



РЕПУБЛИКА БЪЛГАРИЯ
ИНСПЕКТОРАТ КЪМ ВИСШИЯ СЪДЕБЕН СЪВЕТ

гр. София 1000, ул. „Георг Вашингтон” № 17, тел.: 02 9057502, факс: 02 9057503

Изх. № ПЛД-20-20
Дата: 09.12.2020г.

А К Т

**ЗА РЕЗУЛТАТИ ОТ ИЗВЪРШЕНА ПЛАНОВА ПРОВЕРКА
ВЪЗЛОЖЕНА СЪС ЗАПОВЕД № ПЛД-20-20 ОТ 29.05.2020 Г. НА
ГЛАВНИЯ ИНСПЕКТОР НА ИВСС**

РАЙОНЕН СЪД – ПОПОВО

На основание чл. 56-58, ал. 1, във връзка с чл. 54, ал. 2 от Закона за съдебната власт (ЗСВ), във връзка с чл. 18, ал. 2 от Закона за защита на личните данни, (ЗЗЛД), обн., ДВ, бр. 17 от 26.02.2019 г., приетата Годишна програма за проверки на Инспектората към Висшия съдебен съвет (ИВСС) за 2020 г. и Заповед № ПЛД-20-20 от 29.05.2020 г. на главния инспектор на ИВСС се извърши планова проверка по документи на РС- Попово, в качеството му на администратор на лични данни по смисъла на ЗЗЛД и на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. (Регламента).

Срок за извършване - 15.06.2020 г.

СЪСТАВ НА ПРОВЕРЯВАЩИЯ ЕКИП:

ИНСПЕКТОР: Мария Нейкова

ЕКСПЕРТИ: Надежда Желева и Юлия Меранзова.

I. ЦЕЛ И ОБХВАТ НА ПРОВЕРКАТА:

Цел на проверката е да се установи дали РС- Попово, в качеството му на администратор на лични данни спазва принципа за отчетност, установен в чл. 5, § 2 от Регламент (ЕС) 2016/679 и в чл. 45, ал. 4 от ЗЗЛД по отношение на личните данни, които обработва при изпълнение на съдебните си функции.

В чл. 5, § 2 от Регламент (ЕС) 2016/679 и в чл. 45, ал. 4 от ЗЗЛД е установен нов принцип, свързан с обработването на лични данни. Според тези разпоредби администраторът носи отговорност и следва да е в състояние да докаже спазването на основните принципи за защита на личните данни. От внимателния прочит на текстовете следва, че спазването на принципа за отчетност се свежда до изпълнението на два кумулативни елемента:

1. Администраторът е длъжен да спазва и да прилага на практика всички принципи за обработване на лични данни, установени в чл. 5, § 1 от Регламент (ЕС) 2016/679 и в чл. 45, ал. 1 от ЗЗЛД (законосъобразност, добросъвестност и прозрачност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност и поверителност) чрез предприемането на подходящи и ефективни мерки, като носи отговорност за това;

2. Администраторът е длъжен да демонстрира и доказва съответствие на поведението си с посочените принципи, като поддържа и представя надлежни доказателства за тяхното изпълнение на практика.

Тези два елемента на принципа за отчетност са неразривно свързани. Наличието на първия елемент от страна на администратора – правомерно поведение, без обаче да е налице възможност за неговото доказване, е нарушение на принципа за отчетност поради липса на неговия втори елемент. А принципът на отчетност предписва, че тежестта за доказване на

съответствието с Регламент (ЕС) 2016/679 се носи единствено и само от администратора на лични данни.

Изборът на подходящи и ефективни мерки за прилагането на принципите за защита на личните данни варира във всеки конкретен случай, в зависимост от цялостния контекст на обработването, включително и от естеството на данните, техния обем, целите, дейностите по обработване, особеностите на администратора, рисковете, които обработването поражда за правата и свободите на физическите лица. Именно поради тази специфика във философията на Регламент (ЕС) 2016/679, той не съдържа изчерпателен списък от мерки, а само задава крайната цел, която администраторите следва да постигнат – защита на физическите лица. В рамките на тази цел администраторите имат пълната свобода относно избора на начини и средства по организиране на процесите по обработване на данните и дефиниране на подходящи мерки за изпълнение на задълженията, произтичащи от принципите за обработване на данни.

Конкретните мерки, които администраторите въвеждат с цел практическо изпълнение на принципите за защита на личните данни, посочени в чл. 5, § 1 от Регламент (ЕС) 2016/679 и в чл. 45, ал. 1 от ЗЗЛД, следва да бъдат от такова естество, че да постигат и доказват по убедителен начин съответствие с изискванията на Регламент (ЕС) 2016/679.

Принципът на отчетност, който предоставя свобода на администратора в преценката относно начина на изпълнение на изискванията на Регламент (ЕС) 2016/679, не може да бъде противопоставен на общата компетентност на надзорните органи в областта на защитата на личните данни. Затова следва да се има предвид, че чл. 58, § 2, б. „г” от Регламент (ЕС) 2016/679 и чл. 80, ал. 1, т. 4 от ЗЗЛД уреждат едно важно корективно правомощие на ИВСС като надзорен орган – да разпорежда на администраторите да съобразят операциите по обработване на данни с разпоредбите на Регламент (ЕС) 2016/679 и на ЗЗЛД, включително по указан от надзорния орган начин и в определен срок. Това на практика означава, че надзорният орган може да не се съобрази с направените от администратора оценка, изводи и избор на конкретни мерки за доказване на съответствие на неговите дейности по обработване на Регламент (ЕС) 2016/679.

Регламент (ЕС) 2016/679 предвижда различни инструменти, които да подпомогнат администраторите в прилагането на отчетността. Някои от тези механизми имат доброволен характер и могат да се прилагат по преценка на администратора. Такива са например придържането към одобрени кодекси на поведение или одобрени механизми за сертифициране. Други имат задължителен характер и сред тях могат да бъдат посочени: приемането и прилагането на политика за защита на личните данни от администраторите, публичното оповестяване пред субектите на данни и служителите на администратора на политиката за защита на личните данни, включително

осигуряване на прозрачност на информацията по чл. 13 и 14 от Регламент (ЕС) 2016/679 и доказване на този факт, поддържането на регистър на дейностите по обработване на лични данни на основание чл. 30 от Регламент (ЕС) 2016/679 и чл. 62 от ЗЗЛД.

