БЪЛГАРСКИ ЦЕНТЪР
ЗА НЕСТОПАНСКО
ПРАВО

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Наръчник за НПО

Български център за нестопанско право
Програма Достъп до информация
София, 2018

Настоящият наръчник е изготвен в резултат на сътрудничеството на Български център за нестопанско право и Програма Достъп до информация. След влизането в сила на *Общия регламент относно защита на личните данни* на 25 май 2018 г. бяха проведени обучения за неправителствени организации от страната в София, Пловдив и Ловеч.

Целта на Наръчника е да запознае неправителствените организации със специфичните задължения, които произтичат за тях от действащото законодателство за защита на личните данни.

Текста на наръчника подготвиха **Стефан Ангелов, Александър Кашъмов** и **Кирил Терзийски** от правния екип на Програма Достъп до информация.

Авторите изразяват благодарност за ценните бележки на Надя Шабани, директор на Български център за нестопанско право, Гергана Жулева, изпълнителен директор на Програма Достъп до информация и Анна Адамова, програмен директор в Български център за нестопанско право.

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
Наръчник за НПО
адв. Стефан Ангелов, адв. Александър Кашъмов, адв. Кирил Терзийски – автори
дизайн и предпечат – Владимир Любенов
ISBN 978-619-7345-01-8 за хартиения вариант и ISBN 978-619-7345-02-5 за *e-book*

формат 1/16 (А5), 2,75 печатни коли, печат: Алекс-999

БЪЛГАРСКИ ЦЕНТЪР ЗА НЕСТОПАНСКО ПРАВО

Български център за нестопанско право (БЦНП) е създаден през юли 2001 г. за осъществяване на дейност в обществена полза. БЦНП е местният партньор на Международния център за нестопанско право (ICNL) със седалище във Вашингтон и на Европейския център за нестопанско право (ECNL) със седалище в Будапеща. **Мисията на БЦНП** е да оказва подкрепа при изработване и прилагане на закони и политики с цел развитие на гражданското общество, гражданско участие и добро управление в България. БЦНП следва мисията си с разбирането, че развитието на правната рамка на нестопанските организации е основен механизъм за създаване на независимо и просперираще гражданско общество. БЦНП насърчава прозрачността, отчетността и създаването на подходяща структура на управление на юридическите лица с нестопанска цел в България.

За повече информация: Български център за нестопанско право; 1000 София, ул. Хр. Белчев 3
тел.: (+359 2) 981 66 17 info@bcnl.org www.bcnl.org

Програма Достъп до информация (ПДИ) е българска неправителствена организация, основана през 1996 г., за да подпомага гражданите при търсенето на обществена информация и да подтиква публичните институции към прозрачност. ПДИ осъществява целите си, като работи в няколко направления: застъпва се за законодателство в областта на свободата на информацията, наблюдава практиките по предоставяне на информация, предоставя правна помощ на търсещите информация, организира кампании и обучения за разясняването на правото на достъп до информация. Програмата подпомага и защитата на личните данни, като участва активно в публичния дебат за законодателството в областта на личните данни, оказва правна помощ в случаи за спазване на баланса между правото на защитата на личните данни и принципа на прозрачността. След приемането на Закона за защита на личните данни през 2002 г. ПДИ първа стартира „Кампания за разясняване на правото на защита на личните данни“ (2003), проект, подкрепен от Европейска инициатива за демокрация и човешки права. ПДИ заедно с Интернет обществото – България е организатор на церемониите „Големия брат“ за България. През годините са консултирани над 700 казуса, свързани със защитата на личните данни, а след влизане в сила на *Общия регламент за защита на данните* през 2018 г. ПДИ води обучения по темата за представители на неправителствени организации.

За повече информация: Програма Достъп до информация; 1142 София, бул. В. Левски 76, ет. 3
тел.: (+359 2) 988 50 62 office@aip-bg.org www.aip-bg.org

AMERICA FOR BULGARIA FOUNDATION

Настоящият наръчник се издава от Български център за нестопанско право по проект „Продължаваща и разширена подкрепа за организациите на гражданското общество“, финансиран с грант от **Фондация „Америка за България“**. Всички мнения и твърдения, изразени в това или във всяко друго издание на Български център за нестопанско право, са на техния автор и/или издател и не отразяват непременно възгледите на Фондация „Америка за България“ или на нейните директори, служители или представители.

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

ЗЗЛД: Закон за защита на личните данни

КЗЛД: Комисия за защита на личните данни

ОРЗД (*Регламента, Общ регламент относно защитата на данните*): Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета на Европа 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)

ОВЗД: Оценка на въздействието върху защитата на данните

ЮЛНЦ: Юридическо лице с нестопанска цел

СЪДЪРЖАНИЕ

1. КАКВО СА ЛИЧНИ ДАННИ?

1.1. ЛИЧНИ ДАННИ

Лични данни е всяка информация, която се отнася до конкретен човек, ако с нея той може да бъде ясно идентифициран. Според практиката на Комисията за защита на личните данни, един човек например се идентифицира, когато са посочени трите му имена. Той обаче може да бъде идентифициран, дори ако е представен само с две имена, но тяхната уникалност позволява да се досетим за кого става въпрос. И в двата случая – както когато даден човек е ясно идентифициран, така и когато просто можем да се досетим кой е, т.е. е идентифицируем, е приложимо и законодателството[1] за защита на личните данни.

Личните данни относно даден човек включват най-различна информация. Тя може да съдържа характеристики, свързани с физическата, физиологичната, генетичната, психическата, умствена, икономическа, културната или социална идентичност. Може да е снимка на лицето, поради което и видеонаблюдението попада в обхвата на защитата. Може да бъде дори данни за електронна поща или електронни съобщения, когато са свързани с конкретен човек или лесно може да се разкрие кой ги използва, респективно е участник в такава кореспонденция.

Отнасящата се до даден човек информация се смята за лични данни и в случаите, в които са отразени публични аспекти от неговия живот. Така например лични данни са и записите от видеонаблюдение по улиците и площадите, разкрити подробности от личния живот в публикации в медиите, информацията в публичните регистри, съдържащи имена на упражняващите определени видове професии, управителите и собствениците на търговски дружества, собствениците на недвижими имоти и др. В тези случаи публичността на данните е поначало оправдана с основанията, предвидени в Регламента, но в случай на нарушения на изискванията при обработването на лични данни пак се носи отговорност.

Лични данни представлява само информацията, която е записана и се съхранява на някакъв материален носител като хартия, магнитни носители и др. подобни. Не представляват лични данни възприетите от сетивата ни образи и знания, поради което възприемането и предаването на информация от човек на човек не попада в обхвата на защитата на личните данни.

Човек може да бъде идентифициран и чрез единен граждански номер, номер на документ за самоличност – например лична карта, шофьорска книжка, задграничен паспорт. Може да е някакъв код, с който той е несъмнено разпознаваем в електронна база данни, достъпна чрез интернет.

[1] Общ регламент за защита на данните / Регламент (ЕС) 2016/679(ОРЗД) и Закон за защита на личните данни.

С Регламента бяха добавени изрично т.нар. „онлайн идентификатор“ и идентификацията на местонахождението, която може да бъде извършена например чрез разкриване на уникалните данни на притежавано мобилно устройство – телефон, таблет и др., и на трафика на електронни съобщения през такива устройства.

Всяко наличие на идентификатор, с който се разкрива самоличността на даден човек или само може да бъде разкрита с висока степен на вероятност, води до приложимост на Регламента.

1.2. ЧУВСТВИТЕЛНИ ЛИЧНИ ДАННИ

Определена категория лични данни подлежи на защита в по-висока степен от останалите лични данни. Това са данните, свързани със:

- произход: расова и етническа принадлежност;
- убеждения: политически възгледи, религиозни и философски убеждения, както и членство в синдикални организации;
- биологични характеристики: биометрични данни, генетични данни;
- здравословно състояние и сексуален живот и ориентация.

Тези данни се обозначават като „специални категории данни“[2] или „чувствителни данни“.

Като правило обработването, т.е. събирането, използването, съхранението, предаването, разпространяването и т.н., на такива данни е забранено. То е допустимо по изключение, когато е налице изрично съгласие на дадения човек или при други посочени в Регламента основания. Такива са налице в случаите, когато се работи с данни за целите на трудовото право, социалното осигуряване, трудовата медицина, медицинска диагноза, оценка на трудоспособността, осигуряване на здравни или социални грижи, управлението на здравните и социалните услуги.

Следователно когато едно сдружение или фондация е работодател, те биха могли да работят, при спазване на необходимите гаранции, с такива лични данни за изпълнение на задълженията си от трудовоправен и осигурителен характер. Също така неправителствена организация, която извършва социални или здравни услуги, би могла да борави с такива данни за тези цели при стриктно спазване на изискванията на Регламента. По правило е необходимо субектът на данните да бъде предварително информиран.

1.3. ЛИЧНИ ДАННИ, СВЪРЗАНИ С ПРИСЪДИ И НАРУШЕНИЯ

Обработването на лични данни, свързани с установяването, че някой е извършител на престъпление или на административно нарушение, също

[2] Чл. 9 от Регламента.

следва да се осъществява при спазване на изискванията на Регламента. Работа с този вид данни може да се извършва само под контрола на държавен орган или когато обработването е разрешено от закона. Пълният регистър на присъдите по наказателни дела се поддържа само под контрола на държавен орган.

У нас този регистър се съхранява при районните съдилища, където се издават и свидетелствата за съдимост – официалните удостоверителни документи относно обстоятелството, че някой е осъждан или не за извършване на престъпление. В системата на Министерството на вътрешните работи се поддържат регистри, в които се въвеждат данните от полицейската регистрация на привлечените като обвиняеми за извършено умишлено престъпление от общ характер.

2. ОБХВАТ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Посланието на Регламента за защита на личните данни е те да се обработват внимателно и честно по отношение на хората, за които се отнасят. Както предшестващата го Директива, така и Регламентът не забранява събирането, използването, съхранението и другите форми на обработване на лични данни, а създава изисквания за тяхното отговорно обработване. Това се отнася дори до чувствителните лични данни, за които също е допустимо, макар по изключение, да бъдат събирани, използвани и обработвани по всякакви други начини, когато това се осъществява за постигане на предварително определена цел (първо) при спазването на изискването за съразмерност с тази цел (второ) и (трето) на предвидените в Регламента основания.

Защитата на личните данни се отнася само до информация, която е свързана с идентифициран или идентифицируем конкретен човек.

