КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

10

ПРАКТИЧЕСКИ СТЪПКИ ЗА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ

ДЕСЕТ ПРАКТИЧЕСКИ СТЪПКИ ЗА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ

Целта на настоящия документ е да подпомогне практическото прилагане на Общия регламент относно защитата на данните (Регламент 2016/679). Той е чисто информационен, няма задължителен характер и не претендира за изчерпателност.

1. ЗАПОЗНАВАНЕ С НОВИТЕ НОРМАТИВНИ ИЗИСКВАНИЯ В ОБЛАСТТА НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

1.1. Определяне на служители или екип, които да отговарят за привеждане на дейността на дружеството или организацията – администратор на лични данни, в съответствие с новите нормативни изисквания в областта на защитата на личните данни (ръководни служители, други ключови служители в дружеството или организацията (Правен отдел, IT отдел, Човешки ресурси и др.);

1.2. Какво трябва да се познава: Регламент 2016/679 (Общ регламент относно защитата на данните), Закон за защита на личните данни (ЗЗЛД) и подзаконовите актове по прилагането му, ръководствата и насоките на Комисията за защита на личните данни (КЗЛД) и Работната група по чл. 29 (след 25.05.2018 г. – на Европейския комитет по защита на данните).

2. ВЪТРЕШЕН АНАЛИЗ НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

2.1. Какви категории лични данни и на какви категории физически лица (независимо от тяхното гражданство) се обработват:

- „обикновени" лични данни – имена, адрес, електронна поща, IP адрес и т.н.;
- единен граждански номер;
- специални (чувствителни) лични данни – данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация.

2.2. За какви конкретни цели се събират, съхраняват и обработват личните данни (трудови отношения, търговска дейност, счетоводство, реклама, законово определени цели, журналистическа дейност и т.н.).

2.3. На кого се предоставят или разкриват личните данни извън организацията:

- на публични органи (Национална агенция за приходите, Национален осигурителен институт, Министерство на вътрешните работи, съдебни органи, контролни органи, органи на местното самоуправление т.н.);
- на обработващ лични данни (физическо или юридическо лице, което обработва личните данни от името на администратора и по негово нареждане или възлагане) – счетоводна къща, IT компания поддържаща информационната система, подизпълнители по договор и др.;
- на бизнес партньори – за целите на директен маркетинг, съвместни продукти и услуги, др.

2.4. Дали се предават (трансферират) лични данни в други държави, в кои (държава членка на Европейския съюз или трета страна) и на какво правно основание

2.5. Колко време се съхраняват личните данни в организацията и как е определен този срок.

2.6. Какви мерки за сигурност се прилагат за защита на данните.

3. ПРЕЦЕНКА ДАЛИ Е НАЛИЦЕ ЗАДЪЛЖЕНИЕ ДА СЕ ОПРЕДЕЛИ ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

3.1. Задължение да определят Длъжностно лице по защита на данните имат следните администратори на лични данни (физически и юридически лица):

- публичен орган или орган на местно самоуправление;
- администратори, които извършват системно и мащабно наблюдение на субектите на данните;
- администратори, които извършват мащабно обработване на специални (чувствителни) лични данни;
- в други, предвидени в закон случаи.

3.2. Определяне на Длъжностно лице по защита на данните по един от следните алтернативни начини:

- назначаване на служител в дружеството или организацията;
- съвместяване с друга длъжност (без конфликт на интереси);
- по граждански договор с външно за организацията физическо лице.

3.3. Квалификация на Длъжностното лице по защита на данните: да има експертни познания в областта на защитата на данните - законодателство и практика.

3.4. Обучение на длъжностното лице по защита на данните:

- първоначално;
- текущо.

(Препоръчително е да се определи Длъжностно лице по защита на данните преди да се премине към следващите стъпки.)

4. УПРАВЛЕНИЕ НА РИСКА ПО ОТНОШЕНИЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

4.1. Извършване на оценка на риска на основата на:
- естеството, обхвата, контекста и целите на обработването;
- възможните рискове за правата и свободите на физическите лица и тяхната вероятност и тежест;
- последиците за правата и свободите на физическите лица.

4.2. Извършване на оценка на въздействието върху защитата на личните данни при наличие на висок риск (напр. в резултат на профилиране, мащабно обработване на специални (чувствителни) лични данни, систематично мащабно наблюдение на публично достъпна зона, нови технологии и др.).

4.3. Задължителна предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.