На основание чл. 17, ал. 1 от ЗЗЛД, ИВСС осъществява надзор и осигурява спазването на Регламент (ЕС) 2016/679, на ЗЗЛД и на нормативните актове в областта на защитата на личните данни при обработване на лични данни от съда при изпълнение на функциите му на орган на съдебната власт, и от прокуратурата и следствените органи при изпълнение на функциите им на органи на съдебната власт за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания. В пределите на надзорните правомощия на ИВСС, при проверката ще бъдат разгледани действията и механизмите, които проверяваният съд използва, за да докаже, че спазва принципа на отчетност по отношение на личните данни, които обработва при осъществяване на правораздавателната си дейност.

Обработването на лични данни в контекста на правораздавателната дейност е специфично, защото задълженията, които съдилищата имат като администратори на лични данни, са установени в различни нормативни актове – в Регламент (ЕС) 2016/679 по отношение на гражданските дела в най-широк смисъл, и в ЗЗЛД – когато обработването се извършва за целите по чл. 42 от ЗЗЛД (при обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване). Това налага да се уточни, че принципът за отчетност по ЗЗЛД има еднакво съдържание с това по Регламент (ЕС) 2016/679, доколкото той е изискване към администраторите да спазват основните принципи за защита на правата на субектите при обработване на личните им данни и да са в състояние да го докажат. Някои от задълженията, установени спрямо съдилищата в Регламент (ЕС) 2016/679 и в ЗЗЛД са различни, като това следва от различията в естеството и целите на обработване, определени в Глава осма от ЗЗЛД, а именно, че то се осъществява за целите на наказателното преследване на престъпления. Такива са например задължението администраторът на основание чл. 54, ал. 1, т. 6 от ЗЗЛД да информира субектите на данни за възможността при отказ по чл. 54, ал. 3, по чл. 55, ал. 3 и 4 и чл. 56, ал. 6 и 7 от закона да упражни правата си чрез ИВСС; изискването в съдържанието на регистъра на дейностите, който администраторите поддържат на основание чл. 62 от ЗЗЛД, да се съдържа информация дали въз основа на данните се извършва профилиране и други.

Съвкупността от способите за отчетност по отношение на обработването на лични данни в контекста на правораздавателната дейност следва да е така

организирана, че съдилищата да са в състояние да докажат, че спазват основните принципи за защита правата на субектите, установени в Регламент (ЕС) 2016/679 и в ЗЗЛД. Това означава надлежно да бъдат документирани всички процеси по обработване на лични данни, осъществявани в контекста на правораздавателната дейност, които да дават възможност да бъде установено, че обработването на личните данни е законосъобразно, добросъвестно, прозрачно и в минимален обем за постигане на ясно определени цели, като данните се съхраняват точно и само за времето, необходимо за постигане на тези цели, а посоченото обработване е обезпечено с подходящо ниво на сигурност и защита на данните.

Цел на конкретната проверка е да бъдат разгледани представените от РС – Попово документи, за да се установи дали и в каква степен съдът е в състояние да докаже, че е предприел достатъчно и ефективни мерки, за да се гарантира, че обработването на лични данни в контекста на правораздавателната дейност се извършва при спазване на принципите и на задълженията, установени в Регламент (ЕС) 2016/679 и в ЗЗЛД. ИВСС приема, че органите на съдебната власт ще бъдат в състояние да докажат, че спазват принципа за отчетност, ако са идентифицирали естеството, обхвата и целите, за които обработват лични данни в контекста на правораздавателната дейност и са изготвили документи за предприетите от тях мерки за защита на правата на субектите поне в следните четири направления:

1. В отношенията със субектите – администраторът следва да е предприел мерки за спазване на принципа за законосъобразност, добросъвестност и прозрачност. За да бъде обработването законосъобразно по смисъла на Регламент (ЕС) 2016/679, то трябва да бъде осъществявано на някое от основанията, установени в чл. 6, § 1 от Регламент (ЕС) 2016/679 – за „обикновените“ категории лични данни, или в чл. 9, § 2 от същия – за „специалните“, а съобразно чл. 49 от ЗЗЛД – да се осъществява за изпълнение на правомощие на компетентен орган за целите по чл. 42 от закона. Доколкото в контекста на правораздавателната дейност районните съдилища обработват лични данни за изпълнение на свои правомощия или задължения, свързани с правораздаването, то тези операции се извършват на основанията, установени в приложимите към тази дейност закони като ГПК, НПК, АПК, СК и други. Затова за спазването на този аспект на принципа може да се следи индиректно от описаните обхват, цели и естеството на данните, както и от посочените основания за тяхното обработване, които администраторът е документирал. Изрично внимание следва да се обърне на **изискването за прозрачност** в отношенията със субектите на данни. Принципът за прозрачност е уреден в чл. 5, § 1, б. „а“ от Регламент (ЕС) 2016/679, но не се прилага, когато обработването се осъществява за целите по чл. 42 от ЗЗЛД. Той изисква всяка информация и комуникация във връзка с обработването на лични данни да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки.

Този принцип се отнася в особена степен за информацията, която получават субектите на данни за самоличността на администратора и целите на обработването, и за допълнителната информация, гарантираща добросъвестно и прозрачно обработване на данните по отношение на засегнатите физически лица и тяхното право да получат потвърждение и уведомление за съдържанието на свързани с тях лични данни, които се обработват. 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. Районните съдилища следва да могат да докажат, че предприемат мерки за спазване на принципа за прозрачност при обработване на лични данни по граждански дела и изпълнение на задълженията си да информират субектите на данни за личните данни, които обработват в контекста на правораздавателната си дейност на основание чл. 13 и чл. 14 от Регламент (ЕС) 2016/679. Що се отнася до обработването на лични данни за целите на чл. 42 от ЗЗЛД, съдилищата следва да предоставят на субектите информацията по чл. 54, ал. 1 от ЗЗЛД. Тези задължения обикновено се осъществяват с приемането на вътрешни правила (политика или друг акт) и публикуване на информацията на интернет сайта на съда или съобщаването ѝ на субектите по друг подходящ начин.

2. Създаване на подходящо ниво на сигурност на личните данни – на основание чл. 5, § 1, б. „е“ от Регламент (ЕС) 2016/679 и чл. 45, ал. 1, т. 6 от ЗЗЛД, администраторът е длъжен да установи подходящо ниво за защита на данните срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. По силата на чл. 24, § 1 от Регламент (ЕС) 2016/679 и чл. 59, ал. 1 от ЗЗЛД задължение на администратора е да установи в дейността си подходящи мерки за защита на данните и да ги документира. Те следва да бъдат съобразени с естеството, обхвата, целите и контекста на обработването, както и с рисковете за правата на субектите на данни. Съобразяването на мерките с рисковете, пораждащи се при обработването в контекста на правораздавателната дейност на съда се извършва при спазване изискванията на чл. 32, § 2 от Регламент (ЕС) 2016/679, респективно – чл. 66 от ЗЗЛД. Смисълът на тези разпоредби предписва при оценка на подходящото ниво на сигурност да се вземат предвид по-специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

Спазването на тези задължения от страна на съда може да бъде доказано с анализ на рисковете за правата на субектите при обработване на личните им данни в контекста на правораздавателната дейност и приемането на вътрешни правила (политика или друг акт) за техническите и организационните мерки за

защита на личните данни. В тези актове следва да се съдържат и процедури за разглеждане на жалби от субектите и за реакции при инциденти.