Кои данни не са обхванати от защитата?

- данни в обобщен, агрегиран вид: например отразени в резултатите от социологическо проучване. Не подлежат на защита данните на групи от хора, освен ако от тях не може да се разбере кое е конкретното лице;
- данните на починалите, макар че определени изисквания могат да се прилагат и в тези случаи спрямо събраните и съхранявани масиви от лични данни;
- данните на юридическите лица, т.е. на търговски дружества, политически партии, фондации, сдружения, държавни и общински учреждения, тъй като не представляват лични данни;

- данни, събирани и съхранявани единствено за лични или домашни занимания. Така например бележките в личния дневник или записите в личния мобилен телефон, макар формално да съдържат лични данни, не са в обхвата на уредбата относно защитата на личните данни.

Защитата се отнася към всеки етап от процеса на събирането, използването, съхранението и обработването по други начини на лични данни, които са част от регистър или са предназначени да бъдат част от регистър с лични данни. Под регистър се има предвид всеки списък, който съдържа лични данни в индивидуалните записи.[3]

Следователно, ако лични данни се намират в съхранявани от дадена организация документи, които обаче не са подредени в списък, нито са предназначени да бъдат подредени в списък, то работата с тях не се урежда от Регламента. Ако обаче даден документ се намира в организацията, без все още да е подреден в регистъра или „файловата система", но от естеството му е ясно, че би попълнил такава система, тогава се прилага защитата на личните данни.

Защитата обхваща всички случаи на обработка с автоматизирани средства, независимо дали работата с данните е изцяло или само отчасти с такива средства. Така например е възможно в дадена картотека част от документите от индивидуалните досиета да се пазят само на хартия в хартиената папка, а друга част да е отразена и в електронен вид в компютърен файл, който съответно е свързан с другите файлове в списъка от електронната картотека. Независимо че част от данните се обработва с автоматични средства, а друга част – не, то за всички тях се прилагат правилата за защита на личните данни. При автоматизираната обработка по начало винаги е налице „регистър" или „файлова система".

Регламентът обхваща и случаите на обработка с неавтоматизирани средства, когато данните са част от регистър или са предназначени да бъдат част от регистър. Така например един каталог в хартиен вид на документи, поддържани в същия вид, вече представлява регистър, поради което се прилагат изискванията за защита на личните данни. Това означава, че тази защита се разпростира и над бази данни, които са създадени преди повече време и не са били дигитализирани.

Регламентът се прилага за обработването на лични данни на територията на Европейския съюз (ЕС), както и в случаите, когато администраторът, който обработва данните, е установен на територия извън съюза, но на място, където се прилага правото на държава член на ЕС по силата на международното право. Такива са например някои отвъдморски територии, в които се прилага отчасти или изцяло правото на държава член на ЕС.

[3] В текста на Регламента, както и на отменената с него Директива на английски език се използва изразът "filing system", т.е. „файлова система", който е преведен на български език като „регистър".

От съществено значение е, че Регламентът се прилага, дори и само една от операциите по обработването да е на територията на ЕС. Така например, ако съществената част от тези операции се извършват в държава извън територията на ЕС, но данните се споделят с някой на територията на ЕС или се обработват по възлагане от организация на територията на ЕС, то вече е приложима регламентацията на ЕС относно защитата на данните.

3. КАКВО Е ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ?

Обработването на лични данни обхваща широк кръг от операции с тях. Тук попада тяхното събиране, записване и използване, както и предаването им на други организации или хора или публичното им разкриване. Простият факт на съхранението на данните обаче също се смята за обработване. Дори унищожаването на лични данни е форма на обработването им. Операции като промяна, адаптиране, както и подреждане, организиране, структуриране на лични данни също попадат в тази категория.

Специфична форма на обработване е т.нар. **„профилиране“**, при което личните данни се използват с цел оценка, анализ, прогноза на изпълнението на професионални – трудови или служебни задължения, икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение. Профилирането е необходимо, за да се извършват адекватни действия по оценка и прогноза. Същевременно то е и потенциален източник на злоупотреби и нарушения, като рискът е валиден особено за случаите, когато се вземат решения по отношение на даден човек само или главно на основата на такова автоматизирано обработване на неговите лични данни. Иначе профилирането и вземането на решения само на основата на автоматизирано обработване е рутинна процедура – например при отпускане на т.нар. „бързи кредити“.

Много лични данни се съдържат в публични регистри, достъпът до които е свободен. Обработването обаче на такива данни по несъвместим с Регламента начин може да доведе до нарушение и съответни санкции.

4. РОЛИТЕ В ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Отношенията, които възникват по отношение на работата с лични данни и защитата им в този процес, предполагат различни участници:

- **човекът, за когото се отнасят данните е „субект на данните“;**
- **администраторът;**

- **длъжностното лице по защита на данните;**
- **трета страна;**
- **държавен орган по надзор.**

4.1. СУБЕКТ НА ДАННИТЕ

Субект на данните е човекът, за когото се отнасят данните. Следователно субект на данните може да бъде само физическо, но не и юридическо лице. В този смисъл търговско дружество, фондация, сдружение, политическа партия или държавно учреждение не могат да бъдат субекти на данните.

Всяко човешко същество, за което се отнасят определени лични данни, е субект на защитата на данните. Правото на защита на личните данни не е ограничено само до гражданите или постоянно пребиваващите в дадена държава член на ЕС. Обратно, подобно на правото на достъп до обществена информация, то се отнася до всеки, независимо от неговото гражданство, пребиваване, местонахождение. **Право на защита на личните данни имат и лицата без гражданство.** Достатъчно е да става въпрос за обработване на отнасящи се до тях данни на територията на ЕС или територия, на която се прилага правото на държава член на ЕС.

Правата на субекта на данни съществуват независимо от възрастта му. В случаите, когато става въпрос за малолетно дете, правата му се упражняват от родителите или настойниците, съгласно разпоредбите на Семейния кодекс. Според Регламента при възраст над 16 години човек вече може самостоятелно да упражнява правата си, свързани със защитата на личните данни. Националният закон може да предвиди и по-ниска възраст. Според българското законодателство младежите между 14 и 18 години могат самостоятелно да вземат решения по въпроси, които ги засягат, но със съгласието на родител или настойник.

4.2. АДМИНИСТРАТОР

Като „администратор“ се обозначава този, който носи основната отговорност за събирането, съхранението, използването и другите начини на обработване на лични данни. Администраторът задължително определя на предварителен етап целите и средствата за обработването на лични данни. Най-често администраторът на лични данни е юридическо лице – неправителствена организация, търговско дружество, политическа партия и др., както и публична институция. В определени случаи администратор може да бъде и физическо лице, което изпълнява определена професия или се занимава с определена дейност – едноличен търговец, лекар, зъболекар, нотариус, адвокат и др.

Целите трябва да са ясно определени и документирани от страна на самия администратор. Също така администраторът следва да разполага със система от мерки за изпълнение на задълженията по Регламента, които съответстват на правата на хората, за които се отнасят личните данни. Т.е. той трябва да е определил политиката си за обработване на лични данни, да е информирал хората за какви цели обработва техните данни, за какъв период ги съхранява, какви са правата им, пред кого могат да отправят жалба.

Например: Работодателят е администратор на обработваните за целите на трудовото, осигурителното и данъчното право данни на работниците и служителите в дадената организация. Министерството на вътрешните работи е администратор по отношение на данните, събирани за целите на полицейската регистрация. Болницата е администратор по отношение на данните, събирани за целите на здравното обслужване на пациентите. Училището е администратор по отношение на данните на записаните в него ученици.

4.3. ОБРАБОТВАЩ

Често пъти администраторът не обработва самостоятелно личните данни. В много случаи **друго лице – било то човек специалист или организация, извършва цялостната обработка или част от нея от името на администратора**. Така например базите данни и интернет страницата на дадена фирма, неправителствена организация или държавно учреждение се поддържа от IT-специалист или фирма. Този човек или фирма се обозначава като „обработващ“. Основната разлика с администратора е, че обработващият не определя самостоятелно целите и средствата на обработването на лични данни, а по възлагане от администратора. По тази причина и използването на данните, и резултатът от това използване не са в полза на обработващия, а за администратора. Обработващият носи самостоятелна отговорност за спазването на изискванията, свързани с обработваните от него лични данни.

4.4. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Длъжностно лице по защита на данните следва да се назначи само от определени администратори в определени случаи. Ролята на този служител е определена в Регламента и се изразява в дейност по консултиране и подпомагане на администратора в хода на извършваното от него обработване на лични данни.

Задължение за назначаване на длъжностно лице по защита на данните имат публичните институции. На следващо място – длъжни да назна-

чат такъв служител са организации и учреждения, чиито основни дейности предполагат редовно и систематично мащабно наблюдение на определени хора.

Какъв е обхватът на наблюдението, за да се приеме за „мащабно“, се определя от националния закон. Когато основните дейности на администратора се състоят в мащабно обработване на „чувствителни данни“, в това число свързани с присъди и нарушения, тогава също е необходимо да се прибегне до назначаването на такъв служител. Същите задължения са налице и за обработващи лични данни, т.е. не администратори, чиято работа попада във втората и третата категория.

Например: В рамките на периодичното преброяване на населението и други изследвания на органите на Националния статистически институт се събират и обработват голямо количество чувствителни лични данни, свързани с етнически произход, религиозни убеждения, здравословно състояние, които изискват задължителното назначение на длъжностно лице по защита на данните.

4.5. ТРЕТА СТРАНА

Като трета страна в процеса на обработването на лични данни се обозначава дадено физическо, юридическо лице или публична институция, което има връзка с този процес, но не е нито субект на данните, нито администратор, нито обработващ, нито лице, на което е възложено от администратора да обработва данните. Типична трета страна са например органите на Националния осигурителен институт и Националната агенция по приходите, на които регулярно дадена организация изпраща данни, свързани с получения доход от служителите и с плащането на осигуровките и определянето на данъчните задължения на служителите. В тези случаи НОИ или съответно НАП се явяват трета страна. Те са различни от субекта на данните, който е служител в организацията, и от самата организация, която се явява работодател и администратор на данните. Различни са и от счетоводната фирма, която евентуално е обработващ данните по възлагане от организацията работодател. В случаите, когато основанието за предоставяне на лични данни е съгласие на субекта на данните, това съгласие трябва да обхваща и получателите на данните, които са трети страни. От друга страна, при обработване на лични данни на основание легитимен интерес, този интерес може да е на администратора, но може и да е на трета страна. Всички държавни органи, на които трябва по силата на закон да се предоставят лични данни, както и фирми или физически лица, които на основата на договор в изпълнение на законови задължения получават такива данни, като например службите по трудова медицина, са трети страни.

