НСБС Българската асоциация за спедиция, транспорт и логистика

БРАНШОВА ПРЕПОРЪКА ЗА ПОВЕДЕНИЕ НА СПЕДИТОРИТЕ, ЧЛЕНОВЕ НА НСБС

ВЪВ ВРЪЗКА С РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 27 април 2016

БРАНШОВА ПРЕПОРЪКА NSBS GDPR	*На основание чл. 18 от ЗАПСП правото да ползват* **Знака „Браншова препоръка GDPR НСБС“** *принадлежи изключително на членовете на Сдружението.* *Затова ви препоръчваме да се уверите, че спедиторската или логистична фирма, която декларира, че работи по тази Обща препоръка, е член на НСБС на линк:* http://nsbs.bg/members/

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

Съдържание

I. Въведение

На 25.05.2018 г. влезе в сила **РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).** Целта на Регламента е да се хармонизира защитата на основните права и свободи на физическите лица по отношение на дейностите по обработване на данни и да се осигури свободното движение на лични данни между държавите членки, както и контролирано обработване на лични данни на европейски граждани извън рамките на ЕС.

II. Представяне

НАЦИОНАЛНО СДРУЖЕНИЕ НА БЪЛГАРСКИТЕ СПЕДИТОРИ - НСБС е национално представителна браншова организация, която представлява интересите на транспортно-спедиторския и логистичен бранш. Сдружението обединява почти всички доказани фирми, които покриват целия спектър на спедицията и логистиката.

НСБС е член на ФИАТА, Международната федерация на спедиторските асоциации и КЛЕКАТ, Европейската асоциация за спедиторски, транспортни, логистични и митнически услуги.

„Спедиторски и логистични услуги означават всички услуги отнасящи се до транспорт (унимодален или мултимодален), консолидация, складиране, обработка, пакетиране или дистрибуция на стоката, също така предоставяне на консултантски услуги свързани с тези дейности, включително по митнически и финансови въпроси, деклариране на стоките за официални нужди, осигуряване застраховка на стоката, както и събиране или осигуряване на плащане или документи свързани със стоката. Спедиторските услуги включват също и логистичните услуги, осъществявани чрез модерни информационни и комуникационни технологии свързани с превоза, обработването или складирането на стоката, т.е. цялостно управление на веригата на доставките“.[1]

III. Структура на Браншова препоръка за поведение на спедиторите, членове на НСБС

Настоящата Браншова препоръка е структурирана в пет раздела:

1. Раздел I разглежда целите, обхвата, терминологията и принципите за работа с лични данни по смисъла на Регламента;
2. Раздел II разглежда въпросите, свързани с видовете лични данни и субектите на данни;
3. Раздел III разглежда правните основания, обработването на личните данни.
4. Раздел IV разглежда въпроси, свързани с регистрите в организациите, взаимоотношенията с надзорния орган и уведомяване за нарушенията на сигурността на личните данни

[1] Официална дефиниция на FIATA и CLECAT

5. Раздел V разглежда въпросите, свързани с необходимостта от назначаване на длъжностно лице по защита на лични данни и неговите задължения.

Раздел I. Цели, обхват, терминология, принципи

I.1. Цели на Препоръката

1. да даде препоръчителна рамка за действие на организации членки на Националното сдружение на българските спедитори, както и да обобщи начини и подходи при извършването на операции по обработване на лични данни за бранша. Документът е предназначен да се използва като препоръчителна основа за изготвяне на документацията и процесите по защита на личните данни в спедиторските организации;
2. чрез приемането на препоръките от настоящия документ да се насърчи прилагането на браншови стандарт по отношение на спазването на приложимото законодателство на РБ и ЕС за защита на данните.

I.2. Обхват на Препоръката

Браншовата препоръка е насочена както към спедитори, които обработват лични данни за собствени цели самостоятелно или съвместно с техните клиенти или трети страни (администратор на данни или съвместен администратор на данни), така и към спедитори, които обработват лични данни от името на своите клиенти (обработващи на данни). Тя засяга дейността на администраторите и/или зависими от тях дружества и техните служители.