3. Надлежно уреждане на отношенията с надзорния орган – съгласно чл. 31 от Регламент (ЕС) 2016/679, за администраторите е установено общо задължение да сътрудничат на надзорните органи. Такова е задължението по чл. 33 от Регламент (ЕС) 2016/679, съответно по чл. 67 от ЗЗЛД, да се уведоми без забавяне надзорния орган в случай на нарушение на сигурността на личните данни. Изпълнението на това задължение може да бъде документирано в процедура за уведомяване, като тя може да има самостоятелен характер или да бъде част от друг акт на администратора.

Съгласно чл. 37, § 1, б. „а“ от Регламент (ЕС) 2016/679 и чл. 69, ал. 4 от ЗЗЛД, в контекста на правораздавателната дейност съдилищата не са длъжни да определят длъжностно лице по защита на данните. Затова в рамките на проверката няма да се следи за спазването на това задължение.

4. Изпълнение на други задължения на администратора по осигуряване на отчетност - чл. 30, § 1 от Регламент (ЕС) 2016/679 и чл. 62, ал. 1 от ЗЗЛД, съдилищата са длъжни да водят регистър на дейностите по обработване, за които отговарят. Съдържанието и формата на този регистър са определени в Регламент (ЕС) 2016/679 и в ЗЗЛД. Администраторът е длъжен да представя регистъра на надзорния орган при поискване. Регистърът на дейностите по обработването е много полезно средство за извършването на анализ на евентуални усложнения, които може да породят обработването на данни, било то планирано или съществуващо. Той улеснява извършването от администратора фактическа оценка на риска, който дейностите по обработването могат да породят по отношение на правата и свободите на физическите лица. В допълнение, по този начин се улеснява идентифицирането и въвеждането на подходящи мерки за сигурност на личните данни.

Съобразно изложеното, ако при проверката бъде установено, че проверяваният Районен съд – Попово в качеството на администратор на личните данни не е в състояние да докаже с представените документи, че е приел вътрешни правила (политика или друг акт) за спазване на принципа за прозрачност по чл. 5, § 1, т. 1 от Регламент (ЕС) 2016/679, че е публикувал информацията по чл. 13 и 14 от Регламент (ЕС) 2016/679, респективно чл. 54, ал. 1 от ЗЗЛД на интернет сайта си, не е извършил анализ на рисковете за правата на субектите при обработване на личните им данни в контекста на правораздавателната дейност и не е приел вътрешни правила (политика или друг акт) за техническите и организационните мерки за защита на личните данни, не е приел процедура за уведомяване на ИВСС в случай на нарушение на сигурността на личните данни, обработвани при правораздавателната дейност, не поддържа регистър на дейностите по обработване на лични данни, това ще бъде прието като нарушение на принципа за отчетност по чл. 5, § 2 от Регламент (ЕС) 2016/679, съответно по чл. 45, ал. 4 от ЗЗЛД. В зависимост дали

нарушението засяга дейности по обработване на лични данни за целите по Регламент (ЕС) 2016/679 или по чл. 42, ал. 1 от ЗЗЛД, по отношение на администратора ще бъде приложена принудителна административна мярка на основание чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679 или чл. 80, ал. 1, т. 4 от ЗЗЛД да приведе дейността си в съответствие с нарушените изисквания, като предприеме конкретни действия.

За тези нарушения проверяваният съд няма да бъде санкциониран с имуществена санкция, защото целта на проверките за спазване на принципа за отчетност, заложен в годишната програма на ИВСС, е да се насърчи информираността на администраторите за задълженията им по ЗЗЛД и по Регламент (ЕС) 2016/679.

В случай, че администраторът е документирал в необходимите правила и/или политики мерките и способите, чрез които осигурява защита на правата на физическите лица при обработване на личните им данни в контекста на правораздавателната дейност, но те съдържат непълноти или неточности, на администратора следва да се отправят препоръки да преразгледа приетите документи. Препоръките имат незадължителен характер, като спазването им ще бъде отчетено при евентуални бъдещи проверки на администратора.

Осигуряването на защита на физическите лица във връзка с обработването на техни лични данни е непрекъснат процес, който изисква периодичен преглед на степента на изпълнение на нормативните изисквания и ефективността на предприетите мерки за защита на правата на субектите на данни и на сигурността по обработването. Съобразно това администраторите следва да извършват периодични проверки за адекватност на въведените от тях способности за отчетност и при необходимост да ги актуализират.

II. КОНСТАТАЦИИ

На основание чл. 12, ал. 1, т. 2 и ал. 2 от Методиката за извършване на проверки по Закона за защита на личните данни от екипи на Инспектората към Висшия съдебен съвет в органите на съдебната власт (приета с Решение по протокол № 17/08.11.2019 г. на Инспектората към Висшия съдебен съвет), с писмо изх. № ПЛД-20-20/02.06.2020 г. до РС – Търговище е изпратено уведомление за предстоящата проверка, заедно с екземпляр от заповедта за извършването ѝ и въпросник по образец, изготвен от ИВСС за преценка спазването на изискванията на Регламент (ЕС) 2016/679 и на ЗЗЛД за защита на правата на физическите лица при обработване на личните им данни от съда при изпълнение на функциите му на орган на съдебната власт.

С писмо вх. № КПЛД-20-20/17.06.2020 г. в указания срок са постъпили надлежно оформен екземпляр от заповедта за проверка, попълнен въпросник и заверени преписи на следните документи:

1. Вътрешни правила за защита на личните данни в РС - Попово;

2. Заповед № 73/15.11.2019 г. на адм. ръководител на РС - Попово за утвърждаване на Вътрешни правила за защита на личните данни в РС – Попово;
3. Заповед № 74/15.11.2019 г. на адм. ръководител на РС -Попово, с която се определя длъжностно лице по защита на данните, въвежда се Регистър на дейностите по обработване на лични данни и се утвърждават видове регистри относно дейностите по обработване на лични данни в РС – Попово;
4. Регистър на дейностите по обработване на лични данни, на основание чл. 30 от ОРЗД;
5. Уведомление до КЗЛД за определено длъжностно лице по защита на данните.