4.6. НАДЗОРЕН ОРГАН

Функцията на надзорен орган по защитата на личните данни у нас се изпълнява от **Комисията за защита на личните данни**. Тя има контролни правомощия по отношение на тематиката, свързана със защитата на личните данни и спазването на изискванията на Регламента и на Закона за защита на личните данни. В изпълнение на тези правомощия тя може да издава указания, да извършва проверки, да отправя предписания и да налага санкции.

5. ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Водещи са принципите за законност, добросъвестност и прозрачност при обработването на данните. Прозрачността предполага откритост към хората, чиито данни се обработват от дадения администратор, който трябва да е подготвил и публикувал кратко разяснение по тези въпроси. Друг принцип е свързан с целта на обработването, която трябва да е предварително определена, конкретна, а не обща, и легитимна. Данните не могат да се обработват след постигане на целта по начин, несъвместим с нея. Освен това те трябва да бъдат обработвани по начин, съразмерен на постигането на целта – принцип на пропорционалност. Точност и актуалност на съхраняваните данни в поддържаните масиви е също важен принцип, който е свързан със задължението при поискване данните да се коригират и актуализират, ако това е съвместимо с изпълнението на целите, или неточните данни да се изтрият и то своевременно.

На принципите кореспондират правата на субектите на данни и съответните задължения на администраторите. След влизане в сила на Регламента, администраторите следва да се отнасят отговорно към събираните и използвани лични данни, както и да са прозрачни и открити по отношение на целите на използване към хората, за които те се отнасят.

6. КОГА МОГА ДА ОБРАБОТВАМ ЛИЧНИ ДАННИ СПОРЕД ЗАКОНА?

Администратор ли съм или обработващ? Първо трябва да определите в каква роля обработвате личните данни – като администратор или като обработващ. Администраторът определя целите и средствата за обработването на лични данни**.** Администраторът трябва предварително или най-късно в момента на събирането да е определил законовото основание, на което личните данни биват събирани. Това значи, че обработващият не

се нагърбва с тези задачи. Ако някой изисква от Вас или Ви възлага да обработвате лични данни, тогава вероятно сте само обработващ лични данни (вж. повече в *предходния Раздел 4*).

Внимание! ***Обработващият*** **обработва лични данни само по задължение, възложено му от администратора, т.е. на основание изпълнение на договор (вж. 6.1.Б по-долу). Целите и средствата за обработване, включително начините на събиране, използване, съхранение и т.н. на личните данни, са винаги определени от** ***администратора*****.**

Цел срещу законово основание – винаги трябва ясно да можете да разграничите целта от законовото основание за обработване. Администраторът определя целта на обработване на личните данни съобразно спецификата на дейността си. Целта отговаря на въпроса: „Защо, за какво ми е нужно да събирам, съхранявам или използвам нечии данни?“. Целите трябва да се вписват в някое от правните основания за обработване на лични данни. Правното основание съответства на определената от закона възможност за администратора да обработва лични данни. Правното основание отговаря на въпроса: „В кой случай, според коя разпоредба на закона мога да обработвам лични данни?“

Понякога е възможно целта да съвпадне с основанието за обработване (законово задължение, защита на жизненоважни интереси и задача от обществен интерес), както ще видим по-долу.

Конкретните цели, за които се обработват лични данни, трябва да бъдат **ясни, законни и определени най-късно към момента на събирането на личните данни**. Ако сте администратор, винаги трябва да сте определили предварително на кое правно основание или основания от Регламента събирате личните данни във всеки отделен случай. Можете да определите няколко правни основания за обработване дори по една цел.

В някои случаи е законно след като сте събрали и обработвали лични данни на едно законово основание (напр. съгласие или изпълнение на договор), да продължите да ги обработвате за друга предвидима цел на друго законово основание – законово задължение, защита на жизненоважни интереси на субекта на данните, задача от обществен интерес или легитимен интерес. Например изпълнили сте договор с даден клиент, като за целите на договора сте събрали данните за контакт на клиента. След приключването на договора (и стига клиентът вече да не е изразил несъгласие!) можете да продължите да използвате данните за контакт на бившия клиент с цел да го информирате за Ваши следващи инициативи, продукти или услуги.

Внимание! Всички ***правни основания*** **са алтернативни и равнопоставени. Те нямат йерархична зависимост помежду си. Едно правно основание не се налага, не е по-силно от другите. Но някои** ***правни основания*** **могат да бъдат по-лесно защитими от други. Наличието на което и да е от тях прави обработването законосъобразно, при условие че са спазени и другите изисквания на Регламента.**

6.1. ПРАВНИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Правните основания за обработване на лични данни според чл. 6 от Регламента са шест:

а) съгласие:

б) изпълнение на договор:

в) законово задължение за администратора;

г) защита на жизненоважните интереси на субекта на данните;

д) задача от обществен интерес или при упражняването на официални правомощия на администратора;

е) легитимни интереси на администратора или на трета страна.

Националното право може да конкретизира тези основания и да създава нови в рамките на законови задължения, задачи от обществен интерес или при възлагането на официални правомощия на администратора, както и в рамките на уточняването на легитимните интереси на администратора или на третите страни.

А. Съгласие

Внимание! Съгласието не е най-често използваното основание за обработване. Винаги, когато смятате, че би се наложило да поискате съгласие за обработването на лични данни, проверявайте дали не е налице друго правно основание за обработване като например законово задължение или договор. Винаги когато смятате, че трябва да обработвате лични данни на основание съгласие, помислете какви биха били последиците, ако лицето оттегли съгласието си.

Съгласието трябва да бъде дадено свободно, за конкретните цели на обработването, информирано, недвусмислено и трябва да бъде документирано. Съгласие за обработване на личните му данни може да даде всяко дееспособно лице (над 18 години и не поставено под запрещение).

Съгласието трябва да бъде **дадено свободно**. То трябва да представлява свободно изразяване на съзнателен избор. Наличието на свободно съгласие е валидно, само „ако субектът на данните е в състояние да упражни реален избор и не съществува риск от измама, сплашване, принуда или значителни отрицателни последици, ако той не се съгласи“[4].

Например: При трудови правоотношения или при предоставянето на административни и социални услуги е налице очевидна неравнопоставеност между субекта на данните и администратора. В тези случаи субектът няма да може да оттегли съгласието си без неблагоприятни за него последици като частично или цялостно спиране на изпълняване на договора или спиране на предоставяне-

[4] Article 29 Working Party (2011), Opinion 15/2011 on the notion of consent, WP 187, Brussels, 13 July 2011, p. 12

то на съответните административни услуги (съображение 43). В тези случаи липсва свободен избор и даденото съгласие не може да бъде смятано за свободно. Администраторът трябва да потърси друго законово основание за обработването на лични данни.

Съгласието трябва бъде **информирано**. Информацията трябва да бъде в разбираема и лесно достъпна форма, на ясен и прост език, без жаргон. Ако се използва декларация за съгласие, тя не трябва да съдържа неравноправни клаузи (съображение 42).

Минималната информация, която администратор предоставя при събирането на съгласие за обработване на лични данни, е следната:

- кой е администраторът – идентификационните данни и координати, длъжностното лице за защита на личните данни и координатите за връзка, ако има такова лице?
- какви са конкретните цели на всяко отделно обработване?
- какви данни (категории данни) ще бъдат събрани и използвани?
- правото на субекта да оттегли съгласието си;
- ще бъде ли информацията използвана за автоматизирано взимане на решения и/или профилиране?
- ще бъде ли информацията предавана на трети страни?[5]

Съгласието трябва да бъде дадено за **конкретните цели** на обработването. Това означава, че субектът може да даде едно съгласие за няколко конкретни цели на обработването, но всяка една от целите трябва да бъде посочена поотделно, т.е. конкретно. Това е нужно, за да може субектът да бъде достатъчно информиран и за да могат да се определят разумните му очаквания за бъдещото обработване на неговите данни. Най-накрая задължителното посочване на всяка отделна конкретна цел дава възможност на субекта на данните да даде съгласието си за някои цели и да го откаже или оттегли за други.

Съгласие трябва да бъде дадено **недвусмислено**. Това означава, че трябва да бъде дадено с активно действие – било то *кликване*, подпис или дори изречено устно. Не трябва да има съмнение, че съгласието е дадено. Бездействието не може да бъде смятано за недвусмислено съгласие. Изречения, публикувани на интернет страницата, от рода на „като използвате нашите услуги (като посещавате нашата страница), вие се съгласявате да обработваме вашите лични данни“ не са достатъчни за получаването на недвусмислено съгласие.

Съгласието трябва да бъде **документирано**. Администраторът, съответно обработващия лични данни, трябва да може да докаже кога и под каква форма е получил съгласието за обработване на лични данни. Макар и

[5] Article 29 Working Party (2011), Opinion 15/2011 on the notion of consent, WP 187, Brussels, 13 July 2011, p. 12

това да не е изрично посочено в нормативната уредба, администраторът трябва да може да докаже и каква информация е предоставил на субекта на данни при получаването на съгласието за обработване. Няма изисквания как тази документация трябва да бъде създавана и съхранявана. Това може да бъде отделен хартиен или електронен регистър, могат да бъдат отделни приложения (бланки) към регистъра на обработвания по чл. 30 от Регламента или могат да бъдат писма с изразени съгласия, пратени и съхранявани в електронната поща.

Б. Договор

Това правно основание ще бъде използвано в два най-общи случая.

Първо, администраторът ще го използва преди сключването на самия договор, когато обработва лични данни на лице, което е поискало да сключи договор с администратора. Това включва всички действия преди сключването като оформяне на оферта, събиране, изготвяне и проверки на документите, нужни за договора. Целта на обработването на личните данни ще бъде редовното, т.е. законосъобразното, сключване на договор. Администраторът няма право на това основание да изисква предоставянето или въобще да обработва повече лични данни, от колкото са му нужни за редовното сключване на конкретния договор.

Във втория случай администраторът ще обработва лични данни, когато това е необходимо за изпълнението на предмета и целите на договор между него и субекта на данните. Тогава целта или целите на обработването на данните ще бъдат определени в самия договор. Това правно основание е приложимо за всеки договор, по който едната страна е физическо лице.

