



РЕПУБЛИКА БЪЛГАРИЯ
ИНСПЕКТОРАТ КЪМ ВИСШИЯ СЪДЕБЕН СЪВЕТ

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

Изх. № ЛДИ-26-1
Дата: 10.03.2026г.

ДО
СЪДИЙСКАТА КОЛЕГИЯ НА
ВИСШИЯ СЪДЕБЕН СЪВЕТ

СТ А Н О В И Щ Е

по чл. 94г, ал. 2 от Правилника за организацията на дейността на
Инспектората към Висшия съдебен съвет и за дейността на
администрацията и на експертите

Инспекторатът към Висшия съдебен съвет (ИВСС), като разгледа докладваната от инспектор Игнат Георгиев преписка, рег. № ЛДИ-26-1/02.02.2026 г. по описа на ИВСС, намира следното:

Производството е по реда на чл. 94г, ал. 2 от Правилника за организацията на дейността на Инспектората към Висшия съдебен съвет и за дейността на администрацията и на експертите (ПОДИВССДАЕ) за изразяване на становище по принципи въпроси, свързани с обработване на лични данни от органите на съдебната власт.

Образувано е по самосезиране на Инспектората към Висшия съдебен съвет по повод на сключените от Висшия съдебен съвет (ВСС) Договор № ВСС-15840/22.12.2023 г. с предмет: „Надграждане на центровете за данни във ВСС“ с изпълнител „Сиенсис“ АД и Договор № ВСС-14008/02.10.2025г. с предмет: „Наблюдение и управление на информационно-комуникационна инфраструктура (ИКИ) и осъществяване на дейности, свързани с киберсигурността на ВСС и съдилищата, с изключение на административните съдилища и Върховния административен съд“ с изпълнител „Информационно обслужване“ АД.

Двата договора са сключени за придобиване на техническо оборудване и софтуерни лицензи за надграждане на съществуващата хардуерна и комуникационна инфраструктура, върху която работят или предстои да работят централизираните информационни системи от ключово значение за съдебната система като ЕИСС, СИСМА, ЕПЕП и др., както и да бъде внедрено единно решение за киберсигурност.

Предвиденото решение за киберсигурност е платформата за сигурност на крайни точки Trelix Endpoint Security (HX) (наричан по-нататък за краткост „Треликс“). Този софтуер няма самостоятелна бизнес или административна логика и не реализира функционалности, характерни за регистрови или административни системи. В този смисъл Треликс представлява средство за откриване, анализ и ограничаване на заплахи за информационната сигурност.

Крайните точки, които следва да бъдат обхванати от софтуера за киберсигурност (работни станции и сървъри), са 10 000 на брой и са разположени в съдилищата с изключение на административните съдилища и Върховния административен съд, а централната конзола – в информационния център на ВСС.

Организацията по внедряването и използването на Треликс включва задължителното участие на Висшия съдебен съвет в качеството му на администратор на автоматизираните информационни системи за органите на съдебната власт и възложител по сключените договори, всеки съд като администратор на личните данни, обработвани под негов контрол в тези системи и „Информационно обслужване“ АД като изпълнител по сключените договори с ВСС.

В процеса по внедряването на Треликс на съответните крайни устройства в съдилищата са изразени принципни притеснения от административните ръководители на някои съдилища за начина, по който разпределението на правата за управление на функционалностите на платформата, се отразява на способността на всеки отделен съд да осъществява контрол върху достъпа на трети лица до информацията, която съдилищата съхраняват и използват в електронна форма на крайните устройства, достъпващи съответните информационните системи.

Всичко това поставя принципните въпроси от областта на защитата на личните данни, попадащи в компетентността на ИВСС по чл. 17, ал.1, т. 1 от Закона за защита на личните данни, свързани с внедряването на решението

за киберсигурност Треликс в съдилищата: осъществява ли се обработване на лични данни; какви са правните качества на отделните участници и какви са техните роли, и отговорности във връзка с обработването на лични данни; как се спазват принципите за обработване на лични данни; какви са рисковете за правата и свободите на физическите лица, засегнати от внедряването на конкретния продукт. За да изрази становище по поставените въпроси, ИВСС разгледа всички документи и становища, представени по темата за заседанията на Пленума на ВСС от 04.12.2025 г. и от 22.01.2026 г., и за заседанията на Съдийската колегия на ВСС от 27.01.2026 г., от 06.02.2026 г. и от 17.02.2026 г., до които разполага с достъп на основание чл. 32, ал. 4 от Закона за съдебната власт.

С Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), наричан по-нататък за краткост ОРЗД/Регламентът/Регламент (ЕС) 2016/679, се определят правилата относно защитата на физическите лица във връзка с обработването на лични данни, както и правилата относно свободното движение на такива данни. Регламентът се прилага за обработването на лични данни, което се извършва изцяло или частично с автоматични средства, както и за обработване с други средства на лични данни, които са част от регистър или които са предназначени да съставляват част от регистър с лични данни (чл. 2, пар. 1 от ОРЗД). В този смисъл той се прилага спрямо всеки субект, независимо от правноорганизационната му форма, който извършва една или повече операции по обработване на лични данни, попадащи в материалния му обхват. Предвид това и при отчитане на съображение 20 от Регламента, което изрично посочва приложимостта, *inter alia*, на регламента спрямо дейността на съдилищата, обработването на лични данни от съда, вкл. при изпълнение на функциите му на орган на съдебната власт, се урежда от правилата на ОРЗД (с изключение на дейността по обработване на лични данни от съда за целите на наказателното преследване на престъпления по чл. 42 от Закона за защита на личните данни (ЗЗЛД), в които случаи приложим правен акт е Глава осма от

ЗЗЛД¹). Съдът на Европейския съюз (Съдът на ЕС/СЕС) изрично посочва в редица свои решения, че „освен в случаите, посочени в член 2, параграфи 2 и 3 от Регламент 2016/679, този регламент се прилага към дейностите по обработване, извършвани както от частноправни субекти, така и от публични органи, включително – както се посочва в съображение 20 от него – съдебните органи, каквито са съдилищата“ (решение от 24 март 2022 г. по дело С-245/20, ECLI:EU:C:2022:216, т. 25 и решение от 2 март 2023 г. по дело С-268/21, ECLI:EU:C:2023:145, т. 26). Поради това, при обработването на лични данни в качеството им на органи на съдебната власт, за цели, различни от наказателното преследване на престъпления, съдилищата следва да прилагат правилата и изискванията на ОРЗД.