1. Административна и организационна структура:

Утвърденият щат на съда е 25 души, от които председател и 3 съдии в районен съд, 1 съдия по вписванията, 1 държавен съдебен изпълнител и 19 съдебни служители. Всички щатове са заети. Към момента на извършване на проверката РС- Попово се ръководи от съдия Маринела Стефанова - „административен ръководител- председател“.

2. Организация на способите за спазване на принципа за отчетност в РС – Попово.

От отговорите от попълнения и изпратен от РС – Попово въпросник не се установява дали съдът е обособил личните данни, които обработва в контекста на правораздавателната си дейност в отделни регистри.

От отговорите във горепосочения въпросник и от Заповед № 74/15.11.2019 г. на адм. ръководител на РС – Попово се установява, че съдът е идентифицирал дейностите по обработване за целите на всеки отделен регистър с лични данни съгласно чл. 30, § 1, б. „ж“ от Регламент (ЕС) 2016/679 и е обособил шест регистъра на дейностите по обработване на данни на физическите лица:

1. Регистър „Съдебни дела“;
2. Регистър „Бюро съдимост“;
3. Регистър „Човешки ресурси“;
4. Регистър „Финансово-счетоводна дейност“;
5. Регистър „Контрагенти“;
6. Регистър „Искания по Закона за достъп до обществена информация“.

Съобразно посочените във въпросника естество, обхват и цели, за които се обработват лични данни във всеки от регистрите е видно, че в контекста на правораздавателната си дейност РС – Попово обработва лични данни в **регистър „Съдебни дела“**. Обработваните лични данни в този регистър се отнасят до следните аспекти от идентичността на физическите лица – ищци, ответници и други участници в съдебния процес. Подсъдими, жалбоподатели,

тържители, нарушители по УБДХ, молители в делата по реабилитация, в производствата във връзка с изпълнение на наказанията и искания до съда в досъдебното производство, лицата по отношение на които се иска прилагане на принудителна медицинска мярка и други участници в съдебния процес, взыскател, длъжник и други участници в изпълнителния процес.

Посочено е правното основание за обработване – ГПК, СК, ЗЗДетето, ЗЗД, ЗС, ЗГР, ЗЗДН, НПК, НК, ЗЗ, ЗБПМН, ЗЕС, ЗАНН и др.

Обработват се следните категории лични данни: име; ЕГН; месторождение; адрес; данни за лична карта; телефон; информация за номер на банкова сметка; образование; трудова дейност; психическо състояние; умствено състояние; психическо здраве; имотно състояние; финансово състояние; участие и/или притежаване на дялове или ценни книжа в други дружества, културни интереси; социален произход; расов произход; етнически произход; политически, религиозни и/или философски убеждения.

2.1. Отношения със субектите.

Със Заповед № 73/15.11.2019 г. на административния ръководител на съда са утвърдени „Вътрешни правила за защита на правата на физическите лица при обработване на техни лични данни в РС- Попово“. Правилата са публикувани на интернет страницата на съда – <https://popovo-rs.justice.bg/bg/10014> за запознаване на гражданите с предприетите от РС – Попово като администратор на лични данни мерки по защита на личните данни и тяхното обработване.

С оглед съдържанието, документът може да бъде определен като политика за прозрачност при обработване на лични данни. В правилата изрично е указано, че имат за цел в съответствие с изискванията за информираност по чл. 13 и чл. 14 от Регламент (ЕС) 2016/679 да информират обществеността за извършваните от РС – Попово дейности по обработването на лични данни, целите, за които се обработват, данните, мерките и гаранциите за защита на обработваните данни, правата и начина, по който могат да бъдат упражнени.

В съдържанието на политиката са посочени данните, които идентифицират администратора и координатите за връзка с него, съгл. чл. 13, § 1, б. „а“ от Регламент (ЕС) 2016/679. В раздел „Категории лични данни, цели и основания, на които се обработват“ от Вътрешните правила са идентифицирани целите, обхвата и естеството на различните категории дейности по обработване на личните данни – „Правораздаване“, „Контрагенти“, „Искания по закона за достъп до обществена информация“, „Посетители“. Не са идентифицирани отделните регистри с лични данни, които администраторът следва да поддържа в рамките на всяка дейност, която извършва. Не е посочено правното основание за обработване на личните данни, а именно, че същите се обработват на основание чл. 6, § 1, б. „д“ от Регламент

(ЕС) 2016/679, като не е направено разграничение, че личните данни, които се обработват за целите на наказателното преследване не попадат в материалния обхват на Регламент (ЕС) 2016/679 по силата на чл. 2, § 2, б. „г“ от Регламент (ЕС) 2016/679, а се обработват на основание чл. 49 ЗЗЛД.

В правилата е указано, че обработваните от администратора лични данни се предоставят на трети лица само когато това е предвидено в закон. Това правило се спазва и при предаването на лични данни на чужди държавни органи – те се предоставят единствено в изпълнение на задължения, произтичащи от нормативни актове (изпълнение на съдебна поръчка, договор за правна защита и др.), в съответствие с разпоредбите на Регламент (ЕС) 2016/679.

Във Вътрешните правила също така е указано, че като администратор на лични данни РС – Попово прилага принципа за ограничаване съхраняването и съхранява лични данни в периоди, подходящи за целите, за които данните се обработват, като се отчита научно-историческото и справочното им значение. В съда е утвърдена Номенклатура на делата със срокове за съхранението им, съобразно ПАС и Закона за Националния архивен фонд.

По отношение правата на физическите лица – субекти на данни във Вътрешните правила е посочено, че съгласно Регламент (ЕС) 2016/679 те имат следните права във връзка с обработване на личните им данни: право на достъп до данните; право на коригиране или изтриване на свързани със субекта лични данни; право на ограничаване на обработването; право на преносимост на данните, право на субекта да не бъде обект на изцяло автоматизирано решение и право на възражение срещу обработването – правата по чл. 15 – чл. 22 от Регламент (ЕС) 2016/679. За упражняване на изброените права във Вътрешните правила е предвидена кратка и ясна процедура.

По отношение на правото на субектите на данни на жалба до надзорен орган във Вътрешните правила не се съдържа информацията, която РС – Попово е следвало да предостави съгласно чл. 13, § 2, б. „г“ и чл. 14 § 2, б. „д“ от Регламент (ЕС) 2016/679 в политиката за прозрачност, а именно, че субектът на данни има право съгласно чл. 77 от Регламента да подаде жалба до надзорен орган, ако счита, че правата му в областта на защита на личните данни са нарушени. Посредством предоставяне на тази информация администраторът създава условия субектът на данни да упражни правото си на защита по административен ред, произтичащо от чл. 77 от Регламент (ЕС) 2016/679.