I.3. Терминология

По смисъла на Регламента (чл. 4) настоящата Браншова препоръка използва следните определения:

1) „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано;
2) „субект на данни“ е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;
3) „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

4) „регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;
5) „администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни;
6) „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;
7) „съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;
8) „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.
9) „регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип
10) „трета страна“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни
11) „надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно член 51.

I.4. Принципи, свързани с обработването на личните данни

1. Ограничаване до определена цел

1.1 Личните данни могат да се обработват само за целта, която е била определена преди събирането им. Последващите промени в целта са възможни само в ограничени случаи и изискват обосновка.

1.2 По-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели, съгласно член 89, параграф 1.

2. Законосъобразност, добросъвестност и прозрачност

2.1 Личните данни следва да се обработват законосъобразно, добросъвестно и прозрачно.

2.1.1 Законосъобразно – с идентифицирана законна основа/правно основание.

2.1.2 Добросъвестно – администраторът предоставя необходимата информация на субектите на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

2.1.3 Прозрачно – във всеки един момент администраторът е в състояние да предостави обобщена, кратка и разбираема информация по достъпен начин относно:

i. идентифициране на дружеството или организацията – наименование и начин за контакт (адрес, електронна поща, телефон и т.н.);

ii. какви категории лични данни се събират и за какви цели се обработват;

iii. категориите получатели на лични данни извън дружеството или организацията, както и дали ще се предават (трансферират) данни в трети страни извън ЕС;

iv. срока за съхранение на данните;

v. 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;

vi. правото на субектите на данни да подадат жалба до КЗЛД или до съда;

vii. дали предоставянето на лични данни е задължително по закон или договорно изискване, както и евентуалните последствия, ако тези данни не бъдат предоставени;

viii. (ако е приложимо) дали има автоматизирано вземане на решения, включително профилиране.

3. Свеждане на данните до минимум;

3.1. Личните данни, които организацията обработва, следва да са адекватни, относими, ограничени до това, което е необходимо за обработването им

спрямо съответната цел с оглед спазване на принципа на минимално необходимото.

3.2. Ръководството на организацията – спедитор следва регулярно да преглежда обработваните от нея лични данни, за да се гарантира, че те са адекватни и относими, и не са прекомерни.

4. Точност

Личните данни трябва да бъдат точни и актуални във всеки един момент и да са положени необходимите усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.

4.1 Данните, които се съхраняват от спедиторска компания в ролята ѝ на администратор, трябва да бъдат преглеждани и актуализирани при необходимост.

4.2 Задължение на субекта на данните е да декларира, че данните за съхраняване, които предава на администратора, са точни и актуални. Попълването от субекта на данни на формуляр, предназначен за администратора, трябва да включва изявление, че съдържащите се в него данни са точни към датата на подаване.

4.3 От служителите (клиентите/партньорите) се изисква да уведомяват администратора за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорност на администратора е да гарантира, че всяко уведомление относно промяната на обстоятелствата е регистрирано и се предприемат действия.

4.4 Ръководството на спедиторската компания носи отговорност да се гарантира, че са налице подходящи процедури и политики за поддържане на точност и актуалност на личните данни.

4.5 Най-малко веднъж годишно Ръководството следва да предприема действия за преглеждане на сроковете на съхранение на всички лични данни, обработвани от администратора, като се позовава на инвентаризацията на данните и да идентифицира всички данни, които вече не се изискват в контекста на регистрираната цел. Тези данни следва да бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.

4.6 Ръководството е отговорно за вземане на подходящи мерки, в случаите когато организациите на трети страни имат неточни или остарели лични данни, да ги информира, че информацията е неточна или остаряла и да не се използва за вземане на решения относно лицата, да информира съответните страни и да препраща всяка корекция на лични данни към третите страни, когато това е необходимо.

4.7 Коригиране на лични данни може да бъде осъществено и по инициатива на субекта на данни. В този случай администраторът следва да коригира или допълни неточните или непълни данни.

