно анализирайте и преценете конкретния подход, по който ще позволи по най-ефективен и подходящ за конкретните ви нужди да приведете дейността си в съответствие.

Задължително ли е да премина през одит/ GAP анализ?

В момента на пазара редица консултанти с най-различен профил на експертиза предлагат своите услуги за извършване на одити, GAP анализи и др. под. дейности в посока привеждането на организациите в съответствие с изискванията на Регламента.

Създава се впечатление, че това е едва ли не задължителна дейност, която трябва да бъде премината от всеки администратор или обработващ лични данни. Трябва да се подчертае, обаче, че Регламентът не въвежда изискване за извършване на такава дейност. Безспорно без да се анализира текущото състояние на дейностите по обработване на лични данни в една организация, не би могло да се прецени доколко те съответстват на изискванията на Регламента и да се набележат необходимите промени в тяхното осъществяване.

Нямате, обаче, ***задължението да разполагате с някакъв специален доклад*** или др. подобен документ от извършен „одит“, за да се счете, че сте в съответствие с изискванията на Регламента.

Стъпка 3 – Мерки по привеждане в съответствие

В зависимост от резултатите от анализа конкретните мерки, които е необходимо да предприемете могат да бъдат от най-разнообразен характер.

Знайте, че ***няма*** **универсално решение** или продукт, който **да ви направи в съответствие с изискванията на Регламента.**

Необходимо е да изберете и приложите мерки, които ***съответстват на вашата дейност*** *и които* ***в действителност ще спазвате и ще прилагате*** на практика.

Наличието на някакъв формален наръч от документи не е равностойно на съответствие с Регламента.

Сред мерките (неизчерпателно), които биха ви били необходими са:

- Изготвяне на **Регистри по чл. 30 на Регламента** – ***отделен регистър за всяка една дейност по обработване на лични данни***.

Това е задължително най-малкото за всяка ваша основна дейност по обработване, независимо от размера на организацията ви.

Това задължение ще замести необходимостта от регистрация в КЗЛД, която след 25. 05. 2018 г. ще отпадне.

Вижте материала в настоящия брой на списанието: *"Задължението за водене на регистри по чл. 30 GDPR - някои практически съвети".*

- Поддържайте **актуални и налични вашите Регистри по чл. 30** на Реглмента. Те ***трябва да бъдат на разположение в случай на проверка от КЗЛД.***
- Изготвяне или актуализиране на **Политики за защита на личните данни**/ ***Декларации за информираност, които да съдържат цялата необходима информация по чл. 13 и чл. 14*** от Регламента, за да се гарантира **информираността на физическите лица** относно обработването на техните лични данни.

Не смесвайте в един единствен документ несъвместими дейности – например, **не би могло** ***един и същи***

документ да се ползва, за да информирате ***едновременно:***

- своите служители и
- своите клиенти

относно обработването на личните им данни.

Колкото по-пълни, ясни и разбираеми са тези Политики, толкова по-близо до изискванията и духа на Регламента сте.

- **Сведете по подходящ начин до знанието на физическите лица вашите Политики по защита на личните данни по чл. 13 и чл. 14** от Регламента и си осигурете ***подходящо доказателство, че сте го направили***.

За служители – можете да им ги връчите за подпис, за да се удостовери, че са запознати; **но не смесвайте това действие с искане на съгласие**.

Това са две напълно различни неща.

За клиенти – **публикувайте я публично в уебсайта си** или я направете приложение от сключваните с тях договори, или др. под.

За видеонаблюдение – поставете подробни информационни табели на входовете на офисите/ сградите/ помещенията.

- **Допълнете и изменете по надлежен начин договорите си с третите лица** (администратори или обработващи лични данни), с които обменяте лични данни.

Най-добре **оформете обособени писмени анекси**/ споразумения относно обработване и защита на личните данни. Знайте, че нямате необходимост от такива споразумения, когато предоставяте/ обменяте данни с публични органи в контекста на осъществяването на техните правомощия (напр. НАП, МВР, НОИ и други подобни.).