На субектите на данни следва да се предостави информация, че съгласно чл. 38, ал. 1 от ЗЗЛД при нарушаване на правата им по Регламент (ЕС) 2016/679 и по ЗЗЛД имат право да сезират Комисия по защита на личните данни, а когато нарушението е допуснато при обработване на лични данни от РС – Попово в контекста на правораздавателната дейност, правото на жалба се упражнява пред ИВСС, който е компетентен надзорен орган съгласно чл. 17, ал. 1 ЗЗЛД.

Във Вътрешните правила също така не се съдържа информацията, която компетентните органи са длъжни да предоставят на субектите по силата на чл. 54, ал. 1 и ал. 2 ЗЗЛД, когато обработват техни лични данни в контекста на правораздавателната дейност за целите по чл. 42 ЗЗЛД. Тази информация има по-ограничен обхват от информацията, предоставяна на основание чл. 13 и чл. 14 от Регламент (ЕС) 2016/679, като се отнася до данните, които идентифицират администратора, и координатите за връзка с него, правното основание и целите, за които се обработват личните данни, правото на жалба до ИВСС, правото да се изиска от администратора достъп до данните, коригиране, допълване или изтриване на лични данни и ограничаване на обработването на лични данни, срока, за който ще се съхраняват личните данни, а ако това е невъзможно – критериите, използвани за определяне на този срок и когато е приложимо – получателите или категориите получатели на личните данни, включително в трети държави или международни организации. Съществена отлика в обхвата на информацията, която администраторите са длъжни да предоставят на субектите на данни е и задължението на основание чл. 54, ал. 1, т. 6 ЗЗЛД за информиране на субектите за възможността им при отказ по чл. 54, ал. 3, по чл. 55, ал. 3 и ал. 4 и по чл. 56, ал. 6 и ал. 7 ЗЗЛД да упражнят правата си на информация, на достъп до данните, право на коригиране, допълване, изтриване или ограничаване на обработването чрез ИВСС.

2.2. Създаване на подходящо ниво на сигурност на личните данни

От информацията в р. I, т. 3 от попълнения от РС – Попово въпросник става ясно, че Вътрешните правила за защита на личните данни, с оглед съдържанието си, са вътрешният акт на съда, който е съобразен с изискванията на Регламент (ЕС) 2016/679 и ЗЗЛД и съдържа задълженията на администратора на лични данни за поддържане на сигурността на данните, включително и оценка на въздействие на предвидените операции по обработване върху защитата на лични данни в съда. В раздел „Технически и организационни мерки за защита на личните данни” от посочените е разписано, че администраторът на лични данни осигурява необходимите финансови, технически и човешки ресурси за определянето и въвеждането на подходящи организационни и технически мерки, които да съответстват на рисковете с различна вероятност и тежест за правата и свободите на физическите лица. В т. 1 – т. 4 от раздела е разписано, че РС – Попово като администратор на лични данни осигурява подходящи технически и организационни мерки за осигуряване на ниво на сигурност, съобразено с рисковете за правата и свободите на физическите лица. При оценката на подходящото ниво на сигурност се вземат предвид преди всичко рисковете, свързани с обработването като случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до обработвани лични данни.

Мерките могат да включват и псевдонимизация и криптиране на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите за обработване, способност за своевременно възстановяване на наличността и достъпа до лични данни в случай на физически или технически инцидент, процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационни мерки. Подходящите мерки се въвеждат към момента на определяне на средствата за обработване и към момента на самото обработване. Задължението за въвеждането им се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. С тези мерки администраторът гарантира, че по подразбиране се обработват лични данни, които са необходими за всяка конкретна цел на обработването.

В т. 6 от Вътрешните правила са регламентирани технически и организационни мерки за защита на личните данни:

- **Физическа защита** – предвиден е ограничен достъп до сградата на съда и до помещенията, в които се обработват лични данни;

- **Персонална защита** – достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп, при спазване на принципа „Необходимост да се знае” и след запознаване с нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане, опасностите за личните данни, обработвани от администратора и Вътрешните правила за защита на личните данни в РС – Попово;

- **Документална защита** – установени са процедури по обработване на лични данни, регламентиране на достъпа, унищожаване и срокове за съхранение. Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само при възникнала необходимост;

- **Защита на автоматизираните информационни системи и мрежи** – електронната обработка на лични данни се извършва с помощта на специализирани софтуерни продукти и чрез стандартни средства за текстообработка, като се използват само лицензирани системи и приложни софтуерни продукти или компютърни програми. Идентификацията и автентификацията на потребителите се извършва чрез потребителско име и парола. Работните конфигурации се използват единствено за служебни цели. Забранено е ползването на преносими носители на данни за лични нужди. Забранен е отдалечен достъп до данни от регистрите. Инсталирана е антивирусна програма и се извършва ежеседмична профилактика на софтуера и системните файлове.

- **Криптографска защита** – използват се стандартните криптографски възможности на операционната система, на системите за управление на бази

данни, на комуникационното оборудване както и квалифицирани електронни подписи.

Посочените разпоредби по същество нямат характер на оценка на въздействието по смисъла на чл. 35 от Регламент (ЕС) 2016/679, която трябва да бъде направена преди да бъде извършено обработването, като това изискване е проявление на концепцията за защита на данните на етапа на проектирането. Спрямо вече извършвани към момента на влизане в сила на Регламента операции по обработване, оценка на въздействието може да се налага само в две хипотези:

- ако обработването е било обект на предварителна проверка от надзорен орган и е настъпила промяна в дадените от надзорния орган условия за обработване, ако това обработване създава високи рискове и

- ако при периодичното преразглеждане на анализа на риска се констатира, че за съществуващи операции е настъпила промяна в обстоятелствата (примерно се внедряват нови технологии или се удължават сроковете за съхранение), която обосновава наличието на висок риск за правата на субектите.

На следващо място, оценка на въздействието се извършва по отношение на конкретни операции по обработване, за които има вероятност да породят висок риск за правата и свободите на субектите на данни – чл. 35, пар. 1 от Регламент (ЕС) 2016/679. Тя не се изисква за всяка операция по обработване. Примерни операции по обработване, които има вероятност да породят висок риск са посочени в чл. 35, пар. 3 от Регламента, както и в списъка по чл. 35, пар. 4 от Регламента, утвърден от Комисията за защита на личните данни.

