



РЕПУБЛИКА БЪЛГАРИЯ
ИНСПЕКТОРАТ КЪМ ВИСШИЯ СЪДЕБЕН СЪВЕТ

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

Изх. № ПЛД-20-6
Дата: 16.12.2020

ПРОВЕРКА
НА ИНСПЕКТОРАТА КЪМ ВИСШИЯ СЪДЕБЕН СЪВЕТ

А К Т

ЗА РЕЗУЛТАТИ ОТ ИЗВЪРШЕНА ПЛАНОВА ПРОВЕРКА ПО
ЗАПОВЕД № ПЛД-20-6/29.05.2020 г.
НА ГЛАВНИЯ ИНСПЕКТОР НА ИВСС

РАЙОНЕН СЪД - ПЕЩЕРА

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), приетата Годишна програма за проверки на Инспектората към Висшия съдебен съвет (ИВСС) за 2020 г. и заповед № ПЛД-20-6/29.05.2020 г. на главния инспектор на ИВСС се извърши планова проверка по документи на Районен съд (РС) – Пещера 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. 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, наричан по-нататък Регламент (ЕС) 2016/679.

Срок за извършване - 15.06.2020 г.

СЪСТАВ НА ПРОВЕРЯВАЩИЯ ЕКИП:

ИНСПЕКТОР: Стефка Мулячка

ЕКСПЕРТИ: Юлия Меранзова и Цветан Иванчовски.

ЦЕЛ И ОБХВАТ НА ПРОВЕРКАТА

Цел на проверката е да се установи дали РС – Пещера 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 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 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 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 за организиране на процесите по обработване на данни 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 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 с 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. Сред тях са например придържането към одобрени кодекси за 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. 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 Инспектората към ВСС; 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 на 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 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.

Цел на конкретната проверка е да бъдат разгледани представените от Районен съд – Пещера документи, за да се установи дали и в каква степен съдът е в състояние да докаже, че е предприел достатъчни и ефективни мерки, за да се гарантира, че обработването на лични данни в контекста на правораздавателната дейност се осъществява при спазване на принципите и 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 - 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 на 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 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 14 от Регламент (ЕС) 2016/679. Що се отнася до обработването на лични данни за целите по 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 на 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 организационни 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 задължени 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 – на основание 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 за 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 – Пещера в качеството на администратор на лични 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 - по 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 организационни 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 проверваният съд няма да бъде санкциониран с имуществена санкция, защото целта на проверките за спазване на принципа за отчетност, заложена 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 на 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. 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-20-6/01.06.2020 г. до РС – Пещера е изпратено уведомление за предстоящата проверка, заедно с екземпляр от заповедта за проверка 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. рег. № КПЛД-20-6/11.06.2020 г. в ИВСС са постъпили надлежно оформен екземпляр от заповедта за проверка, попълнен въпросник и копия от следните документи :

1. Вътрешни правила за защита на личните данни, утвърдени от административния ръководител – председател на съда Камен Гатев.

2. Документ, озаглавен „Защита на личните данни“.

3. Примерна номенклатура на делата със срокове за съхраняването им, образувани от дейността на окръжните и районните съдилища, утвърдена на 16.03.2008 г. от председателя на Държавна агенция „Архиви“ д-р Б. Бужашка.

1. Административна и организационна структура

В РС - Пещера има 4 щатни длъжности за съдии, от които едната е за председател, един държавен съдебен изпълнител, един съдия по вписванията. Съдебната администрация включва 19 служители. Изпълняващ функциите административен ръководител – председател на съда е Атанаска Павлова.

2. Организация на способите за спазване на принципа за отчетност в Районен съд – Пещера

Информация в тази връзка се извлича от Вътрешните правила за защита на личните данни, утвърдени от административния ръководител на съда, и от отговорите в представения въпросник. Установява се, че РС – Пещера е обособил и обработва лични данни на физически лица в седем регистъра: Регистър „Персонал“; Регистър „Кандидати за съдебни служители“; Регистър „Съдебни дела“; Регистър „Вещи лица, преводачи и съдебни заседатели“; Регистър „Бюро съдимост“; Регистър „Лични данни на лица, подали молби, жалби, предложения, сигнали и искания“; Регистър „Контрагенти“.