4.4. Избор на подходящи технически и организационни мерки, за да може да се гарантира и докаже спазване на Регламент 2016/679 и ЗЗЛД. Възможни подходящи мерки могат да бъдат:
- псевдонимизация на личните данни;
- криптиране на личните данни;
- гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;
- водене на записи (log files) на дейностите по обработване на данни в системите за автоматизирано обработване;
- обучение на служители и др.

4.5. Предприемане на мерки за защита на данните на етапа на проектирането и по подразбиране:

- на етапа на проектирането: въвеждане както към момента на определянето на средствата за обработване, така и към момента на самото обработване, на подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване;
- по подразбиране: въвеждане на подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

4.6. Евентуално присъединяване към кодекси за поведение и/или сертифициране *(незадължително)*.

5. ПРИЕМАНЕ НА ПЛАН ЗА ДЕЙСТВИЕ ЗА ВЪВЕЖДАНЕ НА ОПРЕДЕЛЕНИТЕ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

5.1. Определяне на отговорник и екип.

5.2. Определяне на срокове и етапи за изпълнение.

5.3. Осигуряване на необходими финансови, технически и човешки ресурси.

6. ПРЕГЛЕД НА ПРАВНИТЕ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ, ВКЛЮЧИТЕЛНО ВЪЗ ОСНОВА НА СЪГЛАСИЕ НА ЛИЦАТА

6.1. Преглед на използваните до момента алтернативни правни основания за обработване на лични данни:

- съгласие;
- сключване или изпълнение на договор;
- законово задължение за администратора;
- защита на жизненоважни интереси на субекта на данните или на друго физическо лице;
- изпълнение на задача от обществен интерес или упражняването на официални правомощия, предоставени на администратора;
- легитимни интереси на администратора или на трета страна, когато същите имат преимущество над интересите или основните права и свободи на субекта на данните (неприложимо за публични органи).

6.2. Преценка дали е законосъобразно и целесъобразно обработването на лични данни - да е на основание единствено съгласието на лицето. В този случай администраторът следва да е в състояние да докаже, че съгласието е:

- свободно изразено – не дадено под натиск или заплаха от неблагоприятни последици *(напр. по-висока цена на услуга)*;
- конкретно – отделно съгласие за всяка конкретно определена цел, а когато е относимо - и за конкретна категория лични данни;
- информирано – дадено на основата на пълна, точна и лесно разбираема информация;
- недвусмислено – не се извлича или предполага на основата на други изявления или действия на лицето;
- изрично изявление или ясно потвърждаващо действие – мълчанието на лицето вече не може да се приеме за съгласие.

6.3. Документиране на съгласието с цел доказване пред Комисията за защита на личните данни и съда (декларации и др.).

6.4. Осигуряване на практическа възможност на субекта на данните да оттегли по всяко време съгласието си толкова лесно, колкото го е дал.

6.5. В случай на пряко предлагане на услуги на информационното общество на дете под 14 години - избор на процедура и/или технология за удостоверяване, че съгласието е дадено или разрешено от носещия родителска отговорност за детето.

(Когато е налице правно основание за обработване на лични данни, различно от съгласието, напр. нормативно задължение или договор, администраторът не следва да дублира това основание и със съгласие на лицето).

7. ИНФОРМИРАНОСТ НА СУБЕКТИТЕ НА ДАННИТЕ И ПРОЗРАЧНОСТ НА ОБРАБОТВАНЕТО

7.1. Предоставяне на обобщена, кратка и разбираема информация чрез интернет сайта на дружеството/организацията или по друг достъпен за субектите на данни начин относно:

- идентифициране на дружеството или организацията – наименование и начин за контакт, включително с Длъжностното лице по защита на данните, ако има такова (адрес, електронна поща, телефон и т.н.);
- какви категории лични данни се събират и за какви цели се обработват;
- категориите получатели на лични данни извън дружеството или организацията, както и дали ще се предават (трансферират) данни в трети страни извън ЕС;
- срока за съхранение на данните;
- съществуването на конкретни права на субектите на данните (право на достъп, коригиране или изтриване на лични данни, ограничаване на обработването, възражение срещу обработването, преносимост на данните) и реда за упражняването им;
- правото на субектите на данни да подадат жалба до КЗЛД или до съда;
- дали предоставянето на лични данни е задължително по закон или договорно изискване, както и евентуалните последствия, ако тези данни не бъдат предоставени;
- (ако е приложимо) дали има автоматизирано вземане на решения, включително профилиране.