Компетентен да осъществява надзор върху обработването на лични данни от органите на съдебната власт (съд, прокуратура и следствени органи) при изпълнение на функциите им на органи на съдебната власт, вкл. за целите по чл. 42 от ЗЗЛД, е ИВСС. Надзорът върху обработването на лични данни от тези органи за цели, различни от посочените, се осъществява от Комисията за защита на личните данни.

Правилата на горепосочените актове (ОРЗД или ЗЗЛД) са приложими винаги, когато е налице т.нар. обработване на лични данни. Обработване на лични данни по смисъла на чл. 4, т. 2 от ОРЗД, респ. § 1, т. 4 от Допълнителните разпоредби на ЗЗЛД (ДРЗЗЛД) е операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

Във връзка с посочената легална дефиниция за обработване на лични данни следва да се има предвид, че платформи за сигурност на крайни точки с разширени функционалности (каквото представлява цялостното решение за киберзащита Треликс в конкретния случай) могат:

¹ Със Закон за изменение и допълнение на Закона за защита на личните данни (обн. ДВ, бр. 17/2019 г.) в Глава осма на ЗЗЛД са въведени разпоредбите на Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета.

- технически да позволяват целево извличане на файлове от защитаваните крайни точки;
- да предоставят детайлна информация за дейността на потребителите;
- да създадат възможност за достъп до работни файлове, включително такива, свързани с правораздавателната дейност.

Това налага внимателен анализ на допустимостта на такива платформи от гл.т. на правилата за обработването на лични данни чрез тях и на рисковете за физическите лица. Целта на такъв анализ е да се установи дали е налице правно основание за обработването и да бъдат въведени подходящи гаранции за субектите на данни на най-ранен етап, така че рисковете за техните права и свободи да бъдат сведени до приемливо ниво.

Платформата за сигурност на крайни точки Треликс по своята архитектура събира и централизира телеметрични данни за крайните устройства, които могат да включват идентификатори на потребители, системни акаунти, IP адреси и информация за активността на потребителите.

Допълнително, следните функционалности² на Треликс агентите имат отношение към обработването на лични данни, доколкото реализирането им на практика би могло да представлява една или повече самостоятелни операции по обработване съгласно горепосочената дефиниция:

1.1. Функцията Enterprise search, която позволява в уеб интерфейса на Endpoint Security (HX) да се търсят заплахи или индикатори за заплахи в крайните устройства (хостове). Търсенето се изпълнява върху файловата система и системните обекти на крайните устройства. При наличие на файлове, съдържащи лични данни (напр. proekt-reshenie.docx) търсенето представлява достъп до тях. Търсенето може да включва преглед на съдържание или метаданни. Достъпът и/или извличането на лични данни са операции по обработване на лични данни по смисъла на чл. 4, т. 2 от ОРЗД, респ. § 1, т. 4 от ДРЗЗЛД.

1.2. Функцията Data acquisition (събиране на данни), която позволява да се придобие необходимата информация от единично работещо крайно устройство. Събирането на данни може да включва файлове, части от файлове, системна информация. Ако файловете съдържат информация, съставляваща лични данни, то е налице обработване на лични данни под

² Посочените функционалности са описани в публично достъпната техническа документация на производителя, публикувана в Trellix Documentation Portal.

формата на събиране, респ. записване и съхранение съгласно горепосочените дефиниции по чл. 4, т. 2 от ОРЗД, респ. § 1, т. 4 от ДРЗЗЛД.

1.3. Функцията Requesting Triage Acquisitions (ускорена форма на събиране), която представлява механизъм за бързо събиране на данни от избрани хостове, които могат да бъдат заявявани, изпълнявани и изтегляни чрез уеб интерфейса на системата. Това е автоматизиран процес на извличане, като обхватът му зависи от конфигурацията, но потенциално включва файлове и съдържание. В този случай обработването на лични данни се осъществява под формата на извличане и/или осигуряване на достъп до данните по друг начин (чл. 4, т. 2 от ОРЗД, респ. § 1, т. 4 от ДРЗЗЛД).

1.4. Функция автоматизирано обработване посредством използване на API интерфейс, която осигурява достъп до информацията относно крайните устройства, събирането на данни (acquisitions), алармите, първоизточниците на аларми (source alerts), условията, индикаторите и изолирането на устройства (containment). Тези функционалности позволяват извършване на търсене, извличане на данни и централизирано съхраняване на резултатите.

Видно от горепосочените функции на Треликс, касае се за операции по обработване на лични данни под формата на извличане и съхранение съгласно легалната дефиниция за обработване на лични данни по чл. 4, т. 2 от ОРЗД, респ. § 1, т. 4 от ДРЗЗЛД. Предмет на обработване по този начин са данни и информация, съхранявани в крайните устройства, на които агентите са инсталирани.

Съгласно чл. 4, т. 1 от ОРЗД, респ. § 1, т. 1 от Допълнителните разпоредби на ЗЗЛД лични данни са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“). Физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за неговата идентичност (физическа, физиологична, генетична, психическа, умствена, икономическа, културна или социална идентичност).

Преценката дали дадена информация съставлява лични данни се прави във всеки отделен случай.

В редица свои решения Съдът на ЕС е постановил, че „дадена информация засяга физическо лице, което е идентифицирано или може да бъде идентифицирано, ако поради своето съдържание, крайна цел или последици тя е свързана с лице, което може да бъде идентифицирано“ (решение по дело С-604/22, ECLI:EU:C:2024:214, т. 37; решение по дело С-487/21, ECLI:EU:C:2023:369, т. 24 и решение по дело С-434/16, EU:C:2017:994, т. 35). Съгласно съображение 26 от ОРЗД, за да се определи дали дадено физическо лице може да бъде идентифицирано, следва да се вземат предвид всички средства, като например подбирането на лица за извършване на проверка, с които е най-вероятно да си послужи администраторът или друго лице, за да идентифицира пряко или непряко даденото физическо лице. За да се установи дали има достатъчна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат наличните към момента на обработване на данните технологии и технологичните развития. Съгласно решение на Съда на ЕС по дело С-604/22, ECLI:EU:C:2024:214, т. 40, „... за да могат определени данни да се квалифицират като „лични данни“ по смисъла на член 4, точка 1 от този регламент, не се изисква цялата информация, която позволява идентифицирането на субекта на данните, да се намира в ръцете на едно-единствено лице“.