Съобразно информацията от Вътрешните правила и 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 – Пещера обработва лични данни в два от тези регистри - Регистър „Вещи лица, преводачи и съдебни заседатели“ и Регистър „Съдебни дела“.

Данните в тези регистри се отнасят до следните аспекти от идентичността на физическите лица:

Регистър „Съдебни дела“

В регистъра се обработват лични данни във връзка с участие на лицата в съдебния процес.

Посочено е правното основание за обработване - ГПК, НПК, ЗСВ, Правилник за администрацията в съдилищата (ПАС).

Обработват се лични данни на лица - участници в процеса по наказателните и гражданските дела. За тези субекти се обработват лични данни за физическа идентичност: имена, ЕГН, адрес и телефон и електронна поща за връзка; социална идентичност: данни относно образование, трудова дейност, месторабота, стаж, професионална биография; семейна идентичност - данни за семейното положение на лицата; икономическа идентичност - данни относно възнаграждението за заеманата длъжност и възнаграждението на лицата.

Изброени са категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации – данните могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение, за изпълнение на куриерски услуги, а при трансфер в други държави се предоставят данни единствено с оглед физическата и социалната идентичност на лицата, като се спазват изискванията на глава V от Регламент (ЕС) 2016/679.

Регистър „Вещи лица, преводачи и съдебни заседатели“

В регистъра се обработват лични данни за участващите в съдебните производства вещи лица, преводачи и съдебни заседатели. Личните данни се обработват с цел изпълнение на нормативните изисквания на ЗСВ, ПАС, ГПК, НПК, Наредба за възнагражденията на вещите лица, Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството и други.

Събраните данни се използват за целите на гражданските и наказателните дела, за телефонни контакти и кореспонденция със субектите, отнасящи се до изпълнение на задълженията им по делата, за водене на счетоводна отчетност относно възнагражденията им.

Не е посочено правното основание за обработването на тези данни.

Обработват се следните категории лични данни: физическа идентичност - имена, ЕГН, адрес, месторождение и други; социална идентичност - данни относно образование, месторабота; икономическа идентичност – данни относно възнагражденията; лични данни относно съдебното минало на лицата, когато това се изисква от нормативен акт.

Посочени са категории получатели: съдебни деловодители, съдебни секретари, системен администратор, административен секретар и други, при спазване на принципа „необходимост да се знае“. Данните от този регистър не се трансферират в други държави.

2.1. Отношения със субектите

В тази връзка следва да се отбележи изпратеният от РС – Пещера документ със заглавие „Защита на личните данни“. Липсва заповед за утвърждаване на този акт, но с оглед неговото съдържание същият може да бъде определен като политика за прозрачност при обработване на

информацията, тъй като изрично е указано, че е изготвен в изпълнение на чл. 13 и 14 от Регламент (ЕС) 2016/679, с цел да се информират физическите лица - субекти на данни за извършваните от съда дейности по обработването на личните данни. В съдържанието на политиката са посочени данните, които идентифицират администратора и координати за връзка с него. За всеки регистър с лични данни, включително за Регистър „Вещи лица, преводачи и съдебни заседатели“ и Регистър „Съдебни дела“, са посочени целите на обработването и правното основание за обработването, описани са съответните категории лични данни. Посочено е, че личните данни в Регистър „Съдебни дела“ се обработват на основание чл. 6, § 1, б. „в“ от Регламент (ЕС) 2016/679 и Закона за съдебната власт. Не е посочено, че личните данни, които се обработват в този регистър 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 от ЗЗЛД.

В документа е записано, че обработваните в двата регистъра лични данни могат да бъдат предоставени на трети лица само когато това е предвидено в закон. По отношение на хипотезите, в които лични данни, обработвани от РС – Пещера в контекста на правораздавателната дейност, могат да бъдат предадени на трета държава е предвидено, че трансфер на лични данни се извършва по дела с участие на лице от чужбина или по дела със съдебни поръчки в друга държава.

В политиката за прозрачност също така изрично е указано, че личните данни, обработвани в двата регистъра, се съхраняват за сроковете, определени в номенклатурата на делата със срокове за съхраняването им, образувани от дейността на окръжните и районните съдилища, утвърдена на 16.03.2008 г. от председателя на Държавна агенция „Архиви“.