Дадена организация (администратор) сключва договори за предоставяне на определена социална услуга с клиентите си – физически лица. В този случай целта на организацията (администратора) ще бъде тя да предоставя услугата си и за това вероятно ще е необходимо да използва имената, личните адреси за кореспонденция, електронните пощи и/или телефонните номера на клиентите. Стига организацията (администраторът) да ограничи използваните лични данни само до единствено необходимите ѝ за предоставяне на услугата, тогава правното основание за обработването на лични данни ще бъде „необходимост за изпълнението на договор".

В текста на договора между администратора и субекта на данните могат да бъдат изрично определени и срокът на съхранение, начините на обработване, техническите и организационни мерки за защита на личните данни и всички останали условия за обработването. Ако подобни разпоредби не са включени в договора, тогава администраторът ще трябва сам да ги определи, водейки се от това дали обработването на лични данни е необходимо за предмета, целите и срока на изпълнение на самия договор.

В. Законово задължение

На това правно основание администраторът ще обработва лични данни, когато това е необходимо за спазването на негово конкретно законово задължение. Законът определя най-малко целта на обработването, начина на определяне на администратора на лични данни, вида данни, които подлежат на обработване, съответните субекти на лични данни, органите, пред които могат да бъдат разкривани лични данни, периода на съхранение. В допълнение съответното законово задължение може да добави и други мерки за гарантиране на законосъобразното и добросъвестно обработване. Един закон може да даде основания за няколко различни видове обработвания на лични данни.

Например: Работодателите ще трябва да събират, съхраняват, създават нови масиви от данни (като ведомостите) и да изпращат лични данни на Националния осигурителен институт и на Националната агенция за приходите на основание на задълженията им по данъчното и осигурително законодателство.

Г. Защита на жизненоважни интереси

Обработването на лични данни ще бъде законосъобразно и когато е необходимо, за да се защити интерес от първостепенно значение за живота на субекта на данните или на друго физическо лице. Това законово основание ще бъде използвано много рядко. Първо, то би послужило за законосъобразното обработване на лични данни, само ако друго правно основание не е налично. Второ, **най-вероятните случаи на приложение са при нужда от спешни животоспасяващи мерки, когато субектът на данните не е в състояние да изрази своето съгласие**. В останалите случаи на обработване на лични данни това основание по-вероятно ще се комбинира със съгласие при оказване на медицинска помощ на един или малък брой субекти или със задача от обществен интерес, когато обработването е необходимо за хуманитарни цели, включително за наблюдение на епидемии и тяхното разпространение или при спешни хуманитарни ситуации – по-специално в случай на природни или причинени от човека бедствия.

Д. Задача от обществен интерес

За неправителствените организации често пъти това е важно основание за обработване на лични данни, свързано с изпълнението на задача от обществен интерес. За разлика от държавните органи, които събират и използват лични данни при упражняването на официални правомощия, неправителствените организации не изпълняват пряко задачи, възложени от закона. Същевременно обаче в рамките на определените от своите устави цели и за изпълнение на определената в мисията си дейност те събират и използват лични данни. Така например социалните услуги често пъти се извършват с посредничеството на или изцяло от фондации или сдружения. **Неправителствени организации работят в сферите на образованието,**

здравеопазването, превенцията на заболявания и др. Те съответно обработват лични данни за постигането на задача от обществен интерес.

Ето защо е необходимо те да са събрали предварително и да поддържат собствен масив със съответните лични данни, отразяващи осъществената от тях дейност по отношение на съответните хора, които подлежат на такива услуги. В редица случаи тези данни са получени от официални бази данни, съхранявани от държавни институции. За да отговаря на изискването на Регламента, задачата от обществен интерес не е необходимо да е изрично описана в закон, но следва да има основанието си в закон. Така например предоставянето на социални услуги от организации, различни от публичните институции, е предвидено като възможност в Закона за социалното подпомагане.

Събирането на данни например за изграждане на профил на магистратите с цел проследяване на тяхното кариерно развитие и интегритет също може да бъде използване на публични регистри и публична информация в обществен интерес, когато е в рамките на спазването на законодателството за защита на личните данни.

Е. Легитимен интерес

Обработването на лични данни ще е законосъобразно, когато е необходимо за целите на легитимните интереси на администратора или на трета страна. Тези интереси трябва да надделяват над интересите или основните права и свободи на субекта на данните.

Правното основание „легитимен интерес“ е най-близката алтернатива на съгласието за обработване. Ако администраторът на лични данни не може да докаже, че изпълнява всички условия за събирането на съгласие за определено обработване, най-вероятно той ще се насочи към позоваването на „легитимен интерес“. Поради тази причина Регламентът въвежда много условности и ограничения, както и преценка за всеки отделен случай дали законосъобразно се обработват лични данни на основание на легитимния интерес на администратора или на трета страна.

Внимание! Това правно основание не се прилага за обработването на данни от публичните органи при изпълнението на техните задачи. Основанието е практически неприложимо и за специалните категории чувствителни лични данни (по чл. 9 от Регламента) и лични данни, свързани с присъди и нарушения (по чл. 10 от Регламента). Приложението на легитимен интерес за обработване на лични данни на деца също е максимално ограничено.

Преди да започне да обработва лични данни администраторът трябва да определи дали може да използва това правно основание за обработване на лични данни чрез специфичен **тест за пропорционалност в три стъпки**:

- **Съществува ли легитимен интерес** на администратора или на трета страна? Каква е целта на обработването? Обработването на лични данни трябва да бъде за цели на администратора, незабранени от закона?
- **Необходимост от обработването.** Администраторът или третата страна не биха могли да изпълнят легитимния си интерес, ако не обработват конкретните лични данни. Обаче, ако администраторът или третата страна обработват повече лични данни или повече категории лични данни от строго необходимото за постигането на целта им, тогава не биха имали право да използват това правно основание за обработване;
- Преценка за **баланс на интересите**. В тази част трябва да се преценят рисковете от обработването за субекта на данните, като се вземат предвид нейните/неговите основателни очаквания и това дали се налага извършването на задължителна оценка за въздействието върху защитата на данните:
  - Какви са **категориите лични данни**, които ще се обработват?
  - Какви са **основателните очаквания** на субекта? Съществува ли определено **взаимоотношение** между администратора и субекта на данните? **По времето и в контекста на събирането на данните** субектът има ли основания да очаква, че може да се осъществи обработване на неговите лични данни за целта на въпросния легитимен интерес? Регламентът сочи няколко ситуации, в които би имало легитимен интерес:
    - субектът на данни е например **клиент, предоставя услуга** или е **подчинен** на администратора на лични данни;
    - администратори, които представляват част от **група предприятия** или институции, свързана с централен орган, могат да имат законен/легитимен интерес да предадат личните данни в рамките на групата предприятия за вътрешни административни цели, включващи обработването на лични данни на клиенти или служители.
  - Предварителна **оценка на риска**. Какво би било въздействието от обработването върху субекта на данните? Изисква ли се задължителна оценка на въздействието върху защитата на данните? **Съществува ли висок риск** за правата и свободите на физическите лица?

Администраторът трябва да покаже, че вероятността от настъпването на риска, комбинирана с тежестта от настъпването на риска за субекта на данните, отстъпва пред легитимния интерес на администратора да обработва личните данни. Съответно, при вероятност от „висок риск“ за правата и свободите на физическите лица би било изключително трудно да се докаже съществуването на разумен легитимен интерес от обработване.

Освен чрез прилагането на теста Регламентът дава примери на съществуване на легитимен интерес. В първия съществува легитимен инте-

рес, ако обработването е необходимо за целите на **предотвратяването на измами**.

Според втория може да съществува легитимен интерес, ако обработването е необходимо за целите на **директния маркетинг,** т.е. в някои случаи[6], ако администратор е получил данни за контакт с потребител по електронен път при търговска сделка за предоставяне на продукти или услуги, тогава този администратор може да използва тези данни за изпращане на съобщение за маркетинг и реклама на негови собствени сходни продукти или услуги.

Внимание! Когато обработвате лични данни за целите на директния маркетинг, трябва винаги изрично да посочвате възможността/правото на субекта да изрази несъгласие с бъдещо получаване на подобни съобщения. Ако субектът на данни възрази срещу обработване за целите на директния маркетинг, администраторът е длъжен да прекрати обработването.

Други примери от практиката за случаи на приложение на легитимен интерес на администратора или трета страна за обработване на лични данни дава Комисията за защита на личните данни: предприемането на мерки за сигурност и охрана, включително чрез видеонаблюдение; проверка на лица и регистрация на достъпа до сгради; действия за гарантиране на информационната и мрежовата сигурност; обработване на лични данни за защита на правата на администратора по съдебен или несъдебен ред, например за подаване на иск за неизпълнение на договор или за търсене на отговорност за причинени вреди[7].

6.2. ВЪПРОСИ И ОТГОВОРИ

В: Трябва ли наново да събираме съгласие за обработване на лични данни от членовете на организацията си?

О: Какви лични данни на членовете си обработвате? Ако обработвате чувствителни (специалните категории) лични данни, вижте следващия *Раздел 6.3*. Ако обработвате нечувствителни лични данни и такива, които не се свързани с присъди и нарушения, събирането на ново съгласие от членовете на организацията ви не е наложително, но трябва да ги информирате за новите правила. При присъединяването си в организацията членовете са предоставили личните си данни, нужни за дейностите на организацията, т.е. са дали своето съгласие организацията да ги обработва за целите на

[6] Разяснение ни дават чл. 13, пар. 2 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации (2002/58/ЕО) и въвеждащият я на национално ниво чл. 261, ал. 2 от Закона за електронните съобщения.

[7] Практически насоки на КЗЛД в кои случаи не е необходимо съгласие за обработване на лични данни, Комисия за защита на личните данни, https://www.cpdp.bg/index.php?p=element&aid=1163

своите дейности. Ако не можете да удовлетворите условията за доказване на законосъобразно събрано и дадено съгласие от членовете (субектите на данните), тогава можете да използвате основанието за обработване – легитимен интерес на администратора (организацията). Първо, този интерес съществува, защото организацията има нужда да обработва данните на членовете си поне за контакт, но може и за повече специфични цели в зависимост от дейностите на организацията. Второ, разбира се, трябва да ограничите съхраняваните и обработвани лични данни само до категориите, строго необходими за постигане на целите. И трето, вече съществува взаимоотношение между администратора и субектите на данните. Това е фактът на самото членуване в организацията. Оттам следва, че членовете имат основателни очаквания организацията да обработва техните лични данни за своите цели, с които те са запознати. Единственото допълнително действие, което трябва да направи организацията, е да информира членовете си за новите правила за защита на личните данни и конкретно за правата на субектите на данните, кои категории техни лични данни се обработват, какви защити се прилагат, правата на възражение и жалба и т.н.