5. Ограничение на съхранението

Администраторът не трябва да допуска събиране на лични данни предварително и съхраняването им за потенциални бъдещи цели. Администраторът трябва да съхранява обработвани лични данни за срокове, предвидени в законодателството на страната.

5.1 Личните данни трябва да се съхраняват в такава форма, че субектът на данните да може да бъде идентифициран само толкова дълго, колкото е необходимо за обработването.

5.2 Когато личните данни се запазват след датата на обработването, те следва да бъдат съхранявани по подходящ начин (минимизирани), за да се защити самоличността на субекта на данните в случай на нарушение на сигурността на данните.

5.3 Лични данни следва да бъдат унищожавани в съответствие с одобрена процедура за унищожаване на данните, след като е преминал срокът им за съхранение.

6. Цялостност и поверителност на данните

6.1 Личните данни трябва да се обработват по начин, който гарантира подходящо ниво на сигурността им, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически и/или организационни мерки;

6.2 Личните данни се третират като поверителна информация и за опазването им са осигурени подходящи организационни и технически мерки с цел предотвратяване на неоторизиран достъп, нелегална обработка или разпространение, както и случайна загуба, промяна или унищожаване.

7. Отчетност

7.1 Регламент (ЕС) 2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност в чл. 5, пар. 2 изисква от администратора да докаже, че спазва останалите принципи и изрично заявява, че това е негова отговорност.

7.2 Администраторът трябва да доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, внедряване на подходящи технически и организационни мерки, приемане на техники по защита на данните на етапа на проектирането и защита на данните по подразбиране, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и др.

Раздел II. Лични данни, субекти на лични данни

II.1. Права на субекта на данни

1. Администраторът трябва да осигурява практическа възможност за упражняване на правата, които Регламент 2016/679 предоставя на субектите на данни:

1.1 право на достъп до личните данни, които се обработват от администратора;
1.2 право на коригиране или допълване на неточни или непълни лични данни;
1.3 право на изтриване („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.);
1.4 право на ограничаване на обработването – при наличие на правен спор между администратора и субекта на данни до неговото решаване и/или за установяването, упражняването или защитата на правни претенции;
1.5 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.
1.6 право на възражение – по всяко време и на основания, свързани с конкретната ситуация на субекта, 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;
1.7 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. Организацията следва да уведомява субектите на данни, че не прилага процедури, чрез които е възможно автоматизирано вземане на решения и профилиране;
1.8 право на жалба до надзорен орган.

Администраторът следва да има разписани вътрешни процедури за приемане, разглеждане и отговаряне в законоустановения срок на искания от физически лица за упражняване на правата им като субекти на лични данни.

II.2. Категории субекти лични данни

Спедиторите обработват лични данни най-често на следните категории субекти на лични данни:

1. Законни или упълномощени представители на юридически лица, както и техни служители;
2. Физически лица – настоящи и потенциални потребители на услугите на администратора, служители на фирми-подизпълнители, на доставчици на различни видове услуги за администратора и др.
3. Физически лица, които са или са били страна по трудови или граждански правоотношения с администратора (както и техни роднини, когато това се изисква с цел спазване на трудовото законодателство), както и кандидати за работа.

II.3. Категории лични данни, които спедиторите могат да обработват:

Категории лични данни, които могат да се обработват от спедиторите, са:

1. Имена, дата и място на раждане, ЕГН, друг личен идентификационен номер, възраст, пол;
2. Адрес, телефонен номер, данни от документ за самоличност;
3. Снимка, обучение и квалификация, информация за трудовата заетост;
4. Семейно положение, деца;
5. Здравословно и психическо състояние;
6. Финансова информация (банкови данни).
7. Онлайн идентификатор (IP идентификатор, cookies, MAC адрес и др.);
8. Електронни данни за локализиране (GSM location, GPS, др.).
9. Данни за лицето от свидетелство за съдимост и следствието, ако лицето работи във фирмата.