Информацията, обект на обработване чрез функционалностите на Треликс, която се отнася до физически лица, обхваща: онлайн идентификатори, данни за местонахождение, данни за потребители, данни за защитавани крайни устройства, както и лични данни на физически лица, упоменати в съдържанието на файлове, които могат да бъдат достъпени чрез функционалностите на продукта. Според съдържанието си и информативната си стойност, тази информация или във всички случаи представлява лични данни, или в даден контекст би могла да съставлява лични данни на физически лица (самостоятелно или в съвкупност с други данни). В този смисъл данните за онлайн идентификатори, за местонахождение, за потребители, за защитавани крайни устройства са предварително известни категории информация и доколкото винаги са свързани с физически лица, по правило, се явяват лични данни. За разлика от тях, данните за физически лица, упоменати в съдържанието на файлове,

които могат да бъдат достъпени чрез функционалностите на продукта Треликс, представляват обобщен набор от информация, чието естество и конкретно съдържание не може да бъде предварително определено или прогнозирано. Посочената информация би могла да включва всякакви категории лични данни съгласно дефиницията на това понятие, вкл. специални категории лични данни по чл. 9, пар. 1 от ОРЗД. Такива са данните, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние, данни за сексуалния живот или сексуалната ориентация на физическо лице.

Потенциалната възможност данни от посоченото естество да бъдат достъпени чрез функционалностите на Треликс агентите произтича от предмета на делата, по които тези данни са събирани, респ. са упоменати в съдържанието на съответните файлове, съхранявани на крайните устройства в съдилищата или във файлове, които са част от информационните системи на съдилищата, доколкото същите са достъпни чрез съответните крайни устройства (напр. при изтегляне, локално съхранение или временно кеширане). Във връзка с това следва да се държи сметка за изискванията на съображение 51 от Регламента, което изрично посочва, че на личните данни, които по своето естество са особено чувствителни от гледна точка на основните права и свободи, се полага специална защита, тъй като контекстът на тяхното обработване би могъл да създаде значителни рискове за основните права и свободи.

Гореизброените набори от лични данни – предмет на евентуално достъпване чрез функционалностите на Треликс, са свързани с различни категории субекти на данни: съдии и съдебни служители (за които се отнасят съответните онлайн идентификатори, данните за местонахождение, данните за потребителите, данните за защитавани крайни устройства), участници в съдебни производства (за които се отнасят личните данни, упоменати в съдържанието на файлове, създадени и съхранени за целите на правораздаването), други физически лица, в зависимост от характера на достъпваната информация и нейния източник – напр. договори с външни изпълнители, с които са свързани определени административни дейности на съда.

Обстоятелството, че може да се извършва обработване на лични данни чрез Trellix Endpoint Security NX агенти в конкретен контекст, има за последица задължителното прилагане на изискванията за законодателството за защита на личните данни (ОРЗД и/или ЗЗЛД).

Регламент (ЕС) 2016/679 въвежда множество участници в системата за защита на личните данни: администратор на лични данни, обработващ лични данни, получател, трета страна, субект на данни, независим надзорен орган. Определянето на конкретното правно качество на участник в тази система зависи от неговото фактическо отношение към обработването на лични данни. Съгласно трайната практика на Европейския комитет по защита на данните (ЕКЗД) понятията „администратор“ и „обработващ“ са функционални (т.е. имат за цел да разпределят отговорностите в съответствие с действителната роля на страните, от действителните им дейности в конкретна ситуация) и автономни (т.е. следва да се тълкуват основно в съответствие с правото на ЕС в областта на защитата на данни, без да се засягат от други термини в други области на правото).³ Европейският комитет по защита на данните изрично посочва в своите Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, че „разпределението на ролите обикновено се основава на анализ на фактическите елементи или обстоятелства по случая и поради това не подлежи на договаряне“ (т. 12 от Насоките). Затова правилното определяне на правните качества на всички участници в обработването и дефинирането на техните роли и отговорности в този процес е от ключово значение за законосъобразното обработване на лични данни и за гарантиране упражняването на правата на субектите на данни.

Основният задължен правен субект е т.нар. администратор на лични данни. Съгласно определението по чл. 4, т. 7 от Регламента администратор е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава-членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава

³ Работна група по чл. 29, Становище 1/2010 на Работната група по член 29, РД 169, стр. 9; Европейски комитет по защита на данните, Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, стр. 10.

членка. Администраторът на лични данни носи отговорност за обработването, чиито цели и средства той е определил или чиито цели и средства е нормативно задължен да реализира. Администратори на лични данни в конкретния случай се явяват Висшият съдебен съвет и съдилищата.

Висшият съдебен съвет е конституционноустановен, постоянно действащ орган (юридическо лице), който представлява съдебната власт, осигурява и отстоява нейната независимост, определя състава и организацията на работа на съдилищата, прокуратурите и следствените органи и обезпечава финансово и технически тяхната дейност, без да се намесва в нейното осъществяване (чл. 130 от Конституцията на Република България; чл. 16 от Закона за съдебната власт). При обработването на лични данни, което той осъществява, ВСС се явява администратор съгласно чл. 4, т. 7 от ОРЗД и следва да обработва лични данни при спазване на изискванията на Регламента. Надзор върху неговата дейност по обработване на лични данни осъществява Комисията за защита на личните данни на основание чл. 6 от ЗЗЛД.

Съдилищата, в качеството си на юридически лица и органи на съдебната власт обработват лични данни както за целите на правораздаването, така и за административните си дейности, поради което се явяват администратори на лични данни по смисъла на чл. 4, т. 7 от ОРЗД. Доколкото се касае за администратори-публични органи, целите и средствата за обработването на лични данни по правило са определени от приложимото към дейността на съдилищата материално и процесуално законодателство (правото на ЕС или националното законодателство). В зависимост от конкретните цели, за които обработват лични данни, съдилищата са обект на надзор, както следва: от ИВСС – при обработване на лични данни за целите на правораздаването; от КЗЛД – при обработване за всички останали цели (извън функциите на орган на съдебната власт).