За разлика от оценката на въздействието, анализът на риска е задължителен елемент от процеса по управление на риска за защитата на личните данни. Като такъв той се прилага спрямо всички операции по обработване, извършвани под контрола на администратора. Като резултат от него се определят всички рискове, които могат да засегнат правата на физическите лица при обработване на личните им данни. Ако анализът покаже наличието на висок риск при някои дейности, ще се наложи извършване на оценка на въздействието, а в случай, че и след нея рискът не може да бъде намален, и консултация с надзорния орган. Анализът на риска е предпоставка за предприемане на координирани дейности, чрез които да се постигне сигурността на обработваните лични данни – чл. 32, § 1 от Регламент (ЕС) 2016/679, респективно чл. 66, ал. 1 ЗЗЛД. Съгласно цитираните разпоредби при оценка на подходящото ниво на сигурност администраторите са длъжни да вземат предвид по – специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни. Предвид това, последователността на действията, които трябва да се предприемат в процеса по установяване на подходящо ниво на сигурност, е

анализ на риска – определяне на нивото на сигурност – прилагане на подходящи технически и организационни мерки.

Съобразно изложеното документираната в раздел „Технически и организационни мерки за защита на личните данни” от Вътрешните правила за защита на личните данни в РС – Попово дейност формално представлява анализ на риска и описание на приложените от съда технически и организационни мерки за защита на обработваните от него лични данни. Така е защото тази оценка обхваща всички дейности по обработване, а не само конкретни такива. Освен това, тя се отнася за съществуващи операции, а не за бъдещи такива, които при това не пораждат висок риск за правата на засегнатите субекти.

От съдържанието на Вътрешните правила за защита на личните данни в РС – Попово се установява, че администраторът е идентифицирал всички категории данни, които обработва, като ги е организиран с оглед на целите на обработването им. Въпреки това, няма данни за всяка една от категориите лични данни, които се обработват да е извършен анализ на риска, като на основание чл. 32, § 2 от Регламент (ЕС) 2016/697, респективно чл. 66, ал. 1 ЗЗЛД да са отчетени рисковете по отношение на наличност, цялостност и поверителност на обработваните данни. Следователно, поради липсата на анализ на риска на отделните дейности по обработване, в частност извършваните при осъществяване на правораздавателната функция на съда, не е идентифицирано наличие на „висок“ риск за правата на засегнатите субекти. Съобразно направените в анализа изводи в РС – Попово са установени технически и организационни мерки за защита на данните.

2.3. Надлежно уреждане на отношенията с надзорния орган

Съобразно отговорите в попълнения от РС – Попово въпросник, във Вътрешните правила за защита на личните данни в РС – Попово е разписана процедура по докладване и управление на инциденти във връзка със защитата на личните данни.

В т. 1 – т. 4 от раздел „Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.)” е предвиден следния ред за реакция на служителите в съда - при възникване и установяване на инцидент, веднага се докладва на административния ръководител и в зависимост от обстоятелствата, се уведомяват и съответните институции. С наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, ако това е възможно. За инцидентите се води дневник, в който се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им (съгласно чл. 33, § 5 от Регламент (ЕС) 2016/697). В предвидените в Регламент (ЕС) 2016/697

и ЗЗЛД случаи за инцидента се уведомява надзорния орган – Комисията по защита на личните данни.

Независимо, че формално е разписана процедура за докладване и управление на инциденти във Вътрешните правила за защита на личните данни в РС – Попово същата не е в съответствие с чл. 33 от Регламент (ЕС) 2016/697.

Чл. 33 от Регламент (ЕС) 2016/697 създава задължение за администратора на лични данни да уведомява надзорния орган за нарушение на сигурността на личните данни. По смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/697 нарушение на сигурността на личните данни е всяко събитие, което се изразява в незаконосъобразни действия по отношение на личните данни и което води до нарушаване на тяхната поверителност, цялостност и/или наличност, като случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни. В съображение 85 от Регламент (ЕС) 2016/697 неизчерпателно са изброени възможните неблагоприятни последици, които могат да настъпят в резултат от нарушение на сигурността на личните данни (физически, материални или нематериални вреди за физическите лица). При настъпване на нарушение администраторът следва да направи оценка на вероятността от настъпване на неблагоприятно въздействие върху субектите на данните и тежестта на това въздействие върху правата и свободите им. Рискът е висок, когато след направената оценка се окаже, че въздействието е по-тежко или вероятността от неговото настъпване е по-значителна. При наличие на риск администраторът следва да уведоми на основание чл. 33 от Регламент (ЕС) 2016/697 за нарушението съответния надзорен орган - КЗЛД или ИВСС, когато нарушението на сигурността засяга лични данни, които РС – Попово обработва в контекста на правораздавателната си дейност, а ако се отнася до нарушение на лични данни, обработвани от съда за целите по чл. 42, ал. 1 ЗЗЛД, уведомяването следва да се извърши на основание чл. 67, ал. 1 ЗЗЛД. Минималното съдържание на уведомлението до надзорния орган е уредено в чл. 33, § 3 от Регламент (ЕС) 2016/697, респ. чл. 67, ал. 3 ЗЗЛД. Съгласно посочените норми, администраторът е задължен да документира всяко нарушение на сигурността на личните данни, затова следва да създаде процедури и механизми за реакция при настъпване на такива събития и да въведе регистър на нарушенията. Регистърът на нарушенията следва да е със съдържание, в съответствие с изискванията на чл. 33, § 5 от Регламент (ЕС) 2016/697 и на чл. 67, ал. 5 от ЗЗЛД, като в него се отразява задължителната информация за естеството, мястото и времето на нарушението, брой лица и категории данни, предприети действия за уведомяване на засегнати лица при висок риск, за уведомяване на надзорния орган – КЗЛД или ИВСС. В регистъра следва изрично да се уредят случаите, когато нарушението на сигурността засяга лични данни, които РС – Попово обработва в контекста на правораздавателната дейност. В тези случаи на основание чл. 33 от Регламент (ЕС) 2016/697 във вр. с чл. 17, ал. 1 от ЗЗЛД, за нарушението следва

да се уведоми компетентния надзорен орган в лицето на ИВСС, а ако нарушението засяга лични данни, обработвани от съда за целите по чл. 42, ал. 1 от ЗЗЛД, то уведомяването да се извърши на основание чл. 67, ал. 1 от ЗЗЛД.

От изложеното по-горе следва, че РС – Попово като администратор на лични данни не е регламентирал чрез вътрешен акт процедура по уведомяване на надзорния орган за нарушение на сигурността на личните данни, в съответствие с изискванията на Регламент (ЕС) 2016/679 и ЗЗЛД.