По отношение на всички регистри с лични данни е посочено изрично, че субектите на данни имат възможност да упражнят следните права: право на достъп до данните, право на коригиране или изтриване на свързани със субекта лични данни, право на ограничаване на обработването и правото да се направи възражение срещу обработването, както и право на преносимост и на субекта да не бъде обект на изцяло автоматизирано решение. Не е направена препратка в кои разпоредби на Регламент (ЕС) 2016/679 и/или на ЗЗЛД са предвидени тези права, но за тяхното упражняване е установена кратка и ясна процедура, която също е част от политиката за прозрачност.

По отношение на правото на субектите на данни на жалба до надзорен орган, в политиката за прозрачност е допусната непълнота, като е посочено, че субектите, чиито права по Регламент (ЕС) 2016/679 са били нарушени, имат право на жалба до Комисията за защита на личните данни. Не се съдържа информация, че когато нарушението е допуснато при обработване на лични данни от РС – Пещера в контекста на правораздавателната дейност, правото на жалба се упражнява пред ИВСС, който е компетентен

надзорен орган съгласно чл. 17, ал. 1 от ЗЗЛД.

В политиката за прозрачност 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 от ЗЗЛД, когато обработват техни лични данни в контекста на правораздавателната дейност за целите по чл. 42 от ЗЗЛД. Тази информация има по-ограничен обхват от информацията, предоставяна на основание чл. 13 и 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 Инспектората, 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, а в случаите, 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 задължението на основание чл. 54, ал. 1, т. 6 от ЗЗЛД за информирание на субектите за възможността им при отказ по чл. 54, ал. 3, по чл. 55, ал. 3 и 4 и чл. 56, ал. 6 и 7 от закона да упражнят правата си на информация, на достъп до данните, право на коригиране, допълване, изтриване или ограничаване на обработването чрез ИВСС.

РС – Пещера информира субектите на данни за личните данни, които обработва, чрез публикуване на документа на интернет-страницата на съда <https://peshtera-rs.justice.bg/upload/25251/GDPR.pdf?inline=1>. По този начин информацията, съдържаща се в политиката за прозрачност на РС – Пещера, е лесно достъпна за субектите на данни, като тя е написана разбираемо с използване на ясни и недвусмислени формулировки.

2.2. Създаване на подходящо ниво на сигурност на личните данни

От РС – Пещера е изпратен документ, озаглавен „Вътрешни правила за защита на личните данни“, който е утвърден от административния ръководител на съда Камен Гатев (не е приложена заповед за утвърждаването на правилата). В чл. 1 на Вътрешните правила е предвидено, че те уреждат условията и реда за обработване на лични данни, водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработване на лични данни в Районен съд - Пещера. Изброени са регистрите на лични данни, поддържани в съда, и за всеки регистър подробно са описани: целта на обработване, категории обработвани лични данни, кои лица под ръководството на администратора изпълняват дейностите по обработване, на кои категории лица могат да се предоставят

обработваните данни, както и технологично описание на съответния регистър – уредба относно носителите на данни, технология на обработване, срок за съхраняване и предоставяни услуги.

Във Вътрешните правила са регламентирани технически и организационни мерки за защита на данните:

- Физическа защита;
- Персонална защита;
- Документална защита;
- Защита на автоматизирани информационни системи и/или мрежи;
- Криптографска защита.

Като самостоятелен раздел във Вътрешните правила е предвидено извършването на оценка на въздействието върху защитата на личните данни в РС – Пещера. Съгласно чл. 49 от Правилата, оценка на въздействието се извършва, когато това се изисква от нормативен акт и с оглед на риска за физическите лица и естеството на обработване на лични данни. Посочено е, че оценка на въздействието се извършва във всички случаи на високорискови дейности по обработване. Тази разпоредба по съществото си няма 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 Регламент (ЕС) 2016/679 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;

- 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, § 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, § 3 от Регламент (ЕС) 2016/679, както и в списъка по чл. 35, § 4 от Регламент (ЕС) 2016/679, 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 от 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.