„Информационно обслужване“ АД, поради характера на дейността си, която фактически извършва или се очаква да извършва в конкретния случай (наблюдение и управление на информационно-комуникационна инфраструктура и осъществяване на дейности, свързани с киберсигурността), се явява обработващ лични данни. Съгласно чл. 4, т. 8 от Регламента обработващ лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора. Обработващият лични данни следва да

обработва данните само по документирано нареждане на администратора, освен когато задължението за обработването произтича от правото на Съюза или приложимото национално законодателство. Поради обстоятелството, че обработващият по правило действа от името на администратора, Регламентът въвежда завишени изисквания по отношение контрола, който администраторът е длъжен да упражнява в случаите на възлагане на обработване от обработващ. Разпоредбата на чл. 28 съдържа подробни изисквания по отношение: критериите за избор на обработващ лични данни; ограниченията, които обработващият следва да спазва относно привличането на други обработващи; правния акт или договора, от който произтичат задълженията на обработващия спрямо администратора и неговото минимално изискуемо съдържание. Неспазването на тези изисквания от администратора и/или от обработващия съставлява състав на административно нарушение съгласно чл. 83, пар. 4, б. „а“ от ОРЗД, което подлежи на административно наказание „глоба“ или „имуществена санкция“ в размер до 10 000 000 евро, или, в случай на предприятие – до 2% от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока. Надзор върху обработването, което се извършва или ще се извършва от „Информационно обслужване“ АД в конкретния случай, е компетентна да осъществява Комисията за защита на личните данни.

Въпреки че дефинирането на целите и средствата е прерогатив на съответния администратор на лични данни, в практиката си ЕКЗД застъпва разбирането, че е допустима известна свобода на действие в това отношение и от страна на обработващия⁴. При включване в дейностите по обработване на обработващ, който разполага със специални познания спрямо операциите по обработване, които му се възлагат, няма пречка на този обработващ да бъде делегиран изборът на т.нар. средства за обработване от второстепенна важност (напр. изборът на конкретен хардуер или софтуер или подробните мерки за сигурност⁵). Както отбелязва ЕКЗД в своите Насоки 07/2020, обработващият лични данни обработва лични данни „в полза на администратора“ (т. 79), поради което е допустимо администраторът да му

⁴ Европейски комитет по защита на данните, Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, стр. 16.

⁵ Пак там, стр. 17.

предостави свобода на преценка относно това „как най-добре да бъдат обслужвани неговите интереси“ (т. 80).

Отговорност за определянето на средствата от първостепенна важност винаги носи администраторът. Такива средства са категориите лични данни-предмет на обработване, категориите субекти на данни, категориите получатели, продължителността на обработването, както и всички други параметри, свързани със законосъобразността на обработването, неговата необходимост и пропорционалност⁶. Дори на обработващия лични данни да е делегирана възможността да взема решения относно средствата за обработване от второстепенна важност, решенията относно целите на обработването и контролът върху самото обработване са единствено и само в отговорността на администратора. Затова дейностите, които „Информационно обслужване“ АД в качеството си на обработващ извършва или се очаква да извършва във връзка с използването на функционалностите на Треликс агентите, следва да бъдат съобразени с императивните разпоредби на ОРЗД, по-специално с изискванията на чл. 28.

Разпоредбата на чл. 28, пар. 3 от Регламент (ЕС) 2016/679 изисква обработването от обработващ лични данни да бъде уредено с договор или с друг правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора и който регламентира всички изброени в тази разпоредба въпроси. При отчитане на статута на ВСС и на изискванията на чл. 16 от Закона за съдебната власт (ЗСВ), при необходимост от осъществяване на дейности по обработване от външен за съдилищата изпълнител, този договор следва да бъде сключен между ВСС и съответния обработващ лични данни, в писмена форма, вкл. в електронен формат (чл. 28, пар. 9). С факта на сключването му възниква задължение за външния изпълнител да обработва лични данни от името на администраторите (съдилищата) в обхват и обем, определени с това възлагане. Обвързването на обработващия в конкретния случай („Информационно обслужване“ АД) спрямо администраторите (съдилищата) с клаузите относно предмета, срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни, както и със задълженията по чл. 28, пар. 3 е

⁶ Пак там, стр. 17.

важно не само за спазване на формалните изисквания на Регламента, но и за осигуряване на законосъобразността на обработването от този обработващ.

Следва да се има предвид, че самият избор на обработващ трябва да е съобразен с изискванията на чл. 28, пар. 1 от ОРЗД, който налага използването само на обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на регламента и да осигурява защита на правата на субектите на данни. Преценката дали гаранциите са достатъчни се отнася до експертните познания на обработващия лични данни, надеждността му и ресурсите, с които разполага (съображение 81). Важен аспект от този процес (избора на обработващ и свързаната с това договореност по чл. 28 от Регламента) са конкретните задачи и отговорности, които се възлагат на външния изпълнител в контекста на обработването, както и рискът за правата и свободите на субектите на данни (по арг. от съображение 81).

Обработването на лични данни (в смисъл всяка отделна операция по обработване съгласно дефиницията по чл. 4, т. 2 от ОРЗД, респ. § 1, т. 4 от ДРЗЗЛД) трябва да се извършва въз основа на правно основание и при спазване на изискванията на чл. 5 от Регламента (принципите, свързани с обработването на лични данни). Задължението за едновременното наличие на правно основание за обработване на лични данни и за прилагане на принципите по чл. 5 е ясно очертано в практиката на Съда на ЕС. Изрично в този смисъл съдът се е произнесъл с решения както по отменената Директива 95/46/ЕО, така и по ОРЗД, като например решение от 30 май 2013 г. по дело C-342/12, ECLI:EU:C:2013:355, т. 33; решение от 2 март 2023 г. по дело C-268/21, ECLI:EU:C:2023:145, т. 43; решение от 6 октомври 2020 г. по съединени дела C-511/18, C-512/18 и C-520/18, ECLI:EU:C:2020:791, т. 208; решение от 16 декември 2008 по дело C-524/06, ECLI:EU:C:2008:724, т. 48; решение от 22 юни 2021 г. по дело C-439/19, ECLI:EU:C:2021:504, т. 96; решение от 27 септември 2017 г. по дело C-73/16, ECLI:EU:C:2017:725, т. 104.

Изискването за наличие на правно основание за обработване на лични данни е спазено, ако обработването се извършва въз основа на някое от условията по чл. 6 (законосъобразност на обработването) или чл. 9 (обработване на специални категории лични данни) от ОРЗД. Преценката за това коя група правни основания е приложима в даден случай (групата по

чл. 6 или по чл. 9) зависи от естеството на личните данни – предмет на обработване. Разпоредбата на чл. 9 се отнася единствено до обработване на т.нар. специални категории лични данни⁷; обработването на всички останали категории лични данни се обхваща от нормата на чл. 6.