7.2. Информиране по подходящ начин на работниците и служителите в дружеството/организацията в случай, че работодателят:

- извършва видеонаблюдение на работното място;
- следи средствата за електронна комуникация на работното място, предоставени от дружеството/организацията (интернет, телефон, мобилен телефон), с цел предотвратяване на злоупотреби.

8. ПРАКТИЧЕСКО УПРАЖНЯВАНЕ НА ПРАВА ОТ СУБЕКТИТЕ НА ДАННИТЕ

8.1. Познаване от страна на администратора и неговите служители на правата, които Регламент 2016/679 предоставя на лицата *право на достъп* до личните данни, свързани с лицето, които се обработват от дружеството/организацията;

- *право на коригиране* или допълване на неточни или непълни лични данни;
- *право на изтриване („право да бъдеш забравен")* на лични данни, които се обработват незаконосъобразно или с отпаднало правно основание (изтекъл срок на съхранение, оттеглено съгласие, изпълнена първоначална цел, за която са били събрани и др.);
- *право на ограничаване на обработването* - при наличие на правен спор между дружеството/организацията и физическото лице до неговото решаване и/или за установяването, упражняването или защитата на правни претенции;
- *право на преносимост на данните* – ако се обработват по автоматизиран начин на основание съгласие или договор. За целта данните се предават в структуриран, широко използван и пригоден за машинно четене формат.
- Ако е технически осъществимо, прехвърлянето на данните може да стане пряко от един администратор към друг. Правото на преносимост обхваща само данни, предоставени лично от субекта на данни, както и лични данни, генерирани и събрани от неговата дейност.

- *право на възражение* - по всяко време и на основания, свързани с конкретната ситуация на лицето, при условие, че не съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или съдебен процес;
- *право да не бъде обект на изцяло автоматизирано решение, включващо профилиране*, което поражда правни последствия за субекта на данните или го засяга в значителна степен.

8.2. Разписване на вътрешни процедури за приемане, разглеждане и отговаряне *в едномесечен срок* на искания от физически лица за упражняване на правата им като субекти на лични данни и създаване на организация за прилагането им на практика.

9. УВЕДОМЯВАНЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

9.1. Приемане на вътрешна процедура и/или план за действие в случай на нарушение на сигурността на личните данни.

9.2. Определяне на отговорен служител/екип за реакция при нарушение на сигурността на личните данни, инструктаж на персонала, др.

9.3. Създаване на вътрешна организация за своевременно уведомяване на КЗЛД в срок до 72 часа от узнаването за нарушението.

10. ДОКУМЕНТИРАНЕ И ОТЧЕТНОСТ

В съответствие с принципа на отчетност всеки администратор е длъжен:
- да прилага на практика принципите за защита на личните данни, съгласно Регламент 2016/679;

и
- да удостовери и докаже, че обработването на лични данни съответства на тези принципи.

Дейностите по документиране и отчетност обхващат, като минимум, следните мерки и стъпки:

10.1. Създаване и редовно актуализиране на *вътрешен регистър* на дейностите по обработване на лични данни в дружеството/организацията със следната информация:
- името и координатите за връзка на администратора и, когато това е приложимо, на всички съвместни администратори, на представителя на администратора и на Длъжностното лице по защита на данните, ако има такива;
- целите на обработването;
- описание на категориите субекти на данни и на категориите лични данни;
- категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- когато е приложимо - предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, документация за подходящите гаранции;
- предвидените срокове за изтриване на различните категории данни;
- общо описание на техническите и организационни мерки за сигурност.

10.2. Приемане на вътрешна инструкция/правила/процедури/политика за защита на личните данни в съответното дружество/организация.

10.3. Ако е приложимо - преглед и актуализиране на договореностите с обработващите лични данни с цел включване в тях на всички задължителни реквизити съгласно чл. 28 от Общия регламент относно защитата на данните.

10.4. Ако е приложимо - преглед и при нужда актуализиране на декларациите или другите форми за документиране на съгласието на субекта на данните, когато съгласието на субекта на данните е единственото правно основание за обработване с цел привеждането му в съответствие с изискванията на чл. 4, пар. 11 от Общия регламент относно защитата на данните.

10.5. Ако е приложимо – преглед и актуализиране на правното основание за предаване (трансфер) на данни към получатели в трети страни.

КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

Комисия за защита на личните данни
бул. "Проф. Цветан Лазаров" № 2
1592 София
Електронна поща: kzld@cpdp.bg
Интернет страница: www.cpdp.bg