Категории лични данни, които нямат отношение към пряката дейност на спедиторите и е препоръчително да не се обработват:

1. Расова и етническа информация;
2. Политически убеждения;
3. Религиозни или сходни вярвания;
4. Членства в търговски или други сдружения, общества и др.;
5. Сексуален живот;
6. Синдикална принадлежност.

II.4. Предоставяне на лични данни

Администраторът следва да осигурява условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва и членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред.

Служителите трябва да бъдат предпазливи, когато от тях се поиска от трета страна да разкрият съхранявани лични данни за друго лице. Важно е да се има предвид дали разкриването на информацията е свързано или не с нуждите на дейността, извършвана от организацията.

Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от Длъжностното лице за защита на данните (където е приложимо).

Извън организацията администраторът може да предоставя данни на следните контрагенти:

1. Публични органи – НАП, НОИ, НСИ, НСлС, МВР, Прокуратура, КПКОНПИ и др.
2. На други обработващи лични данни съобразно нуждите на бизнес дейността, напр. счетоводна къща, адвокатска кантора, агенции за подбор на персонал и др.

II.5. Трансфер на данни

1. Спедитор, в ролята му на администратор на лични данни, прехвърля данни към страни извън ЕС (посочени в Регламента като „трети страни“) само при наличието на подходящо ниво на защита на основните права на субектите на данни и спазване на всички специални изисквания на Регламента.
2. Изключения: прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:
   2.1 предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
   2.2 предаването е необходимо поради важни причини от обществен интерес;
   2.3 предаването е необходимо за установяването, упражняването или защитата на правни претенции;
   2.4 предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
   2.5 предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

Раздел III. Правни основания, обработване на лични данни

III.1. Правни основания

1. Съгласие (от клиент, партньор, доставчик, служител и др.)

   1.1 Администраторът трябва да поддържа информация за данните, обработвани въз основа на съгласие на субекта, като във всеки един случай следва да докаже, че даденото съгласие е:

   1.1.1 свободно изразено – не е дадено под натиск или заплаха от неблагоприятни последици;

   1.1.2 конкретно – отделно съгласие за всяка конкретно определена цел, а когато е относимо – и за конкретна категория лични данни;

   1.1.3 информирано – дадено на основата на пълна, точна и лесно разбираема информация;

   1.1.4 недвусмислено – не се извлича или предполага на основата на други изявления или действия на лицето;

   1.1.5 изрично изявление или ясно потвърждаващо действие – не се приема за съгласие мълчанието на даден субект на данни.

   1.2 Администраторът трябва да поддържа документация (на хартия или в електронен вид) за изразено съгласие с цел доказване пред компетентните органи. Записите се съхраняват от администратора до изпълнение на целите, за които са били събрани личните данни или до изтичане на законоустановените срокове.

   1.3 Администраторът трябва да е подсигурил възможност за оттегляне на даденото съгласие по всяко време толкова лесно, колкото е дадено. Начинът на оттегляне на съгласието трябва да бъде еднакъв с начина на даване на съгласието.

2. Сключване или изпълнение на договор, вкл. трудови и граждански договори.
   В трудовите правоотношения личните данни могат да бъдат обработвани при иницииране, изпълняване и прекратяване на трудовото правоотношение. При започване на трудово правоотношение личните данни на кандидатите могат да бъдат обработвани. Ако кандидатът бъде отхвърлен, данните му трябва да бъдат заличени при спазване на определения срок на съхранение, освен ако заявителят не се е съгласил данните му да остават в архив за бъдещ процес на подбор. Необходимо е и съгласие за по-нататъшно използване на данните за кандидатстване.
   Ако в хода на процедурата за подаване на заявления е необходимо да се събере информация за кандидата от трета страна трябва да се спазват изискванията на националното законодателство. В случаи на съмнение, трябва да бъде получено съгласие от субекта на данните.

3. Законово задължение

   Администраторът може законосъобразно да обработва лични данни на това основание, когато обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора. Това са случаите, когато на администратора е вменено задължение съгласно националното законодателство или законодателството на ЕС.