С правно основание за обработване на лични данни разполага само и единствено администраторът на лични данни. Това положение е пряка последица от факта, че администраторът определя целите и средствата на обработването, които са основополагащите аспекти на обработването и съобразно които се дефинира и самото правно качество „администратор на лични данни“. Поради това, че обработващият обработва лични данни от името на администратора (по арг. на чл. 4, т. 8 от ОРЗД, респ. § 1 т. 3 от ДРЗЗЛД), той не разполага със собствено правно основание за обработването за целите, дефинирани от администратора. Затова, ако излезе от пределите на документираните нареждания на администратора, респ. сам определи целите и средствата на обработването, обработващият се счита за администратор по отношение на това обработване (чл. 28, пар. 10 от регламента). Важно е да се отбележи обаче, че самото обработване в този случай би било незаконосъобразно поради липса както на правно основание по чл. 6 или чл. 9, съответно по чл. 49 от ЗЗЛД, така и поради нелегитимност на целите на обработване по чл. 5, пар. 1, б. „б“ от ОРЗД, респ. по чл. 45, ал. 1, т. 2 от ЗЗЛД.

В чл. 6 от ОРЗД изчерпателно са изброени хипотезите, при които обработването на лични данни, спрямо които тази разпоредба се прилага, се счита за законосъобразно (в този см. решение на СЕС от 8 декември 2022 г. по дело C-180/21, ECLI:EU:C:2022:967, т. 83 и решение от 11 декември 2019 г. по дело C-708/18, ECLI:EU:C:2019:1064, т. 37). По-специално, „... за да може обработване на лични данни да се счита за законно, то трябва да спада към един от случаите, предвидени в посочения член 6“ (решение от 22 юни 2021 г. по дело C-439/19, ECLI:EU:C:2021:504, т. 99; в този см. и решение от 11 декември 2019 г. по дело C-708/18, ECLI:EU:C:2019:1064, т. 38).

Съдилищата, като администратори на лични данни, обработват лични данни при изпълнение на функциите си на орган на съдебната власт на

⁷ Специални категории лични данни са данните, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние, данни за сексуалния живот или сексуалната ориентация на физическо лице.

основание чл. 6, пар. 1, б. „д“ (за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора). Като се има предвид разпоредбата на чл. 6, пар. 3 от ОРЗД основанието за това обработване произтича от правото на Съюза или от националното право. На практика това означава, че правното основание може да бъде материалноправна или процесуалноправна разпоредба (в този смисъл е решение от 2 март 2023 г. на Съда на ЕС по дело C-268/21, ECLI:EU:C:2023:145, т. 40). Специални категории лични данни съдилищата обработват на основание чл. 9, пар. 2, б. „е“ от ОРЗД, т.е. винаги, когато съдилищата действат в качеството си на правораздавателни органи.

При обработването на лични данни за дейности, които съдилищата осъществяват извън правораздавателните си функции, правното основание може да варира: напр. необходимост от спазване на законово задължение, което се прилага спрямо администратора (чл. 6, пар. 1, б. „в“ от ОРЗД); за целите на легитимните интереси на администратора или на трета страна, когато тези интереси имат преимущество пред интересите или основните права и свободи на субекта на данни, които изискват защита на личните данни (чл. 6, пар. 1, б. „е“ от ОРЗД); за целите на изпълнението на задълженията на администратора по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила (чл. 9, пар. 2, б. „б“ от ОРЗД). В този смисъл е и разпоредбата на чл. 42, ал. 3 от ЗЗЛД, която препраща към ОРЗД като приложим правен инструмент във всички случаи, в които обработването на лични данни от компетентните органи по чл. 42, ал. 1 от ЗЗЛД е за цели, различни от предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания. Предвид това, в анализа по-долу са отчетени единствено нормите на ОРЗД, които се явяват приложими в конкретния контекст.

По принцип за всяка отделна операция по обработване по чл. 4, т. 2 от ОРЗД е необходимо самостоятелно правно основание. В конкретния случай особеност представлява обстоятелството, че обработването на лични данни може да възникне като резултат от използването на функционалностите на Треликс агентите в определен контекст, например при реагиране на събития, свързани с киберсигурността. Касае се за обработване, произтичащо от предназначението на Треликс като средство за кибер защита. Тази особеност

на посочения продукт, свързана с необходимостта за осигуряване на сигурност, е отчетена и в самия Регламент. В съображение 49 се посочва, че обработването на лични данни в степен, която е строго необходима и пропорционална на целите на гарантирането на мрежовата и информационната сигурност, т.е. способността на дадена мрежа или информационна система да издържа, със съответно равнище на доверие, на случайни събития или неправомерни или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхраняваните или предаваните лични данни, както и на сигурността на свързаните услуги, предлагани или достъпни посредством тези мрежи и системи, от страна на публични органи, екипи за незабавно реагиране при компютърни инциденти (ЕНРКИ), екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), доставчици на мрежи и услуги за електронни съобщения и доставчици на технологии и услуги за сигурност, представлява законен интерес на съответния администратор на данни. Това може да включва например предотвратяването на непозволен достъп до електронни съобщителни мрежи и разпространение на зловреден софтуер и спиране на атаки с цел отказване на услугите и вреди за компютрите и електронните съобщителни системи.

Обстоятелството, че самият Регламент квалифицира обработването за горепосочените цели като обработване, представляващо законен интерес на администратора, не означава обаче, че администраторът може директно да се позове на чл. 6, пар. 1, б. „е“ от ОРЗД (т.нар. легитимен интерес за обработване на лични данни) като правно основание за извършването му. За да бъде валидно правно основание за обработване посочената разпоредба, е необходимо да бъде извършен тест за баланса (тест за пропорционалност) между легитимните интереси на администратора или на трета страна и интересите, правата и свободите на засегнатите субекти на данни. Разпоредбата на чл. 6, пар. 1, б. „е“ би била приложимо условие за допустимост на обработването, само ако въз основа на този тест за баланса бъде направен извод за наличие на превес/преимущество на интереса на администратора или на третата страна над интересите или над основните права и свободи на субектите на данни, които изискват защита на личните данни. Като се отчита статутът на една от категориите субекти на данни – съдиите, които се ползват по закон с независимост (чл. 117, ал. 2 от Конституцията на Република България; чл.1а, ал. 2 от Закона за съдебната

власт) и подчинеността на съдебните служители спрямо администратора в работен контекст, което ги прави уязвима категория субекти на данни, едва ли би могло да се изведе извод, че интересът на администратора има преимущество пред интересите, правата и свободите на засегнатите физически лица. В допълнение, следва да се има предвид, че правното основание по чл. 6, пар. 1, б. „е“ от регламента (легитимните интереси на администратора или на трета страна) е неприложимо, когато обработването се извършва от публични органи при изпълнението на техните задачи (чл. 6, пар. 1, алинея втора от ОРЗД).