2.4. Изпълнение на други задължения на администратора по осигуряване на отчетност

На основание чл. 30 от Регламент (ЕС) 2016/679, респективно чл. 62, ал. 1 ЗЗЛД съдилищата са длъжни да водят регистър на дейностите по обработване, за които отговарят. Съдържанието и формата на този регистър са нормативно определени в Регламент (ЕС) 2016/679 и в ЗЗЛД. Той се води в писмена форма и задължително съдържа наименованието и координатите за връзка на администратора и на длъжностното лице по защита на данните, 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, категориите предаване на лични данни на трета държава или международна организация, когато е възможно, предвидените срокове за изтриване на различните категории лични данни, когато е възможно, общо описание на техническите и организационните мерки за сигурност. По отношение на дейностите за обработване на лични данни, извършвани от съдилищата в контекста на правораздавателната дейност за целите по чл. 42, ал. 1 ЗЗЛД регистърът на дейностите трябва да съдържа и информация дали се извършва профилиране, както и правното основание за операцията по обработване, включително предаването на данни, за която са предназначени личните данни.

РС – Попово в качеството на администратор на лични данни поддържа в писмена и електронна форма Регистър на дейностите по обработване на лични данни, утвърден като приложение № 1 към Заповед № 74/15.11.2019 г. на административния ръководител на РС -Попово. Съгласно т. 3 от заповедта е предвидено, че такъв следва да се води в писмена форма и в електронен формат.

Съобразно материалната компетентност, предвидена в чл. 17, ал. 1 от ЗЗЛД, Инспекторатът може да осъществява надзор единствено върху дейностите по обработване на лични данни в регистър „Съдебни дела“. По отношение на този регистър беше установено, че съдържанието му е в съответствие с Регламент (ЕС) 2016/679, респективно ЗЗЛД.

Администратор на лични данни е РС – Попово, посочени са координати за връзка с администратора.

В отделни графи са посочени:

- целите на обработването – данните се събират във връзка с целите на правораздавателната дейност;

- правното основание за обработването – ГПК, СК, ЗЗДетето, ЗЗД, ЗС, ЗГР, ЗЗДН, НПК, НК, ЗЗ, ЗБППМН, ЗЕС, ЗАНН и др.

- категориите субекти на данни - ищци, ответници и други участници в съдебния процес (подсъдими, жалбоподатели, тъжители, нарушители по УБДХ, молители в делата по реабилитация, в производствата във връзка с изпълнение на наказанията и искания до съда в досъдебното производство, лицата по отношение на които се иска прилагане на принудителна медицинска мярка и други участници в съдебния процес. Вискател, длъжник и други участници в изпълнителния процес;

- категориите лични данни, които се обработват - име; ЕГН; месторождение; адрес; данни за лична карта; телефон; информация за номер на банкова сметка; образование; трудова дейност; психическо състояние; умствено състояние; психическо здраве; имотно състояние; финансово състояние; участие и/или притежаване на дялове или ценни книжа в други дружества, културни интереси; социален произход; расов произход; етнически произход; политически, религиозни и/или философски убеждения;

- категориите получатели – обработващи лични данни, субектите на данни, лица – участници в съдебния процес, ОСВ, учреждения и ведомства, които по закон имат право да получават такава информация;

- предаването на лични данни в трети държави – извършва се съгласно изискванията на нормативната уредба, а съдебните поръчки се извършват при условията на чл. 124 от ПАС;

- срокове за изтриване - съгласно номенклатурата за съхранение на делата в РС – Попово;

- общо описание на мерките – физическа защита, персонална защита, документална защита, защита на АИС/М, криптографска защита.

По отношение на дейностите за обработване на лични данни, извършвани от съда в контекста на правораздавателната дейност за целите по чл. 42, ал. 1 от ЗЗЛД регистърът на дейностите трябва да съдържа и информация дали се извършва профилиране, както и правното основание за операцията по обработване, включително предаването на данни, за която са предназначени личните данни. Такава в Регистъра на дейностите на РС – Попово не е предвидена.

Съобразно изложеното се налагат следните

III. ИЗВОДИ:

1. Следва да се заключи, че Районен съд – Попово не доказва в пълна

степен принципа за отчетност, установен в чл. 5, § 2 от Регламент (ЕС) 2016/679 и в чл. 45, ал. 4 от ЗЗЛД. В контекста на осъществяваната правораздавателна дейност администраторът е изготвил Вътрешни правила за защита на данните, утвърдени със Заповед № 73/15.11.2019 г. на адм. ръководител на РС -Попово които са публикувани на интернет сайта на съда. От тези правила и другите изпратени документи е видно, че съдът е проявил активност, за да докаже, че спазва принципа за прозрачност по чл. 5, § 1, т. 1 от Регламент (ЕС) 2016/679. Установи се, че РС – Попово е приел вътрешен акт, с който да документира мерките за защита на личните данни, които се обработват под негов контрол, идентифицирал е целите, обхвата и естеството на различните категории дейности по обработване на личните данни, но не е идентифицирал отделните регистри с лични данни, които следва да поддържа в рамките на всяка извършвана от него дейност. РС – Попово е положил усилия да установи мерки за защита на личните данни, които се обработват под негов контрол, така че обработването да бъде законосъобразно, добросъвестно, прозрачно и в минимален обем за постигане на ясно определени цели, като данните да се съхраняват точни и само за времето, необходимо за постигане на тези цели, а посоченото обработване е обезпечено с подходящо ниво на сигурност и защита на данните, но не е приел процедура за уведомяване на компетентните надзорни органи в случай на нарушение на сигурността на личните данни.

2. РС – Попово като администратор на лични данни не е установил подходящи средства, с които да докаже, че спазва принципа за прозрачност по чл. 5, § 1, т. 1 от Регламент (ЕС) 2016/679, който налага физическите лица 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. В утвърдените със Заповед № 73/15.10.2019 г. на административния ръководител – председател на РС – Попово „Вътрешни правила за защита на личните данни в РС- Попово“, имащи характер на политика за прозрачност на информацията във връзка със защитата на личните данни в съда не е предоставена изцяло информацията по чл. 13 и чл. 14 от Регламент (ЕС) 2016/679.

Установи се, че във Вътрешните правила са идентифицирани целите, обхвата и естеството на различните категории дейности по обработване на личните данни, но не са идентифицирани отделните регистри с лични данни, които РС – Попово следва да поддържа в рамките на всяка извършвана от него дейност.

Също така се установи, че във Вътрешните правила не се съдържа информация, че РС – Попово е в състояние да докаже, че е изпълнил задължението съгласно чл. 13, § 2, б. „г“ и чл. 14 § 2, б. „д“ от Регламент (ЕС) 2016/679 да предостави на субектите на данни информация относно правото им на жалба по чл. 77 от Регламент (ЕС) 2016/679 до надзорен орган, като

когато правата на субектите са нарушени при обработване на личните им данни в контекста на правораздавателната дейност, това право се упражнява пред ИВСС съгласно чл. 17, ал. 1 ЗЗЛД.