4. Легитимен интерес
   Администраторът може законосъобразно да обработва лични данни, основавайки се на легитимния си интерес, при условие че интересите или основните права и свободи на съответния субект на данни нямат преимущество. За да направи преценка дали определена дейност по обработване на данни представлява легитимен интерес, администраторът трябва да извърши балансиращ тест[i], в рамките на който да бъде преценено дали интересите или основните права и свободи на съответния субект на данни нямат преимущество, като се вземат предвид основателните очаквания на субектите на данни въз основа на техните взаимоотношения с администратора. Администраторът трябва да прецени и дали субектът на данни може по времето и в контекста на събирането на данни основателно да очаква, че може да се осъществи обработване на личните данни за тази цел.

III.2. Цели на обработването

1. Основната цел на обработването на лични данни от страна на спедитор е да се осигури надеждност при изпълнение на основната му работа – **осигуряване на транспорт на стоки и товари за клиенти**. Спедиторът следва да е наясно кой изпраща, кой превозва и кой получава стоката/товара - обект на сделката. Във връзка с тази цел (изпълнението на услугата от страна на спедитора) спедиторът следва да анализира вида и обема на данните, необходими за осъществяването на конкретната услуга, както и дали спедиторът самостоятелно или по указание на клиента обработва тези данни. В зависимост от резултатите от направения анализ, спедиторът може да обработва личните данни както на основание легитимния си интерес, така и на основание задълженията си по изпълнението на спедиционния договор.
2. **Трудови отношения** – обработване на лични данни за целите за сключване на трудови и граждански договори;
3. **Счетоводно отчитане** – обработване на лични данни за целите на организацията при изнесено счетоводство;
4. **Търговска и маркетингова дейност** – обработване на лични данни за търговски и маркетингови цели;
5. **Договорни отношения с контрагенти** – обработване на лични данни за целите на договорните отношения с клиенти, доставчици, контрагенти.
6. **Доказателствена сила, с цел разграничаване на отговорности.**

III.3. Сигурност на обработването

Администраторът трябва да е осигурил съответните технически и организационни мерки за сигурност на обработваните данни, подробно описани във вътрешните правила на администратора относно защитата на данните.

Всички служители на администратора са отговорни за гарантирането на сигурността при обработването на данните, за които те отговарят и които администраторът обработва, както и че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако администраторът не е дал такива права на тази трета страна, като са сключили договор/клауза/допълнително споразумение за поверителност в зависимост от това дали са в отношения администратор-обработващ или са съвместни администратори на данни.

Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с изградените правила за контрол на достъпа.

Раздел IV. Регистри, надзорен орган, уведомяване за нарушения

IV.1. Регистри на дейностите по обработване

(1) Спедиторите в ролята им на администратори на лични данни следва да поддържат актуални и точни регистри съгласно чл. 30, ал. 1 от Регламента (регистър на дейностите по обработване).
(2) Спедиторите в ролята им на обработващи лични данни следва да поддържат актуални и точни регистри съгласно чл. 30, ал. 2 от Регламента (регистър на дейностите по обработване).

Изброените по-горе регистри могат да бъдат поддържани в електронен вид и трябва да бъдат точни и актуални във всеки един момент.

IV.2. Взаимоотношения с надзорен орган

Надзорният орган е независими публичен орган, който е отговорен за наблюдението на прилагането на Регламента с оглед защитата на основните права и свободи на физическите лица във връзка с обработването на личните им данни. В Република България надзорният орган е Комисия за защита на личните данни.