Във връзка с необходимостта от обработване на лични данни чрез Треликс за гарантирането на мрежовата и информационната сигурност следва да се отчете и относимото национално законодателство за тези цели. Значително близка по съдържание със съображение 49 от Регламента е разпоредбата на чл. 2, ал. 3 от Закона за киберсигурност, която регламентира понятието „мрежова и информационна сигурност“.

След влизането на 17 февруари 2026 г. в сила на изменения и допълнения на Закона за киберсигурност (обн. ДВ, бр. 17/2026 г.) в обхвата на този закон са включени органите на съдебната власт. С § 55 от Закона за изменение и допълнение на Закона за киберсигурност е направено допълнение в Закона за съдебната власт, с което са разширени правомощията на Пленума на ВСС. Съгласно чл. 30, ал. 2, т. 24 от ЗСВ на Пленума на ВСС са възложени функциите на национален компетентен орган за органите на съдебната власт (субекти по чл. 4, т. 9 от Закона за киберсигурност). Като такъв той има задължения за упражняване на контрол за спазване на изискванията на този закон по отношение органите на съдебната власт (чл. 27е, ал. 1, т. 1 от Закона за киберсигурност във вр. с чл. 30, ал. 2, т. 24 от ЗСВ). Доколкото внедряването на Треликс би могло да съставлява мярка по киберсигурност по смисъла на чл. 3, ал. 1 от Закона за киберсигурност, при наличие на решение на Пленума на ВСС за интегрирането му в инфраструктурата на съдебната власт, приложимото правно основание за обработване на лични данни чрез неговите функционалности би била нормата на чл. 6, пар. 1, б. „в“ от ОРЗД (обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора). Няма правна пречка чрез това техническо средство да бъдат изпълнени едновременно както задълженията за сигурност на обработването по ОРЗД, така и на Закона за киберсигурност,

при условие че то покрива съответните изисквания и в двете предметни области, напр. да гарантира постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване (правораздаване, управление на човешките ресурси и др.). Наличието на правно основание за обработване на лични данни чрез Треликс като мярка за киберсигурност обаче, не изключва задълженията на съдилищата по ОРЗД във връзка с това обработване, по-специално спазването на принципите по чл. 5 и защитата на правата на физическите лица.

За разлика от задължението за законосъобразност на обработването, което изисква наличие само на една от хипотезите по чл. 6, принципите, свързани с обработването на лични данни по чл. 5, се прилагат кумулативно. Тези принципи са „законосъобразност, добросъвестност и прозрачност“, „ограничение на целите“, „свеждане на данните до минимум“, „точност“, „ограничение на съхранението“, „цялостност и поверителност“ и „отчетност“. Посочените принципи имат отношение и следва да се прилагат спрямо обработването на всички регистри с лични данни, които съдилищата поддържат като администратори. В случая обаче отношение към внедряването на Треликс агентите имат по-специално принципите „законосъобразност, добросъвестност и прозрачност“, „цялостност и поверителност“, „ограничение на целите“, „ограничение на съхранението“ и „отчетност“.

Елементът „законосъобразност“ се изразява в наличието на правно основание за обработване на личните данни. В допълнение към анализа по-горе относно допустимостта на обработването на данни чрез Треликс агентите е важно да се отбележи, че въпреки алтернативния характер на правните основания за обработване на лични данни по чл. 6, пар. 1 от Регламента, те не са взаимнозаменяеми. Изборът на подходящо правно основание зависи както от целите на обработването, така и от приложимата към обработването правна уредба. Наличието на повече от едно условие за допустимост не води автоматично до кумулиране на съответните условия. За да бъде легитимно обработването на лични данни, е достатъчно да е налице само едно валидно правно основание. То обаче трябва да е подходящо за конкретната цел на обработване. В този смисъл, при наличие на законово задължение по чл. 6, пар. 1, б. „в“ не е необходимо да се прибегва до чл. 6, пар. 1, б. „е“ от Регламента (легитимен интерес на администратора или на трета страна, който има преимущество пред интересите или основните права

и свободи на субекта на данни). Наличието на законово задължение придава императивен характер на самото обработване, за разлика от обработването на основание легитимен интерес, което изисква доказване на надделяващия интерес на администратора. Както отбелязва Съдът на ЕС в свои решения по дело C-252/21, EU:C:2023:537, т. 94 и дело C-621/22, EU:C:2024:858, т. 32, „когато е възможно да се констатира, че дадено обработване на лични данни е необходимо от гледна точка на едно от основанията, предвидени в член 6, параграф 1, първа алинея, букви б) – е) от ОРЗД, не се налага да се проверява дали това обработване попада в обхвата и на друго от тези основания“.

Следва да се отбележи, че правното основание трябва да е налице преди да стартира самото обработване. Възникването му впоследствие (когато обработването фактически е започнало) не може да валидира вече извършени операции по обработване.

Изискванията на Регламента за прозрачност на обработването налагат предоставянето на информация за внедряването на Треликс агентите на засегнатите физически лица, в т.ч. на информация относно рисковете, свързани с това конкретно обработване. Спазването на задължението за прозрачност само по себе си е важна гаранция за защита на правата, свободите и интересите на физическите лица.

Що се отнася до изискването за добросъвестност на администратора при прилагането на цялостното решение за киберзащита, то спазването на всички останали принципи за обработване на данни и предприемането на мерки за недопускане на масово или неизбирателно извличане на данни от крайни точки чрез Треликс агентите би гарантирало добросъвестност на обработването.

Предвид предназначението на Треликс, а именно техническо средство за киберзащита, неговото внедряване и употреба е пряко свързано и със съдържанието на принципа „цялостност и поверителност“ (чл. 5, пар. 1, б. „е“ от ОРЗД). Съгласно този принцип личните данни следва да бъдат обработвани по начин, който им гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. Тези изисквания пряко кореспондират със задължението на администраторите за осигуряване на сигурност на обработването по чл. 32 от Регламента чрез

прилагането на подходящи технически и организационни мерки за сигурност.

Решението относно това какви технически и организационни мерки ще бъдат внедрени в конкретното обработване на лични данни с цел гарантиране на подходящо ниво на сигурност зависи от нивата на риска, които тези мерки се очаква да минимизират или да неутрализират. Съгласно съображение 76 от Регламента рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до риск или до висок риск. Във връзка с това европейският законодател въвежда различни задължения за администратора на лични данни за управление на сигурността: задължително провеждане на оценка на риска с цел определяне на нивото на риск, която трябва да бъде извършена преди да започне самото обработване; извършване на оценка на въздействието върху защитата на данните (ОВЗД), ако оценката на риска покаже наличието на висок риск; провеждане на предварителна консултация, ако ОВЗД покаже наличие на висок остатъчен риск.