От съдържанието на Вътрешните правила за защита на личните данни е видно, че администраторът РС – Пещера е идентифицирал всички категории данни, които обработва, като ги е организиран в регистри по дейности. Въпреки това, няма данни за всеки от регистрите с лични данни да е извършен анализ на риска, като на основание чл. 32, § 2 от Регламент (ЕС) 2016/679 и/или чл. 66, ал. 1 от ЗЗЛД да са отчетени рисковете по отношение на наличност, цялостност и поверителност на обработваните данни. Не може да бъде направено заключение дали спрямо която и да е от дейностите и в частност извършваните при осъществяване на правораздавателната функция на съда е констатирано наличие на висок риск за правата на засегнатите субекти, а оттам – и въз основа на какви изводи в съда са установените технически и организационни мерки за защита на данните.

За пълнота на анализа е необходимо да се отбележи, че във Вътрешните правила за защита на личните данни, утвърдени от административния ръководител на РС - Пещера, се съдържат процедури за разглеждане на исканията на субектите на данни до администратора, свързани с упражняване на правата им по Регламент (ЕС) 2016/679, и за реакция при инциденти.

2.3. Надлежно уреждане на отношенията с надзорния орган

От изпратените от РС – Пещера документи се установи, че е утвърдена процедура по докладване и управление на инциденти във връзка със защитата на личните данни, която се прилага в съда и е част от

Вътрешните правила за защита на личните данни. В посочената процедура са определени редът и условията за реакция на служителите в РС – Пещера при констатиране на нарушение на сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679. В чл. 51, ал. 1 от Вътрешните правила е предвидено, че когато има вероятност нарушението да породи риск за правата на засегнатите субекти, се уведомява Комисията за защита на личните данни. В същото време, не са уредени изрично случаите, когато нарушението на сигурността засяга лични данни, които РС – Пещера обработва в контекста на правораздавателната дейност. В тези случаи на основание чл. 33 от Регламент (ЕС) 2016/679 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 се извършва на основание чл. 67, ал. 1 от ЗЗЛД.

В установената процедура за докладване и управление на инциденти във връзка със защитата на личните данни е предвидено документиране на допуснатите нарушения на сигурността на личните данни, като то се извършва чрез вписване на обстоятелствата, свързани с всяко отделно нарушение, в специален регистър по чл. 52 от Вътрешните правила. При все че е предвидено воденето на регистър на нарушенията от страна на администратора, с описано съдържание в съответствие с изискванията на чл. 33, § 5 от Регламент (ЕС) 2016/679 и на чл. 67, ал. 5 от ЗЗЛД, образец на такъв регистър не е изпратен в ИВСС.

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

На основание чл. 30 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 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 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.

От представените от РС – Пещера при проверката документи се установява, че съдът в качеството на администратор на лични данни не води самостоятелен документ – регистър на дейностите по обработване на лични данни. Вярно е, че в предоставените Вътрешни правила са изброени поддържаните регистри на лични данни и в най-общ план е посочена информация, която описва дейностите по обработване на лични данни от съда в контекста на правораздаването. Това обаче не е достатъчно да се докаже спазването на Регламент (ЕС) 2016/679 и на ЗЗЛД. Наличието на такъв самостоятелен документ, освен, че е важен елемент от механизмите за отчетност по смисъла на чл. 5, § 2 от Регламент (ЕС) 2016/679 и на чл. 45, ал. 4 от ЗЗЛД, гарантира възможност компетентният надзорен орган да се запознае с извършваните от администратора операции по обработване на лични данни чрез достъп до тази документация.

Съобразно изложеното се налагат следните

ИЗВОДИ:

1. Следва да се заключи, че Районен съд – Пещера не доказва в пълна степен спазване на принципа за отчетност, установен в чл. 5, § 2 от Регламент (ЕС) 2016/679 и в чл. 45, ал. 4 от ЗЗЛД, при все че в контекста на осъществяваната правораздавателна дейност е идентифицирал естеството, обхвата и целите, за които обработва лични данни, и е изготвил Вътрешни правила за предприетите от него мерки за защита на правата на субектите на данни. От тези Правила се установява, че администраторът е проявил активност и е установил 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 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. РС – Пещера не е в състояние да докаже, че поддържа Регистър на дейностите по обработване на лични данни, какъвто изискват чл. 30, § 1 и 3 от Регламент (ЕС) 2016/679 и чл. 62, ал. 1 и 3 от ЗЗЛД.