- **Осигурете си надлежни инструменти за трансфер на данни извън ЕС**, ако извършвате такива.
- Приемете или актуализирате по адекватен начин **Вътрешните си правила за организационни и**

технически мерки за защита на данните и ги сведете до знанието на служителите си. Следете възприетите мерки действително да се изпълняват.

- Определете си **конкретни срокове за съхранение на данните** и за **периодични прегледи** за тяхната необходимост и за тяхното заличаване.
- Осигурете **подходящи практически възможности за физическите лица** да упражняват правата си по Регламента.
- **Следете за нарушения в сигурността на данните**, определете си екип, който да отговаря при установяване на такива да предприеме незабавни действия по преустановяването им, по намаляване на негативните последствия и по информиране на КЗЛД.
- Други необходими и съобразени с дейността ви мерки.

Вместо заключение

Извън изброените по-горе мерки вероятно ще си поставяте и въпроси като:

1. имам ли нужда от Длъжностно лице по защита на данните;
2. трябва ли да извърша Оценка на въздействието върху защитата на данните;
3. трябва ли да премина през Предварителна консултация с КЗЛД и др. под.

Това са изисквания, които не се прилагат към всеки администратор или обработващ лични данни, а само в посочените в Регламента случаи или в други случаи, които изрично ще бъдат посочени в бъдещия закон или указани официално от КЗЛД.

Преди да пристъпите към ангажиране на Длъжностно лице по защита на данните се допитайте до специалисти в материята, за да установите дали действително за вас е налице такова задължение.

Знайте, че Длъжностното лице по защита на данните може да е ваш служител или да ползвате външна услуга, предоставена от физическо лице или организация.

И накрая:

Започнете (ако все още не сте)

Не трябва да се очаква, че Регламентът може да бъде отменен в близко време или че действието му ще бъде отложено. Това не означава, че след 25. 05. 2018 г. органите по защита на личните данни в ЕС ще предприемат масови и радикални проверки.

Същевременно, обаче, българският орган по защита на данните – **КЗЛД, е длъжна и задължително ще разглежда всяка отправена към нея допустима жалба**.

При постъпила такава жалба, която се отнася до нарушения, извършени след 25. 05. 2018 г., КЗЛД и българските съдилища ще са длъжни и съответно ще прилагат правилата на Регламента.

Поради това по никакъв начин не е препоръчително, за който и да е администратор или обработващ лични данни да отлага предприемането на действия в посока привеждане на дейността си в съответствие с изискванията на Регламента.

Това е процес, а не еднократен акт

Дори и да сте привели изцяло дейността си в съответствие с изискванията на Регламента, от тук на сетне ежедневно трябва да следите за спазването на изискванията му. При започване на каквато и да е нова дейност, предлагане или използване на нов продукт или услуга и др. под. – винаги проверявайте дали планираната промяна е съобразена с изискванията на Регламента и актуализирайте мерките си по съответен и подходящ начин.

Настоящият материал няма характера на правен съвет или консултация, и не следва да бъде възприеман като достатъчен за разрешаването на конкретни правни проблеми, казуси и др.

Становищата и мненията, изразени тук, са лични позиции на автора и не отразяват непременно позициите на „Димитров. Петров и Ко.“, Фондация „Право и интернет“, техните подразделения или служители.

ВНИМАНИЕ!

Вижте и **прочетете последователно** всички материали, публикувани в сп. "Данъци ТИТА" от началото на годината относно новия Регламент за защита на личните данни:

1. GDPR - **основни принципи** при защита на личните данни
2. **Основания за обработването на лични данни** и права на гражданите **–** ключови промени по GDPR

3. Основни **задължения на администраторите** на лични данни – ключови промени по GDPR
4. GDPR - **задължения на обработващите** личните данни
5. Привеждане в съответствие с **GDPR – стъпка по стъпка**
6. Задължението за водене на **регистри по чл. 30 GDPR** - някои практически съвети