Установи се също така, че във Вътрешните правила не се съдържа информацията, която компетентните органи са длъжни да предоставят на субектите по чл. 54, ал. 1 и ал. 2 ЗЗЛД, когато обработват техни лични данни в контекста на правораздавателната дейност за целите по чл. 42 ЗЗЛД.

Съобразно тези три констатации, на РС – Попово следва да се отправи препоръка да допълни съдържанието на Вътрешните правила за защита на личните данни.

3. По отношение на мерките за сигурност на личните данни се установи, че във Вътрешните правила за защита на личните данни са регламентирани технически и организационни мерки за защита на данните, които обхващат аспектите на физическа, персонална, документална, криптографска защита и защита на автоматизираните информационни системи и мрежи. Установи се, че макар и формално да са разписани правила относно анализ на риска, такъв не е извършван на основание чл. 32, § 1 от Регламент (ЕС) 2016/279, респективно на основание чл. 66, ал. 1 ЗЗЛД по отношение на всеки от регистрите с лични данни.

Съобразно тази констатация, на РС – Попово следва да се отправи препоръка да извърши анализ на риска на основание чл. 32, § 1 от Регламент (ЕС) 2016/279 по отношение на личните данни, които обработва в контекста на правораздавателната си дейност, и на основание чл. 66, ал. 1 ЗЗЛД - по отношение на личните данни, които обработва за целите по чл. 42, ал. 1 ЗЗЛД.

4. РС – Попово в качеството си на администратор на лични данни не е предприел в пълна степен действия за сътрудничество с надзорните органи в областта на защитата на личните данни.

Разписаната процедура за докладване и управление на инциденти във Вътрешните правила за защита на личните данни в РС – Попово не е в съответствие с чл. 33 от Регламент (ЕС) 2016/679, респ. чл. 67 от ЗЗЛД. Съдът като администратор на лични данни следва да уреди с вътрешен акт процедура по уведомяване на надзорните органи в случай на нарушение на сигурността на личните данни, като в случаите, когато нарушението на сигурността на личните данни е допуснато при обработването им от РС – Попово за целите на чл. 42, ал. 1 от ЗЗЛД следва да се предвиди процедура съгласно чл. 67 от ЗЗЛД. РС – Попово като администратор на лични данни следва да въведе регистър на нарушенията със съдържание, в съответствие с изискванията на чл. 33, § 5 от Регламент (ЕС) 2016/679 и на чл. 67, ал. 5 от ЗЗЛД.

Съобразно тази констатация, на РС – Попово следва да се отправи препоръка.

5. РС – Попово е изпълнил задължението си да води регистър на дейностите по обработване на лични данни на основание чл. 30 от Регламент (ЕС) 2016/697, респективно чл. 62, ал. 1 ЗЗЛД. Необходимо е да се отбележи, че по отношение на дейностите за обработване на лични данни, извършвани от съда в контекста на правораздавателната дейност за целите по чл. 42, ал. 1 от ЗЗЛД регистърът на дейностите трябва да съдържа и информация дали се извършва профилиране, както и правното основание за операцията по обработване, включително предаването на данни, за която са предназначени личните данни. Такава в Регистъра на дейностите на РС – Попово не е предвидена.

Съобразно това на РС – Попово следва да се отправи препоръка да се допълни съдържанието на регистъра на дейностите.

Съобразно направените изводи и на основание чл. 19, ал. 1 във вр. с чл. 17а, ал. 2, т. 2 и чл. 80, ал. 2 във вр. с чл. 17а, ал. 2, т. 2 от ЗЗЛД намирам, че на Районен съд – Попово като администратор на лични данни следва да се отправят следните

IV. ПРЕПОРЪКИ:

1. Да допълни съдържанието на Вътрешни правила за защита на личните данни в РС – Попово, като:

- идентифицира отделните регистри с лични данни, които следва да поддържа в рамките на всяка извършвана от него дейност;

- изрично се посочи правото на жалба на субектите на данни по чл. 77 от Регламент (ЕС) 2016/679 до надзорен орган, като когато правата на субектите са нарушени при обработване на личните им данни в контекста на правораздавателната дейност, това право се упражнява пред ИВСС съгласно чл. 17, ал. 1 от ЗЗЛД;

- се отрази информацията, която компетентните органи за длъжни да предоставят на субектите по чл. 54, ал. 1 и ал. 2 от ЗЗЛД, когато обработват техни лични данни в контекста на правораздавателната дейност за целите по чл. 42 от ЗЗЛД.

2. Да се извърши анализ на риска на основание чл. 32, § 2 от Регламент (ЕС) 2016/679 по отношение на личните данни, които обработва в контекста на правораздавателната си дейност, и на основание чл. 66, ал. 1 от ЗЗЛД - по отношение на личните данни, които обработва за целите по чл. 42, ал. 1 от ЗЗЛД.

3. Да се разпише във вътрешен акт на администратора процедура за докладване и управление на инциденти в съответствие с чл. 33 от Регламент (ЕС) 2016/697, респ. чл. 67 от ЗЗЛД. Изрично да се предвиди процедура

съгласно чл. 67 от ЗЗЛД в случаите, в които нарушението на сигурността на личните данни е допуснато при обработването им от РС – Попово за целите на чл. 42, ал. 1 от ЗЗЛД. РС – Попово като администратор на лични данни да въведе регистър на нарушенията със съдържание, в съответствие с изискванията на чл. 33, § 5 от Регламент (ЕС) 2016/679 и на чл. 67, ал. 5 от ЗЗЛД.

4. Да се допълни съдържанието на регистъра на дейностите по обработване на лични данни, който РС – Попово е води на основание чл. 30 от Регламент (ЕС) 2016/697, респективно чл. 62, ал. 1 от ЗЗЛД по отношение на дейностите за обработване на лични данни, извършвани от съда в контекста на правораздавателната дейност за целите по чл. 42, ал. 1 от ЗЗЛД. В регистъра да се включи и следната информация: извършва ли се профилиране на личните данни, правното основание за операцията по обработване, включително предаването на данни, за която са предназначени личните данни.

Указва на администратора на лични данни РС – Попово да изпълни препоръките в тримесечен срок от съобщаване на акта, като за изпълнението им бъде уведомен Инспекторатът към ВСС.

Екземпляр от акта да бъде изпратен на административния ръководител на РС – Попово като представляващ администратора на лични данни.

ИНСПЕКТОР:

Заличено на
осн. ЗЗЛД

М. Николов