Координати:

Адрес: София 1592, бул. „Проф. Цветан Лазаров” № 2
Електронна поща: kzld@cpdp.bg **тел. 02/91-53-555**

IV.3. Уведомяване за нарушения

1. В случай на нарушение на сигурността на личните данни спедитор в роля на администратор без ненужно забавяне и когато това е осъществимо, но не по-късно от 72 часа, след като е разбрал за него, трябва да уведомява за нарушението на сигурността на личните данни КЗЛД като надзорен орган за Република България в съответствие с член 33. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.
2. Спедитор в ролята на обработващ лични данни уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.
3. В уведомлението се съдържа най-малко следното:
   - 3.1 описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
   - 3.2 посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
   - 3.3 описание на евентуалните последици от нарушението на сигурността на личните данни;
   - 3.4 описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.
4. Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.
5. Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. За тази цел администраторът поддържа регистър на нарушенията на сигурността на обработваните лични данни в съответствие с чл. 57, ал. 1, буква „ф“ от Регламента. Тази документация дава възможност на надзорния орган да провери дали е спазен член 33 от Регламента.
6. Администраторът следва да уведоми субекта на данни за нарушението на сигурността на личните му данни без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице, за да му се даде възможност да предприеме необходимите предпазни мерки.

В уведомлението следва да се посочва естеството на нарушението на сигурността на личните данни, както и да се дават препоръки на засегнатото физическо лице за това как да ограничи потенциалните неблагоприятни последици. Такива уведомления до субектите на данни следва да бъдат правени веднага, щом това е разумно осъществимо и в тясно сътрудничество с надзорния орган, като се спазват насоките, предоставени от него или от други съответни органи, като правоприлагащите органи. Така например необходимостта да се ограничи непосредственият риск от вреди би наложила незабавното уведомяване на субектите на данните, докато необходимостта от предприемането на целесъобразни мерки срещу продължаването на нарушения на сигурността на личните данни или срещу подобни нарушения би оправдало по-дълги срокове за уведомлението. (рец. 86 от Регламент 2016/679).

Раздел V. Длъжностно лице по защита на лични данни

Съгласно чл. 37 от Регламента длъжностно лице е необходимо да бъде назначено в организации, които са публични или обработват мащабно лични данни. За определяне дали една организация има задължение да назначи (или наеме външно) длъжностно лице по защита на данните се следват конкретните препоръки, дадени от КЗЛД.

[i] **Пример**

Балансиращият тест се използва за определяне на основанието „легитимен интерес“ при обработване на лични данни.

Въведение

Регламент 2016/679 урежда шест основания за законосъобразно обработване на лични данни. Едно от тях е обработване на данни в рамките на законните интереси на администратора, уредено в чл. 6, пар. 1, буква е) на Регламента: „*обработването е необходимо за целите на законните интереси, преследвани от администратора или от трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете*".

Въпросът с легитимния интерес е разгледан и в рецитал (съображение) 47 от преамбюла на Регламента: *„законните интереси на даден администратор, включително на администратор, пред когото може да бъдат разкрити лични данни, или на трета страна могат да предоставят правно основание за обработването, при условие че интересите или основните права и свободи на съответния субект на данни нямат преимущество, като се вземат предвид основателните очаквания на субектите на данни въз основа на техните взаимоотношения с администратора. Такъв законен интерес може да е налице, когато например между субекта на данни и администратора на лични данни съществува съответното определено взаимоотношение, например когато субектът на данни е клиент или подчинен на администратора на лични данни. ...“*

В духа на Регламента законният интерес на практика може да се разглежда като правно основание за обработване на данни, доколкото тази дейност е необходима, т.е. ако може разумно да се постигне същият резултат по друг, по-малко ангажиращ начин, законните интереси като основание няма да се прилагат.

Съществена част от разбирането на законния интерес е балансът между интересите на администратора и правата и свободите на субекта, т.е. това, което е необходимо с оглед на законните интереси на администратора се претегля спрямо интересите или основните права и свободи на съответното физическо лице. Резултатът от един такъв „тест за балансиране“ определя дали чл. 6, пар. 1, буква е) от Регламента може да служи за правно основание за обработването. В някои случаи този тест може да доведе до заключението, че при съпоставянето превес имат интересите и основните права на съответните физически лица и следователно обработването на основание „законни интереси“ не може да се осъществи.