В: Можем ли (ЮЛНЦ) да продължим да използваме адресите на електронни пощи, събрани в миналото, за да изпращаме новини и информация за нашите дейности?

О: Да, ако субектите на данните са дали съгласието си или имат основателно очакване да получават тази информация. Ако хората, които са Ви предоставили адресите си на електронна поща, са дали своето съгласие за целта да получават новини и информация за Вашата дейност, Вие сте ги информирали за правата им, можете да продължите да им изпращате информацията. Ако не можете да удовлетворите условията за доказване на законосъобразно събрано и дадено съгласие от получателите, тогава можете да използвате основанието за обработване легитимен интерес на администратора (организацията). Ако не променяте нищо в практиката си и продължавате да изпращате същите по вид новини и информация (бюлетин) за същия период от време, тогава за хората, които вече са получатели (стари абонати) има основателно очакване да продължат да получават тази информация. Разбира се, когато вътрешните Ви правила за защита на данните са подновени, трябва да информирате за това и получателите. Може да информирате еднократно получателите чрез специфично съобщение или като част от обичайните новини (бюлетин). Освен това трябва да направите тази информация леснодостъпна при търсене, така че е добре да я публикувате на видно и леснодостъпно място в интернет страницата си.

Изпращането на новини и информация за дейностите на дадена организация е вид *директен маркетинг*, така че за вас (администраторите) съществува задължението винаги, т.е. във всяко писмо, изрично да посочвате възможността/правото на субекта да изрази несъгласие с бъдещо получаване на подобни съобщения.

В: Ако мой колега (от същата организация) в професионалното си качество е получил контактна информация (визитна картичка, адрес на ел. поща) на потенциален клиент или на друг човек, мога ли аз в професионалното си качество да изпращам до този човек информация или предложения за дейността на нашата организация?

О: Да. Човекът (субектът на данните), когато е предоставил личната си информация на Вашия колега, е създал за себе си основателното очакване, че ще получи професионална информация от Вашата организация. Съответно, на основание на Вашия легитимен интерес да разпространявате информация за дейностите на Вашата организация можете да използвате контактната информация на потенциалния клиент, за да му изпратите подобна информация. Не забравяйте, че трябва ясно да посочите възможността/правото на потенциалния клиент да изрази несъгласие с бъдещото получаване на подобна информация и да възрази на всякакво бъдещо обработване на неговите лични данни.

6.3. ПРАВНИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ЧУВСТВИТЕЛНИ ЛИЧНИ ДАННИ

Регламентът ги нарича „специални категории лични данни“ – това са личните данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и генетични данни, биометрични данни, обработвани единствено за целите на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице. **Тяхното обработване е по принцип забранено.** Регламентът добавя, че обработването на снимки, стига да не е със специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице, не трябва да се смята за обработване на биометрични данни.

Изключения от това правило, т.е. основания за обработване на специалните категории лични данни, Регламентът предвижда в десет случая.

А. При изрично съгласие

Както при другите видове лични данни **съгласието трябва да бъде дадено свободно, за конкретните цели на обработването, информирано и трябва да бъде документирано. Съгласието трябва да бъде и дадено изрично**. Съгласие за обработване на личните му данни може да даде всяко дееспособно лице. Това означава, че деца – малолетни и непълнолетни – независимо от възрастта им, не могат да дадат собственото си съгласие за обработването на специалните категории техни лични данни. Само родителите или настойниците им могат да предоставят такова съгласие.

Б. Задължения и права от трудовото и осигурителното право (социалната сигурност и социалната закрила)

Администраторът на лични данни може да обработва специалните категории лични данни, ако това е необходимо за изпълнението на задълженията и упражняването на правата на администратора или на самия субект на данните, произтичащи от трудовото или осигурителното право. Конкретното основание трябва да произтича от правото на ЕС или българското трудово или осигурително право, по-конкретно в областта на социалното осигуряване и социалната защита, или съгласно колективен договор, в който се предвиждат подходящи гаранции за основните права и интересите на субекта на данните. Подобни специални категории лични данни биха били данните за здравословното състояние или за членство в синдикални организации.

В. Защита на жизненоважни интереси

Обработването на специални категории лични данни ще бъде законосъобразно, когато е необходимо да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице. Това законово основание може да бъде използвано, само когато субектът на данните е физически или юридически неспособен да даде своето съгласие.

Г. Обработване на лични данни за членове и бивши членове в хода на законните дейности на ЮЛНЦ

Това основание, т.е. изключение от общата забрана за обработване на чувствителни лични данни, се прилага за администратори, които са юридически лица с нестопанска цел, политически партии, философски обединения, вероизповедания и религиозни организации или синдикати. Администраторът може да обработва специални категории лични данни, свързани с членовете или бившите членове на тази структура или с лица, които поддържат редовни контакти с нея във връзка с нейните цели. Администраторът трябва да предостави подходящи гаранции за защита на данните, съобразени с тяхното естество, т.е. трябва да приложи по-високо ниво на защита от стандартното, което да гарантира, че личните данни не могат да бъдат разкривани без съгласието на субектите на данните. **Администраторът може да обработва специални категории лични данни, само доколкото това е за целите на определените по устава му дейности.**

Д. Чувствителни лични данни, направени обществено достояние от субекта на данните

Регламентът посочва, че личните данни трябва са направени обществено достояние по явен начин. Значението на този термин обаче не е определено в текста. Може да се предположи, че действието на субекта на данните трябва да е преднамерено. Иначе казано – субектът трябва по собствено желание да е направил данните публично достояние.

Е. Правни претенции

Това изключение от забраната за обработване на чувствителни лични данни предвижда два случая. Първо, обработването на специални категории лични данни ще е законосъобразно, ако е необходимо с цел установяване, упражняване или защита на правни претенции, независимо дали това е в рамките на съдебна, административна или друга извънсъдебна процедура. В този случай обработването трябва да е свързано с конкретна правна претенция и може да бъде извършено от всяка от страните в спора.

Във втория случай това са съдилищата, когато действат в качеството си на правораздаващи органи, и могат да обработват специални категории лични данни по повод правораздавателните си функции.

Ж. Важен обществен интерес

Регламентът предвижда и възможност за обработване на специални категории лични данни по причини от важен обществен интерес, като поставя няколко условия:

- важният обществен интерес трябва да е основан на националното право или правото на ЕС;
- обработването трябва да бъде пропорционално (достатъчно за постигане) на преследваната цел;
- обработването трябва да зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

З. Превантивна или трудова медицина, оценка на трудоспособността на служителя, медицинска диагноза, осигуряване на здравни или социални грижи или лечение, управление на услугите и системите за здравеопазване или социални грижи

За целите на всички тези дейности, свързани със системата на здравеопазването, по изключение могат да бъдат обработвани специални категории лични данни. Конкретното основание трябва да бъде идентифицирано от националното право или правото на ЕС, но може да бъде посочено и в договор с медицинско лице. Обработването на личните данни трябва да се извършва от лице, обвързано от задължение за тайна или под ръководството на професионален работник, обвързан от задължението за професионална тайна.

И. Съображения от обществен интерес в областта на общественото здраве

Регламентът определя за такива съображения защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия. Конкретното основание трябва

да бъде идентифицирано от националното право или правото на ЕС и да гарантира, че обработването ще се извършва под професионална тайна.

Й. Архивиране в обществен интерес, научни или исторически изследвания или статистически цели

Конкретното основание за приложение на това изключение трябва да бъде идентифицирано от националното право или правото на ЕС. Обработването на специалните категории лични данни трябва да бъде пропорционално на преследваната цел, да зачита същността на правото на защита на данните и да предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните. Вероятно ще се наложи по-високо ниво на мерки на техническа защита.

6.4. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ, СВЪРЗАНИ С ПРИСЪДИ И НАРУШЕНИЯ

За тези категории лични данни Регламентът също отрежда особени правила свързани с основанията за обработване. В групата на засегнатите категории лични данни влизат установените нарушения и произнесените санкции в рамките на повдигането на наказателна и административнонаказателна отговорност, както и наложените мерки за сигурност, т.е. самите наказания, мерките за неотклонение и другите мерки за процесуална принуда, в тези случаи.

И тъй като обработването на тези категории лични данни от „компетентните органи“ (полиция, прокуратура, съдилища и т.н.) не влиза в приложното поле на Регламента, тук става дума основно за обработването от частни лица. Единият вариант е обработването да се извършва под наблюдението на официален орган. Другият вариант е обработването да следва някое от основанията за обработване на „обикновени“ лични данни, като в допълнение е разрешено от конкретен правен акт на националното право или правото на ЕС, където са предвидени подходящи гаранции за правата и свободите на субектите на данни.

7. ПРАВА НА СУБЕКТА НА ДАННИТЕ

Правото на защита на личните данни има следните елементи[8]:

Защитата на физическите лица следва да се прилага за обработването на лични данни с автоматични средства, както и за ръчното им обработ-

[8] При все това, в обяснителната записка към Регламента е посочено, че правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа за пропорционалност.

ване, ако данните се съхраняват в регистър с лични данни[9].

Субектите на лични данни упражняват правата си чрез подаване на искания до администратора на данните. Администраторът следва да осигури възможност за подаване на искания по електронен път, особено когато личните данни се обработват електронно. Администраторът дължи отговор по полученото искане най-късно до един месец. Отказът на администратора да се съобрази с искането на субекта на данните следва да е мотивиран.

7.1. ПРАВО НА ИНФОРМАЦИЯ

Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни, и за начините, по които да упражняват правата си по отношение на обработването.

Информация за обработването на лични данни следва да се предоставя на субекта на данните в момента на събирането им, а когато данните са получени от друг източник – в рамките на разумен срок.

При получаване на лични данни (без значение дали данните се получават директно от субекта на данните или от друго място) администраторът е длъжен да предостави на субекта на данните следната основна информация:

- данни, идентифициращи администратора и контактна информация;
- целите на обработването, за което личните данни са предназначени;
- правното основание за обработването.