Съображение 83 от Регламент (ЕС) 2016/679 гласи: с цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на настоящия регламент, администраторът или обработващият лични данни следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид достиженията на техническия прогрес и разходите по изпълнението спрямо рисковете и естеството на личните данни, които трябва да бъдат защитени. При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, материални или нематериални вреди. Задължението за осигуряване на подходяща степен на сигурност и поверителност се отнася не само до личните данни-предмет на обработване, но и до оборудването за тяхното обработване (съображение 39).

Управлението на рисковете за правата и свободите на физическите лица е задача, която не се изчерпва с действието „анализ/оценка на риска“.

То е процес, който изисква тези рискове „редовно да се идентифицират, анализират, преценяват, оценяват, третира (например като се ограничават) и преразглеждат“⁸.

При идентифициране на висок риск, обработването задължително трябва да бъде предшествано от извършване на оценка на въздействието върху защитата на данните съгласно изискванията на чл. 35 от ОРЗД. В своите Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679 Работната група по член 29⁹ разглежда ОВЗД като инструмент за отчетност. Съгласно определението, което Работната група дава на този инструмент, оценката на въздействието „представлява процес, чиято цел е да опише обработването, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни, като ги оцени и определи мерки за справяне с тези рискове“.

Разпоредбата на чл. 35 от Регламент (ЕС) 2016/679 съдържа неизчерпателен списък на ситуации по обработване, в които извършването на оценка на въздействието е задължително поради високия риск, който това обработване поражда. По правило предмет на оценката е една или повече сходни операции по обработване. Изрично в своите Насоки Работната група за защита на личните данни обаче посочва, че обект на ОВЗД може да бъде и даден технологичен продукт (напр. хардуер или софтуер, ако се планира използването му от различни администратори за различни операции по обработване). В този смисъл, в конкретния случай с агентите Треликс, няма пречка, ако оценката на риска покаже наличието на високи рискове за правата и свободите на физическите лица, да бъде извършена ОВЗД на самия продукт за киберзащита. Това дори би било целесъобразно: да има една – единствена ОВЗД, от която да се ползват всички съдилища,

⁸ Работна група за защита на личните данни по член 29. Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679 (стр. 6).

⁹ Работната група по член 29 е независим консултативен орган в областта на защитата на личните данни съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни. С Регламент (ЕС) 2016/679, който отменя Директива 95/46/ЕО, считано от 25 май 2018 г. е създаден Европейски комитет по защита на данните, който е орган на ЕС и притежава правосубектност. Този комитет осигурява съгласуваното прилагане на Регламент (ЕС) 2016/679.

участващи в инициативата за внедряване на това цялостно кибер решение. Подобен подход е възприет и от самия Регламент, който в съображение 92 посочва, че при определени обстоятелства може да бъде разумно и рентабилно предметът на дадена оценка на въздействието върху защитата на данните да обхваща повече от един проект, например когато обществени органи или структури възнамеряват да създадат общо приложение или платформа за обработване на данни или когато няколко администратори планират внедряването на общо приложение или среда за обработване на данните в цял промишлен сектор или сегмент или за широко използвана хоризонтална дейност.

Следва да се отбележи, че дори при съмнение дали да се извършва ОВЗД, Работната група препоръчва прибегването до този инструмент за отчетност предвид неговата полезност от гл.т. на законодателството за защита на личните данни. В своите Насоки Работната група извежда девет критерия, които да бъдат вземани под внимание при извършване на преценка дали операции по обработване има вероятност да доведат до висок риск. Два от тези критерии, относими и в конкретния случай, са „систематично наблюдение“ и „данни относно уязвими субекти на данни“. Сред примерите за обработване, които Работната група дава като високорискови дейности, които изискват извършването на ОВЗД на базата на тези два критерия, са систематичното наблюдение на дейностите на служители, вкл. наблюдение на работните станции на служителите, дейността им в интернет и др.

В Насоките се обръща внимание, че „на колкото повече критерии отговаря обработването, толкова по-вероятно е да поражда висок риск за правата и свободите на субектите на данни, поради което ще изисква ОВЗД независимо от мерките, които администраторът планира да въведе“¹⁰. Едновременно с това Работната група посочва, че „в някои случаи администраторът може да заключи, че обработване, което отговаря само на един от тези критерии, изисква ОВЗД“. Независимо от това, Работната група не изключва възможността дадена операция по обработване да отговаря на критериите за високорисково обработване „и все пак администраторът да заключи, че не „съществува вероятност да породи висок риск“. Този подход

¹⁰ Пак там, стр. 11-12.

обаче налага мотивирано документиране на причините, поради които не следва да се извършва ОВЗД.

Важно е да се отбележи, че използването на нови технологии също е изрично включено в хипотезите по чл. 35, пар. 1 от ОРЗД, които изискват задължителното провеждане на ОВЗД. Преценката дали „внедряването на едно или друго техническо решение“ може да се окачестви като „използване на нови технологии“ е на администратора.

Въпреки че Регламентът въвежда ОВЗД като инструмент за управление на рисковете преди обработването реално да е започнало, такава оценка следва да бъде извършена и при вече започнали операции по обработване, когато има вероятност те да породят висок риск за правата и свободите на физическите лица, какъвто е настоящият казус. В този случай се отчита промяната в рисковете, която е настъпила като се вземат предвид естеството, обхватът, контекстът и целите на обработването.¹¹

Предвид горното, може да се обобщи, че преценката дали е налице висок риск за правата и свободите на физическите лица трябва да отчита спецификите на конкретния контекст на обработване. В такъв аспект трябва да се преценят и рисковете от инсталирането на Треликс агентите на крайните устройства в съдилищата.

Задължението за извършване на ОВЗД е на администратора на лични данни. Няма пречка обаче тя фактически да бъде извършена от външно за организационната структура на администратора лице съобразно неговата компетентност. Това обаче не освобождава администратора от отговорността, която по принцип носи за изпълнение на това задължение.