Най-често срещани ситуации

Най-често срещани ситуации, в които може да възникне въпросът за законния интерес по смисъла на Регламента, представени без да се преценява дали интересите на фирмата са преди тези на субектите на данни:

- директен маркетинг и други форми на маркетинг или реклама;

- непоискани нетърговски съобщения;

- изпълнение на правни искове, включително събиране на вземания по извънсъдебен ред;

- предотвратяване на измами, злоупотреба с услуги или изпиране на пари;

- наблюдение на служители за целите на безопасността или управлението;

- схеми за подаване на сигнали за нарушения;

- физическа сигурност, сигурност на информационни технологии и мрежова сигурност;

- обработване на данни с исторически, научни или статистически цели;

- обработване на данни с учебна, преподавателска, стопанска, научна и/или изследователска цел (включително за пазарни изследвания).

Същност на теста за баланс

Последователност на дейностите за определяне на законен интерес

1. **Отхвърляне на възможността да се приложи друго правно основание.**

Въпроси:

1. Анализирано ли е наличието на друго правно основание за извършването на конкретна дейност по обработване на лични данни?
2. Достатъчно сигурно ли е дейността по обработване да се извършва на основата на договорни отношения?
3. Налице ли е законово задължение за обработване на лични данни?
4. Обработването на личните данни на субекта свързана ли е със защитата на жизненоважните му интереси, за да може тя да бъде основание?
5. Може ли дейността по обработване да се извърши на основата на изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора?

2. **Наличие на законен интерес.**

Въпроси:

1. Определена ли е целта на дейността по обработването? Каква е тя?

2. Належащо ли е обработването за постигането на специфични цели на организацията?
3. Определени ли са причините, поради които дейността по обработването на лични данни е важно за Администратора? (Защо е важно?)
4. Защо дейността по обработване е важна за трети страни, на които данните могат да бъдат разкрити (ако е приложимо)?

3. Проверка за необходимост от обработването.

Въпроси:

1. Има ли алтернативен начин за постигане на целта без разглежданата дейност по обработване на лични данни? (Необходими ли са наистина личните данни за постигането на тази цел?)

4. Определяне на условен баланс чрез преценка на преимуществото между интересите на администратора и тези на субекта.

Въпроси:

1. Субектът на данни очаква ли обработването да се осъществи?
2. Обработването добавя ли стойност към предлаганата от администратора услуга, която субектът на лични данни използва?
3. Може ли обработването да окаже отрицателно въздействие върху интересите и/или правата на субекта на лични данни?
4. Правата на субектите на лични данни по смисъла на Регламента биха ли били ограничени при обработване на личните данни?
5. Възможно ли е да се причини увреждане или страдание на субекта на лични данни, ако обработката се осъществи? А ако не се осъществи?
6. Интересите на администратора на данни ще бъдат ли засегнати, ако обработката се случи? А ако не се случи?
7. Ще бъдат ли засегнати интересите на трета страна, ако обработването бъде осъществено? А ако не бъде осъществено?
8. В интерес на субекта ли е обработването на лични данни?
9. Интересите на субекта на данни съвпадат ли с тези на администратора, който се осланя на законните си интереси за обработването?
10. Каква е връзката между субекта на данни и администратора, който извършва обработването?
11. Какво е естеството на данните, които трябва да бъдат обработени? Има ли данни от такова естество, че да е необходима специална защита по смисъла на Регламента?
12. Как са събрани личните данни – директно от субекта на данните или непряко?
13. Може ли обработването да се счита за натрапчиво или неподходящо? Може ли то да бъде възприето като такова от субекта на данни?

5. **Определяне на крайния баланс**

Въпроси:

1. Предоставено ли е на лицето уведомление за обработване и как е предоставено то? Достатъчно ясно и открито ли е по отношение на целите на обработването?
2. Може ли субектът на данни да контролира лесно дейността по обработване или да възрази лесно?
3. Може ли обхватът на обработването да бъде променен, за да се намалят/смекчат всички рискове, свързани със защитата на личните данни или евентуалните вреди?
4. Може ли да се прилагат разширени технически мерки за обработване на данните?

6. **Доказателства за спазени изисквания и гарантиране на прозрачност.**
7. **Какво се предприема, ако съответното физическо лице упражни правото си на възражение?**