2. Не се установи дали в РС – Пещера е извършен анализ на риска на основание чл. 32, § 2 от Регламент (ЕС) 2016/679, съответно - чл. 66, ал. 1 от ЗЗЛД по отношение на всеки от регистрите с лични данни, въпреки предвидените във Вътрешните правила разпоредби за извършване оценка на въздействието на дейностите по обработване, и въз основа на какви критерии са определени мерките за сигурност на личните данни.

Съобразно тази констатация на РС – Пещера следва да се отправи препоръка да 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. РС – Пещера като администратор на лични данни е установил мерки за спазване на принципа за прозрачност по чл. 5, § 1, т. 1 от Регламент (ЕС) 2016/679. Наличен е документ със заглавие „Защита на личните данни“, който може да бъде определен като Политика за прозрачност при обработване на информацията. В този акт по достатъчно ясен за субектите на данни начин се предоставя информацията по чл. 13 и 14 от Регламент (ЕС) 2016/679.

В същото време, внимателният прочит на Политиката за прозрачност сочи, че липсва информация за нарушаване правата на субектите при обработване на личните им данни в контекста на правораздавателната дейност. Следва да се посочи, че в тези случаи правото на жалба се упражнява пред ИВСС, който е компетентен надзорен орган съгласно чл. 17, ал. 1 ЗЗЛД.

В Политиката за прозрачност също така не се съдържа информацията, която компетентните органи са длъжни да предоставят на субектите по силата на чл. 54, ал. 1 и 2 от ЗЗЛД, когато обработват техни лични данни в контекста на правораздавателната дейност за целите по чл. 42 от ЗЗЛД.

4. Може да се приеме, че РС – Пещера в качеството на администратор на лични данни е предприел действия за сътрудничество с надзорните органи в областта на защитата на личните данни. В съда е утвърдена процедура по докладване и управление на инциденти във връзка със защитата на личните данни, макар и като част от Вътрешните правила за защита на данните. Не са уредени изрично случаите, когато нарушението на сигурността засяга лични данни, обработвани от съда в контекста на правораздавателната дейност. В тези случаи на основание чл. 33 от Регламент (ЕС) 2016/679 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 РС – Пещера за целите по чл. 42, ал. 1 от ЗЗЛД, то уведомяването се извършва на основание чл. 67, ал. 1 от ЗЗЛД.

От изложеното по т. 1 е видно, че са налице следните нарушения от страна на РС – Пещера като администратор на лични данни при изпълнение на функциите му на орган на съдебната власт:

1.1. На чл. 30 от Регламент (ЕС) 2016/679, изразяващо се в това, че към датата на проверката – 15.06.2020 г. в качеството на администратор на лични данни не води регистър на дейностите по обработване на личните

данни, които обработва в контекста на правораздавателната си дейност;

1.2. На чл. 62, ал. 1 от ЗЗЛД, изразяващо се в това, че към датата на проверката – 15.06.2020 г. в качеството на администратор на лични данни не води регистър на дейностите по обработване на личните данни, които обработва за целите по чл. 42, ал. 1 от ЗЗЛД.

С оглед характера и степента на нарушението на Регламент (ЕС) 2016/679 и на ЗЗЛД, законосъобразно и съизмеримо е спрямо администратора на лични данни РС - Пещера да бъдат приложени само принудителни административни мерки, тъй като налагането паралелно с тях или самостоятелно на административно наказание би било прекомерно, както следва: на основание чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679 - „Разпореждане до администратора да съобрази операциите по обработване с разпоредбите на Регламента“, и на основание чл. 80, ал. 1, т. 4 от ЗЗЛД - „Разпореждане до администратора да приведе операциите по обработване в съответствие с Глава осма от ЗЗЛД“. Конкретните мерки следва да се изразяват в това да бъде ангажиран администраторът да изпълни задължението си да води регистър на дейностите по обработване на лични данни на основание чл. 30 от Регламент (ЕС) 2016/679 за личните данни, които обработва в контекста на правораздавателната си дейност, и на основание чл. 62, ал. 1 от ЗЗЛД - по отношение на личните данни, които обработва за целите по чл. 42, ал. 1 от ЗЗЛД. Чрез прилагането на тези мерки ще се постигне не само преустановяване на установеното нарушение, но и ще се способства за предотвратяване и отстраняване на евентуални последици от него.