При получаване на лични данни администраторът е длъжен да предостави на субекта на данните следната допълнителна информация[10], която е необходима за добросъвестно и прозрачно обработване:

- за срока, за който ще се съхраняват данните, а ако е невъзможно – критериите за определяне на този срок;
- за правото да се изиска от администратора достъп до лични данни;
- за правото на коригиране, изтриване, ограничаване или възразяване срещу обработването на данните;
- за правото на жалба до надзорен орган;

---

[9] Досиетата или групите от досиета, които не са структурирани съгласно специфични критерии, не попадат в обхвата на Регламента. От обхвата на Регламента е изключено и обработването на лични данни от физическо лице за изцяло лична дейност, която няма връзка с професионална или търговска дейност.

[10] Тази допълнителна информация задължително се предоставя на субекта на данните и в случаите, когато администраторът възнамерява по-нататък да обработва личните данни с цел, различна от тази, за която са събрани. При по-нататъшно обработване, целите трябва да са съвместими с първоначалните.

- информация дали предоставянето на данни е задължително или договорно изискване, както и информация дали субектът на данните е длъжен да ги предостави и евентуалните последствия, ако не ги предостави;
- съществуването на автоматизирано вземане на решения, включително профилиране, логиката на обработването и последствията от него.

В определени случаи администраторът е длъжен да предостави на субекта на данните и следната информация:

- координати за връзка с длъжностно лице по защита на данните;
- получателите или категориите получатели на данните;
- законните интереси на администратора при обработване на лични данни въз основа съгласието на субекта на данните;
- правото на оттегляне на съгласието по всяко време.

Когато е налице нарушение на сигурността на личните данни и има вероятност това нарушение да породи висок риск за правата и свободите на физическите лица, администраторът (без ненужно забавяне) съобщава на субекта на данните за нарушението на сигурността.

В съобщението до субекта на данните на ясен и прост език се описва естеството на нарушението на сигурността и се посочват най-малко следната информация и мерки:

- името и контакта на длъжностното лице по защита на личните данни или друга връзка за получаване на повече информация;
- описание на евентуалните последици от нарушението;
- описание на предприетите или предложени от администратора мерки за справяне с нарушението и намаляване на евентуалните вредни последици.

Съобщение до субекта на данните не се изисква, ако данните са били криптирани или ако администраторът впоследствие е взел мерки, които гарантират, че няма вероятност да се реализира високият риск за правата и свободите на субектите на данните.

Когато администраторът е определил длъжностно лице по защита на личните данни, субектите на данни могат да се обръщат към това длъжностно лице по всички въпроси, свързани с обработването на техните лични данни и с упражняването на правата им по Регламента.

7.2. ПРАВО НА ДОСТЪП

Всеки субект на лични данни има право да получи от администратора достъп до събраните за него данни!

Когато е възможно, администраторът следва да предоставя достъп от разстояние до сигурна система, която осигурява на субекта на данните пряк достъп до неговите лични данни.

Всеки субект на лични данни има право да получи от администратора и следната информация:

- целите на обработването;
- съответните категории лични данни;
- получателите на данните;
- срока за съхранение на данните или критериите за определянето му;
- съществуването на право на коригиране, изтриване, ограничаване или възразяване срещу обработването;
- съществуването на право на жалба до надзорен орган;
- всяка налична информация за източника на данните, когато те не се събират директно от субекта;
- съществуването на автоматизирано вземане на решения, включително профилиране, логиката на обработването и последствията от него.

7.3. ПРАВО НА КОРИГИРАНЕ И ЗАЛИЧАВАНЕ

Субектът на данните има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него. Това право включва и попълването на непълни лични данни.

Субектът на данните има право да поиска от администратора да изтрие без ненужно забавяне свързаните с него лични данни, когато:

- данните повече не са необходими за целите, за които са събрани;
- субектът на данните оттегли своето съгласие и не е налице друго правно основание за обработване;
- субектът на данните възрази срещу обработването и не са налице законни основания за обработване, които да имат преимущество;
- данните са били обработвани незаконосъобразно;
- данните трябва да бъдат изтрити по силата на правно задължение;
- данните са били събрани във връзка с предлагането на услуги на информационното общество[11].

Когато администраторът е направил данните обществено достояние (в интернет), правото на изтриване следва да бъде разширено. В тези случаи администраторът е длъжен да предприеме разумни мерки за уведомяване на други администратори, които обработват данните, че субектът на данните е поискал изтриване на всички връзки и копия на тези данни.

[11] „Услуга на информационното общество“ е услуга по смисъла на Директива (ЕС) 2015/1535 на ЕП и на Съвета, установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правилата относно услугите на информационното общество.

Правото на изтриване всъщност представлява право „да бъдеш забравен“. То е особено важно, когато субектът на данните е дал съгласието си като дете[12] и не е осъзнавал напълно рисковете, свързани с обработването, а впоследствие желае да премахне такива лични данни, особено когато са в интернет.

„Правото да бъдеш забравен“ не се прилага, когато обработването на данните е необходимо за:

- упражняване на правото на свобода на изразяване и правото на информация;
- спазване на правно задължение, изпълнение на задача от обществен интерес или при упражняване на официални правомощия;
- защита на общественото здраве;
- целите на архивирането в обществен интерес, научни или исторически изследвания, статистически цели;
- установяването, упражняването или защитата на правни претенции.

7.4. ПРАВО НА ОГРАНИЧАВАНЕ

Субектът на данните има право да изиска от администратора ограничаване на обработването, когато е налице едно от следните условия:

- точността на данните се оспорва от субекта на данните;
- обработването е неправомерно, но субектът не желае изтриване на данните, а ограничаване на използването им;
- данните вече не са нужни за целите на обработването, но субектът ги изисква за установяването, упражняването или защитата на правни претенции;
- субектът на данните е възразил срещу обработването.

Методите за ограничаване на обработването на лични данни могат да включват временно преместване на данните в друга система за обработване, временно прекратяване на достъпа на ползвателите до тях или временно премахване на данните от уебсайт.

7.5. ПРАВО НА ПРЕНОСИМОСТ

Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратора, в структуриран, широко използван и машинно четим формат.

Субектът на данните има право да прехвърли тези данни на друг администратор, когато:

[12] Например при посещение на интернет сайт или регистрация за онлайн игра.

- обработването е въз основа на съгласие или договорно задължение;
- обработването се извършва автоматизирано.

Когато това е технически възможно, субектът им право да получи пряко прехвърляне на данните от един администратор към друг.

7.6. ПРАВО НА ВЪЗРАЖЕНИЕ

Когато данните се обработват за изпълнение на задача от обществен интерес и включват профилиране, субектът на данните има право на възражение срещу обработването на основания, свързани с неговата конкретна ситуация.

В тези случаи администраторът е длъжен да прекрати обработването на данни, освен ако не докаже, че:

- съществуват законови основания за обработване, които имат предимство пред правото на субекта на данните;
- данните са необходими за установяването, упражняването или защитата на правни претенции.

Когато данните се обработват за целите на директния маркетинг и включват профилиране, субектът на данните има право на възражение срещу обработването, а администраторът е длъжен да прекрати обработването за тези цели.

При обработване на данни за целите на директния маркетинг субектът на данните изрично следва да бъде уведомен за правото на възражение, което му се предоставя по ясен начин и отделно от всяка друга информация.

7.7. АВТОМАТИЗИРАНО ВЗЕМАНЕ НА ИНДИВИДУАЛНИ РЕШЕНИЯ. ПРОФИЛИРАНЕ

Субектът на данните има право да откаже автоматизирано обработване, включващо профилиране, което решение поражда правни последици за субекта и го засяга в значителна степен.

Това право включва правото на субекта на данните да изиска човешка намеса от страна на администратора (т.е. окончателното индивидуално решение да бъде взето от човек, а не от машина), както и правото на субекта да изрази гледната си точка и да оспори решението.

Това право не намира приложение, ако решението:

- е необходимо за сключването или изпълнението на договор между субекта на данните и администратора;
- е разрешено от правото на ЕС или на държава членка;
- е основано на изрично съгласие на субект на данните.

7.8. ПРАВО НА ЖАЛБА

• Обжалване пред надзорен орган

Всеки субект на лични данни има право да подаде жалба до надзорен орган, ако смята, че обработването на личните му данни нарушава разпоредбите на Регламента.

Всяка държава следва да създаде независим надзорен орган, който да отговоря за прилагането на Регламента. Една от основните функции на този орган е да разглежда жалби.

Надзорният орган е длъжен да информира жалбоподателя за напредъка и резултатите от разследването в разумен срок.

Надзорният орган е длъжен да улеснява подаването на жалбите. Например чрез формуляр за подаване на жалби, който може да бъде попълнен и по електронен път.

Производствата по разглеждане на жалбите следва да са безплатни за субектите на данните.

Когато исканията на субекта на данните са очевидно неоснователни или прекомерни[13], по-специално поради своята повторяемост, надзорният орган може да наложи разумна такса или да откаже да предприеме действия по искането.

Надзорният орган има следните правомощия, които са директно свързани с правата на субекта на данните:

- да разпорежда на администратора или на обработващия лични данни да изпълнят исканията на субекта на данни за упражняване на правата му по Регламента;
- да разпорежда на администратора да съобщава на субекта на данните за нарушения на сигурността на личните данни;
- да разпорежда коригиране, изтриване или ограничаване на обработването на лични данни.

• Съдебна защита

Надзорният орган е длъжен да информира жалбоподателите за възможността за съдебна защита, която следва да е гарантирана по силата на Регламента.

А. Защита срещу надзорен орган

Всеки субект на лични данни има право на ефективна съдебна защита срещу решение на надзорен орган със задължителен характер, отнасящо се до него.

[13] Надзорният орган носи тежестта на доказване на очевидно неоснователния или прекомерен характер на искането.

Всеки субект на лични данни има право на ефективна съдебна защита, когато надзорният орган не е разгледал жалбата или не е информирал жалбоподателя за напредъка в разглеждането ѝ в срок от три месеца.

Когато надзорният орган отхвърли жалбата, жалбоподателят може да заведе дело в съда.

Б. Защита срещу администратор или обработващ лични данни

Всеки субект на лични данни има право на ефективна съдебна защита, когато счита, че правата му по Регламента са нарушени в резултат на неправомерно обработване на личните му данни.

7.9. ПРАВО НА ОБЕЗЩЕТЕНИЕ И ОТГОВОРНОСТ ЗА ВРЕДИ

Всяко лице, претърпяло материални или нематериални вреди в резултат на нарушение на Регламента, има право да получи обезщетение от администратора или обработващия данните за нанесените вреди.