Предвид направените в т. 2, 3 и 4 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, проверяващият инспектор намира за необходимо на РС – Пещера като администратор на лични данни да се отправят следните

ПРЕПОРЪКИ:

1. Да 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.

2. Да се допълнят Вътрешните правила за защита на личните данни, утвърдени от административния ръководител, като:

- се обособи раздел относно дейностите по обработване на лични данни в регистър „Съдебни дела“, с ясно разграничение на дейностите по отделните видове дела – граждански и наказателни;

- в частта, уреждаща процедурата по докладване и управление на инциденти изрично се посочи, че когато нарушението на сигурността засяга

лични данни, които РС – Пещера обработва в контекста на правораздавателната дейност, на основание чл. 33 от Регламент (ЕС) 2016/679 във вр. с чл. 17, ал. 1 от ЗЗЛД за него следва да бъде уведомен ИВСС, а ако нарушението засяга лични данни, обработвани от съда за целите по чл. 42, ал. 1 от ЗЗЛД, то уведомяването се извършва на основание чл. 67, ал. 1 от ЗЗЛД.

3. Да се допълни съдържанието на документа, озаглавен „Защита на личните данни“, който изпълнява функциите на Политика за прозрачност при обработване на информацията, като:

- се опишат обстоятелствата по чл. 54, ал. 1 и 2 от ЗЗЛД и се посочи, че информацията се предоставя на физическите лица, чиито лични данни се обработват в контекста на правораздавателната дейност за целите по чл. 42 от ЗЗЛД;

- изрично се посочи, че когато правата на субектите са нарушени при обработване на личните им данни в контекста на правораздавателната дейност, правото на жалба се упражнява пред ИВСС съгласно чл. 17, ал. 1 ЗЗЛД.

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

Предвид направените в т. 1 изводи, на основание чл. 19, ал. 2 и 3 във вр. с чл. 17а, ал. 1, т. 2 и ал. 3 от ЗЗЛД, проверяващият инспектор предлага на Инспектората към ВСС да приеме следното

РЕШЕНИЕ:

1. Приема, че към 15.06.2020 г. РС – Пещера, в качеството му на администратор на лични данни, не води Регистър на дейностите по обработване на лични данни при изпълнение на функциите му като орган на съдебната власт по смисъла на чл. 17, ал. 1 от ЗЗЛД - нарушение по чл. 30, § 1 от Регламент (ЕС) 2016/679.

Приема, че към 15.06.2020 г. РС – Пещера, в качеството му на администратор на лични данни, не води Регистър на дейностите по обработване на лични данни, които обработва за целите по чл. 42, ал. 1 от ЗЗЛД - нарушение по чл. 62, ал. 1 и 3 от ЗЗЛД.

2. С оглед характера и степента на извършеното нарушение, Инспекторатът към Висшия съдебен съвет разпорежда на РС – Пещера в качеството му на администратор на лични данни:

- а) на основание чл. 84, ал. 1 и 2 от ЗЗЛД във връзка с чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679, да приведе операциите по обработване на

лични данни в съответствие с разпоредбата на чл. 5, § 2 от Регламент (ЕС) 2016/679, като изготви и поддържа в писмена форма, включително в електронен формат, Регистър на дейностите по обработване на личните данни, за които отговаря в контекста на правораздавателната си дейност;

б) на основание чл. 84, ал. 1 и 2 от ЗЗЛД във връзка с чл. 80, ал. 1, т. 4 от ЗЗЛД, да приведе да приведе операциите по обработване на лични данни в съответствие с изискванията на чл. 45, ал. 4 от ЗЗЛД, като изготви и поддържа в писмена форма, включително в електронен формат, Регистър на дейностите по обработване на личните данни, които обработва за целите по чл. 42, ал. 1 от ЗЗЛД.

3. Указва на администратора на лични данни РС - Пещера да изпълни разпореждането по т. 2 в тримесечен срок от влизане в сила на настоящото решение, като за изпълнението му бъде уведомен Инспекторатът към ВСС.

Копие от акта да бъде изпратено на административния ръководител на РС - Пещера като представляващ администратора на лични данни, ведно с решението на ИВСС.

ИНСПЕКТОР:

Заличено на
осн. ЗЗЛД

СТЕФКА МУ