Когато в една и съща операция по обработване, причинила вреда, участват повече от един администратор или обработващ данни, всеки администратор или обработващ носи отговорност за цялата вреда, за да се гарантира действителното обезщетение на субекта на данните.

8. КАКВИ ЗАДЪЛЖИТЕЛНИ ДЕЙСТВИЯ ТРЯБВА ДА ПРЕДПРИЕМА В ПРИЛОЖЕНИЕ НА РЕГЛАМЕНТА?

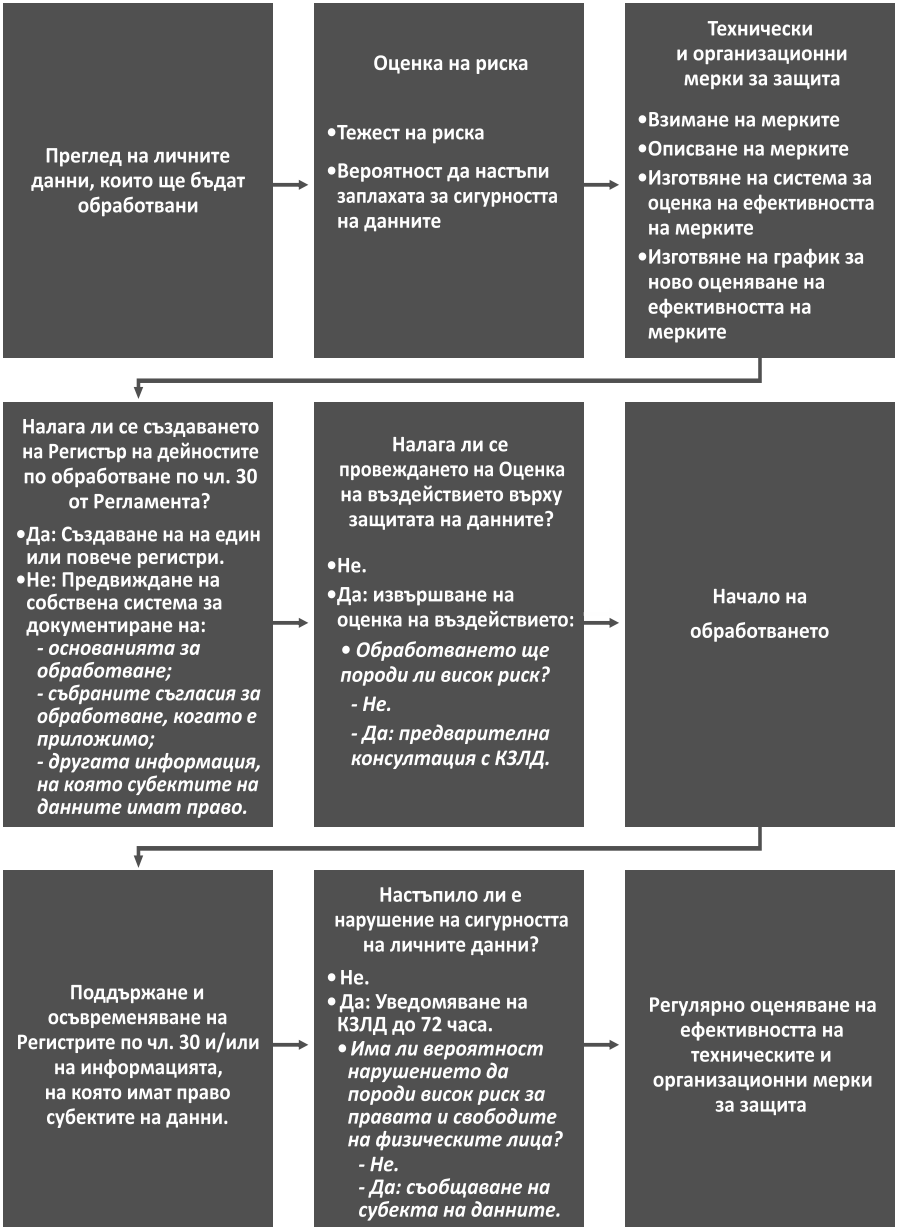
Вътрешни процедури и документи за администраторите и обработващите на лични данни

Регламентът поставя оценката на риска като водеща и предхождаща всички действия на администраторите и обработващите лични данни. Оттам следват и основните задължения за администраторите да организират процедурите на вътрешно ниво за защита на данните, което включва и сигурността чрез подходящите технически мерки, както и успоредно с това да опишат действията си по защита на данните и да могат да дадат отчет за тях.

След като разгледаме общите за всички администратори задължения по Регламента, ще преминем и към тези задължения, които се прилагат при настъпването само на определени обстоятелства.

8.1. КОНКРЕТНИ СТЪПКИ, ЗАДЪЛЖИТЕЛНИ ЗА ВСИЧКИ АДМИНИСТРАТОРИ И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Таблица 1. Хронология на предприемането на стъпките



• Преглед на данните и оценка на рисковете

Администраторите и обработващите лични данни трябва да прегледат всички категории данни, които съхраняват, събират и обработват по всякакъв друг начин. Трябва да установят **целите на обработването** за всяка категория данни, както и **правното основание**. Администраторите и обработващите лични данни трябва да направят **оценка на риска,** разглеждаща най-вероятните възможности за неразрешен достъп или изтичане на данни, за загуба или промяна.

Елементите за оценяване на риска са вероятността от настъпване на заплахата за сигурността на личните данни и тежестта на риска за правата и свободите на физическите лица. Според нивото и възможностите си[14] всеки администратор трябва да изгради за себе си система за оценка на риска. Нищо не пречи и тази система да не бъде разписана в отделен документ, а да се изразява чрез ясното предвиждане на техническите и организационни мерки за защита. Разбира се, някои администратори могат да се ориентират и към по-сложна и ясно определена система за оценка на риска като например тази, предоставяна от Агенцията за информационна сигурност на Европейския съюз (ENISA)[15].

Регламентът също така не дава ясно определение на нивата на риск. В някои случаи – при задължението за информиране на субектите на данните за нарушение на сигурността или при задължението за изготвяне на оценка на въздействие върху защитата на данните – се използва понятието „висок риск". Примери за случаи, в които би могъл да се породи „висок риск" за правата и свободите на физическите лица, са:

- обработване на лични данни за оценяване, включително профилиране и прогнози за физически лица;
- обработване на лични данни за автоматично взимане на решения с правни или подобни по важност ефекти за физическите лица;
- систематично наблюдение на физически лица;
- обработване на чувствителни или „много лични" данни;
- обработване на лични данни в голям мащаб;
- засичане или комбиниране на набори от лични данни;
- обработване на лични данни на уязвими лица;
- иновативно използване на лични данни или прилагане на нови технологични решения;

[14] Чл. 32 от ОРЗД „…достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването…"

[15] Guidelines for SMEs on the security of personal data processing, ENISA, 2017, www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

- когато самото обработване пречи на субекти да упражняват права, да използват услуга или да сключат договор.[16]

Тук трябва да се прецени нужна ли е оценка на въздействието върху защитата на някоя конкретна категория данни (вижте по-долу).

По изискването за защита на данните на етапа на проектирането и по подразбиране администраторите трябва да осигурят **свеждането на събраните данни, степента на обработването, периода на съхраняването им и тяхната достъпност до минимум**.

- **Вътрешни правила и технически мерки за сигурност на обработването**

Администраторите трябва да приложат и подходящите **технически и организационни мерки за сигурност на обработването**. Разбира се, тези мерки трябва да бъдат в разумни граници. Администраторите трябва да намерят най-подходящите и достъпни, включително като разходи, технологични и организационни решения за сигурност, които позволяват защита срещу идентифицираните рискове за данните.

Внимание: Взимането на подходящите технически и организационни мерки за защита има за цел да намали вероятността от настъпването и тежестта на риска за правата и свободите на физическите лица. Ако администраторът вземе подходящите мерки, би намалил вероятността от настъпване на риска и така би гарантирал достатъчно ниво на защита дори и за обработване на данни, пораждащо „висок риск". Важното е администраторът *предварително да е направил тази преценка* и евентуална оценка на въздействието за защитата на данните.

Подходящи **технически и организационни мерки за сигурност** могат да бъдат:

- контрол на физическия и техническия достъп до данните;
- псевдонимизация и криптиране на съхраняваните лични данни, ако е възможно;
- осигуряване на сигурността на информационните системи;
- създаване на вътрешни процедури за обработване, достъп и заличаване на личните данни;
- обучаване на служителите по защитата на личните данни и прилагането на вътрешните правила.

[16] „Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск" за целите на Регламент 2016/679", Работна група по чл. 29, https://www.cpdp.bg/userfiles/file/WP29/wp248%20rev_01_bg.pdf

Администраторите трябва да изпитат надеждността на мерките за сигурност и да предвидят **график за редовно оценяване на ефективността** им.

Регламентът не предвижда формалното създаване на вътрешни правила за администраторите и обработващите лични данни, тоест няма заложена форма, по която те да бъдат създавани. Всеки администратор и обработващ може да реши кое за него е най-подходящото решение за разписване на процедурите за обработване и защита на личните данни и как да запознае служителите си с него.

- **Описване и Регистър на дейностите по обработването**

„Картата", тоест резултатът от прегледа на данните и мерките за сигурност на обработването трябва да бъде подготвена и достъпна в писмена форма, защото хората, субекти на данните, имат право и могат да поискат достъп до тази информация. Достъп до тази информация трябва да бъде осигурен и за проверки от надзорния орган (Комисията за защита на личните данни) или от администратора, ако става дума за „карта", изготвена от обработващ или от съвместен администратор. Всъщност това е и информацията, която трябва да бъде включена в Регистъра на дейностите по обработването (по чл. 30 от Регламента). Разбира се, някои администратори на лични данни нямат задължение да съставят формално такъв регистър, но това не означава, че не трябва да подготвят и да имат налична информацията, която иначе би била включена в него.

Съответно изглежда най-простото решение е всеки администратор и обработващ лични данни да състави за себе си подобен документ или да включи описанието към „вътрешните си правила". Отделно може да реши дали да го нарече **„Регистър на дейностите по обработването по чл. 30 от Регламента"** в зависимост от това дали е длъжен или не да състави такъв.

Администраторският регистър на дейностите по обработването включва:

- името и координатите за връзка на администратора (на съвместните администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива);
- целите на обработването;
- категориите субекти на данни;
- категориите лични данни;
- категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации, ако данните биват изпращани;
- когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на

предаване на данни (посочено в член 49, параграф 1, втора алинея) – документация за подходящите гаранции;

- когато е възможно – предвидени срокове за изтриване на различните категории данни;
- когато е възможно – общо описание на техническите и организационни мерки за сигурност.

Внимание! Субектите на данните имат право на информация и за правното основание, на което администраторите обработват личните им данни. Макар и „правното основание" да не е включено в задължителните категории информация за Регистъра на дейностите по обработването, администраторите трябва винаги да могат да го посочат за всяка категория обработвани лични данни.

Регистърът на дейностите по обработването на обработващ включва:

- името и координатите за връзка на обработващия или обработващите лични данни и на всеки администратор, от чието име действа обработващият лични данни и – когато това е приложимо – на представителя на администратора или обработващия лични данни и на длъжностното лице по защита на данните;
- категориите обработване, извършвано от името на всеки администратор;
- когато е приложимо – предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни (посочено в член 49, параграф 1, втора алинея) – документация за подходящите гаранции;
- когато е възможно – общо описание на техническите и организационни мерки за сигурност.

- **Интернет страницата на администратора**

Специално внимание трябва да бъде отделено на информацията за защитата на личните данни, която администраторите трябва да публикуват на интернет страниците си. Често наричана „политика за поверителност", „политика за данните", „политики за защита на данните" и др. тази информация **отговаря на правото на информация** на субектите на данни, както е описано по-горе. Причината да се публикува на интернет страниците е, че обикновено самите интернет страници автоматично събират данни за своите посетители, както и че често страниците предоставят възможност за „абониране" за някакъв вид бюлетин, новини и предложения или други механизми на директния маркетинг, използвани от администраторите на страницата или техни партньори (трети страни). Така тази информация се явява информацията, предоставяна на субектите при събирането (получаването) на данните им. Обикновено тя съдържа два компонента:

- ***бисквитки* и други проследяващи механизми, права на избор и на информация**

Практически всяка съвременна интернет страница използва различни механизми, за да „разбере" предпочитанията, действията или други данни за ползвателите си. Най-известните подобни „програмки" се наричат *бисквитки*. Те често помагат на интернет страницата да се съобрази с устройството на преглеждащия я посетител, с броя на посетителите, извличат информация за тях (като от кое място в света посещават страницата или от какъв пол и на каква възраст са), изготвят статистика и проследяват действията на посетителите. Собственикът на интернет страницата е администратор на събираните данни, а самите данни влизат в понятието лични данни. Съответно, на интернет страницата администраторът е длъжен да предостави избор на посетителите дали искат да получат *бисквитки* или не.

В същото време в „политиката си за поверителност" или в отделен лесно достъпен документ на интернет страницата си администраторът трябва да обясни какви категории лични данни събира, за какви цели и на какво правно основание, за какъв период ги обработва, дали ги изпраща на трети страни (лица – доставчици на услуги), те за какви цели обработват данните, извършва ли се профилиране, как може субектът на данните да оттегли съгласието си, пред кой надзорен орган може да подаде жалба и т.н., както е описано в *Раздел 7.1. „Право на информация".*

- **„абониране" за информационен бюлетин или други механизми на директния маркетинг**

Често интернет страниците на различни организации дават възможност на посетителите да се абонират за определена информация от организацията, било то под формата на бюлетин, на информация за отделни кампании или предложения или просто за най-новите публикации на самата страница. Моментът, в който ползвателят попълва адреса си на електронна поща в оказаното на страницата поле и натиска съответния бутон, се явява **моментът на събиране на личните му данни** (адрес на ел. поща). Съответно, администраторът на страницата трябва да предостави информацията за целите на обработването, предаването на трети страни, правата на субекта на данните, включително за правото да оттегли съгласието си и т.н., както е описано в *Раздел „Право на информация"* (по-горе) и в раздела относно събирането на информирано съгласие (*Раздел 6.1.*). Предоставянето на тази информация може да се случи чрез хипервръзка към „политиката за поверителност", в която е предварително публикувана тази информация.

8.2. ДЕЙСТВИЯ, КОИТО АДМИНИСТРАТОРЪТ ТРЯБВА ДА ПРЕДПРИЕМЕ В СПЕЦИАЛНИ СЛУЧАИ

Някои задължения за администраторите и обработващите настъпват само при определени обстоятелства. Тук ще разгледаме задълженията за уведомяване на надзорния орган и за информиране на субектите на данни при изтичане на лични данни, за изготвяне на оценка на въздействието при висок риск за данните и за осигуряване на адекватна защита на данните при изпращането им в чужбина.

- **Уведомяване на надзорния орган и съобщаване на субекта на данните за нарушение на сигурността на личните данни**

В случай на нарушение на сигурността на личните данни обработващият е длъжен да уведоми администратора, а той в срок до 72 часа да уведоми надзорния орган (КЗЛД). Администраторът може да удължи този срок, но е длъжен да посочи причините за забавянето пред надзорния орган.

Уведомлението съдържа най-малко следното:

- описание на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- името и контакта на длъжностното лице по защита на личните данни или друга връзка за получаване на повече информация;
- описание на евентуалните последици от нарушението;
- описание на предприетите или предложени от администратора мерки за справяне с нарушението и намаляване на евентуалните вредни последици.

Когато е налице нарушение на сигурността на личните данни и има **вероятност това нарушение да породи висок риск за правата и свободите на физическите лица**, администраторът (без ненужно забавяне) съобщава на субекта на данните за нарушението на сигурността. В съобщението до субекта на данните на ясен и прост език се описва естеството на нарушението на сигурността и се посочват най-малко следната информация и мерки:

- името и контактът на длъжностното лице по защита на личните данни или друга връзка за получаване на повече информация;
- описание на евентуалните последици от нарушението;
- описание на предприетите или предложени от администратора мерки за справяне с нарушението и намаляване на евентуалните вредни последици.

- **Оценка на въздействието върху защитата на личните данни**

Оценката на въздействието върху защитата на данните (ОВЗД) има за цел да опише обработването на личните данни, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от това обработване. ОВЗД оценява рисковете и определя мерки за справяне с тях. ОВЗД е важен инструмент за отчетност, тъй като помага на администраторите на лични данни не само да спазят изискванията на Регламента, но и да демонстрират, че са предприели подходящи мерки за гарантиране на спазването на Регламента[17].

ОВЗД се изисква, само когато съществува вероятност обработването да породи висок риск за правата и свободите на физическите лица. Член 35, пар. 3 от Регламента дава примери за висок риск:

- обработване с нови технологии;
- обработването може да породи висок риск за правата и свободите на физическите лица:
  - автоматично обработване и профилиране;
  - обработване на специални категории лични данни по чл. 9 или на лични данни за присъди и нарушения по член 10;
  - (видео-) наблюдение на публично достъпна зона.

Внимание! Надзорният орган (КЗЛД) на национално ниво *трябва да състави и оповести списък на видовете операции по обработване, за които се изисква оценка на въздействието*. Надзорният орган също може да състави публикува списък на операциите по обработване, за които не се изисква ОВЗД. На нивото на ЕС Европейският комитет по защита на данните може да състави оповести общи такива списъци.

Оценката на въздействието съдържа най-малко следните данни:

- операции по обработване и целите на обработването (вкл. ако има законен интерес);
- оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
- оценка на рисковете за правата и свободите на субектите на данни;
- мерките, предвидени за справяне с рисковете.

[17] Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, WP 248 rev. 01, 17/BG, Работна група за защита на личните данни по член 29, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Преди обработването на личните данни администраторът трябва да се консултира с надзорния орган, когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска (чл. 36, пар. 1 от Регламента).

- **Предаване на лични данни на трети държави или международни организации**

Регламентът се стреми да наложи на администраторите да гарантират адекватно на европейското ниво на защита, независимо къде в света изпращат лични данни за обработване. Затова предвидените възможности за предаване в трети държави са изчерпателно изброени:

- Европейската комисия е взела решение, че тази трета държава, територия или въпросната международна организация осигуряват адекватно ниво на защита. Списъкът на тези държави можете да намерите тук: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- администраторът или обработващият лични данни е предвидил **подходящи гаранции** и са налице **права на субектите на данни и ефективни правни средства за защита;**
- задължителни фирмени правила.

9. КОНТРОЛ И САНКЦИИ

Комисията за защита на личните данни е надзорен орган. Тя отговаря за наблюдението на прилагането на Регламента. Съществена част от функциите ѝ са областта на превенцията. В това отношение тя следва да осигурява информираност на обществото и разбиране по важни въпроси относно защитата на личните данни като рисковете и правилата при тяхното обработване, както и гаранциите и правата в тази връзка. Тя има ангажимент и по информирането на администраторите и обработващите относно техните задължения по Регламента. Комисията следва да консултира държавните органи в сферата на законодателната и изпълнителната власт относно правата и свободите на личността при обработването на данни. Разясняването на тези права на субектите на данни е също сред задълженията ѝ.

Комисията също насърчава приемането на кодекси за поведение в сферата на обработването на личните данни и ги одобрява, одобрява и фирмени правила за защита на личните данни и критерии за сертифициране съгласно Регламента, наблюдава областите, където може да възникне въздейст-

вие върху защитата на личните данни, като съобщителните технологии и търговските практики.

Като надзорен орган тя също така разглежда жалби на засегнати физически лица, свързани с обработването на лични данни. Процедурата, по която се осъществява тази дейност, е уредена в Закона за защита на личните данни.

Според закона жалба може да бъде подадена в едногодишен срок от узнаването на дадено нарушение на изискванията за обработване на лични данни, но не по-късно от изтичането на пет години от извършването на това нарушение.

Обичайният начин на процедиране в настоящия момент е следният: когато прецени, че подадената до нея жалба е допустима, Комисията за защита на личните данни изпраща на съответния администратор копие от жалбата заедно с приложените към нея доказателства и изисква отговор в рамките на 7 дни. Тя може да поиска и представянето на документи. Същевременно КЗЛД може да извърши и проверка на място при съответния администратор. След това обичайно определя дата на открито заседание и провежда такова с изслушването на страните.

С решението си комисията може да даде задължително предписание за спазването на закона, като укаже необходимостта от извършването или преустановяването на определени действия от страна на администратора, като може да даде и срок за това. Възможно е да наложи и санкция. Решенията на комисията, с които се налага санкция, подлежат на обжалване пред Административния съд, а неговото решение – пред Върховния административен съд, който е последна инстанция.