При включване в обработването на обработващ, чл. 28, пар. 3, б. „е“ от Регламента задължава последния да подпомага администратора при изпълнение на задълженията му за управление на рисковете, в т.ч. при извършване на ОВЗД (чл. 32-36). Съгласно съображение 95 от Регламента обработващият лични данни следва да подпомага администратора, за да се гарантира спазването на задълженията, произтичащи от извършването на оценки на въздействието върху защитата на личните данни и от предварителната консултация с надзорния орган, което обработващият прави при необходимост и при поискване. Посоченото в съображение 95 решение се явява напълно относимо в случая с Треликс, с оглед на това, че

¹¹ Пак там, стр. 14.

външният изпълнител е най-наясно с естеството на обработването с този продукт и с рисковете, които неговите функционалности пораждаат. „Това, че обработващият лични данни е длъжен да подпомага администратора не представлява прехвърляне на отговорността, тъй като задълженията са наложени на администратора“¹².

Съображение 90 от Регламента посочва, че ОВЗД има за цел да се оценят конкретната вероятност и тежестта на високия риск, като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска. Тази оценка следва да включва планираните мерки, гаранции и механизми за ограничаване на високия риск. Поради технологичната си неутралност Регламентът не указва конкретна методика, по която да бъде проведена ОВЗД, а оставя тази преценка на администратора. Насоките на Работната група обаче съдържат ясно дефинирани критерии, на които следва да отговаря ОВЗД. На базата на тези критерии на практика може да се извърши и самата ОВЗД.

Ако оценката на въздействието върху защитата на данните покаже наличието на т.нар. висок остатъчен риск (риск, който не може да бъде намален до приемливо ниво въпреки наличните мерки, с които разполага администраторът), администраторът следва да проведе предварителна консултация с надзорния орган (чл. 36). В рамките на тази консултация надзорният орган изразява становище по планираното обработване, като може да използва всяко от правомощията си по чл. 58 от ОРЗД.

Въз основа на рисковете, които са идентифицирани в хода на дейностите по управление на сигурността, посочени по-горе (оценка на риска – оценка на въздействието – предварителна консултация: което е приложимо в съответния контекст), администраторът следва да дефинира и приложи към операциите по обработване набор от технически и организационни мерки. При избора на такива мерки администраторът следва да отчита целите, които се постигат с тях: гарантиране сигурност на обработването (чл. 5, пар. 1, б. „е“ и чл. 32), защита на правата и свободите на физическите лица (чл. 1, съображение 1 и съображение 10) и осигуряване на отчетност (чл. 5, пар. 2 и чл. 24). Това налага мерките, които администраторът дефинира и прилага, да са подходящи. Регламент (ЕС)

¹² Европейски комитет по защита на данните. Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, т. 138.

2016/679 обаче не указва конкретни мерки, които да се считат за подходящи, а предоставя свободата за преценка на съответния администратор на лични данни, респ. обработващ лични данни. Обстоятелството, че Регламентът посочва някои мерки (напр. мерките по чл. 32, чл. 25), не променя технологично неутралния му характер. Изброяването на такива мерки е само примерно и неизчерпателно. Подобен подход е в съответствие с принципа „отчетност“ по чл. 5, пар. 2, съгласно който администраторът носи отговорност за спазването на принципите, свързани с обработването на лични данни и за доказване на съответствие на поведението си с тях. Като пример за подходяща мярка в чл. 32, пар. 1, б. „г“ от Регламента е посочен и самият процес по редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването. Задължението администраторът да докаже ефективността на съответните предприети мерки е изрично посочено в съображение 74.

Предвид това, важен аспект в този процес е преценката, че конкретна техническа и/или организационна мярка е подходяща спрямо рисковете, които обработването поражда. Отправна точка за тази преценка е кумулативното съобразяване на критериите, посочени в чл. 24, чл. 25 и чл. 32: достиженията на техническия прогрес, разходите за прилагането, естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, които (планираното) обработване поражда. Важно е да се отбележи, че за да се счита за подходяща дадена мярка, тя трябва да е относима към целите, за реализирането на които се въвежда (сигурност на обработването, защита на правата и свободите на физическите лица и отчетност на обработването), както и да бъде ефективна и съразмерна спрямо тях.

Ако част от горепосочените критерии са със сравнително обективен характер (достиженията на технически прогрес, разходите за прилагането, естеството, обхват, контекста и целите на обработването), то идентифицирането на рисковете, които обработването би породило за правата и свободите на физическите лица, изисква анализ и оценка. С оглед целта на Регламента по чл. 1, пар. 2 – защита на основни права и свободи на физическите лица и по-специално на правото на защита на личните им данни, идентифицирането на рисковете за тези права и свободи, които обработването поражда, е ключов компонент на „формулата“ за определяне

на подходящи технически и организационни мерки. Това положение е израз на решението на европейския законодател. Общият регламент относно защитата на данните да бъде изграден върху т.нар. подход, основан на риска. Риск по смисъла на § 1, т. 16 от Допълнителните разпоредби на Закона за защита на личните данни е възможността за настъпване на имуществена или неимуществена вреда за субекта на данните при определени условия, оценена от гледна точка на нейната тежест и вероятност. Съображение 76 от Регламента указва, че вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването.

Регламентът съдържа неизчерпателен списък с евентуални неблагоприятни последици, които могат да произтекат от обработването на лични данни. Съгласно съображение 75 от ОРЗД рискът за правата и свободите на физическите лица, с различна вероятност и тежест, може да произтича от обработване на лични данни, което би могло да доведе до физически, материални или нематериални вреди, по-специално когато обработването може да породви дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия; или когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално на деца; или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни.

Предвид функционалностите на Треликс агентите не може да бъдат пренебрегнати рисковете за правата и свободите на физическите лица, които тяхната употреба би могла да породии в процеса по обработване на личните им данни. Рисковете могат да произтичат от инвазивния характер, който използването на Треликс придава на обработването (достъп, извличане, записване, съхранение на данни; наблюдение на поведението), от включването в процеса на използването му на трето външно за съдилищата лице („Информационно обслужване“ АД), от факта на използването му в трудовия контекст (по отношение на служители, които са в йерархично подчинение спрямо съответните работодатели – административните ръководители на съдилищата, както и по отношение на съдии, които, по подразбиране, се ползват с функционална независимост при осъществяване на правомощията си), от мащабите на употребата му – планира се внедряването му във всички 151 общи съдилища, с изключение на ВАС и административните съдилища.

С оглед на горното и предвид факта, че технически и организационни мерки се предприемат с цел осигуряване на сигурност на обработването, защита на правата и свободите на физическите лица и осигуряване на отчетност, за да бъде обективна преценката дали планираната техническа мярка Треликс е подходяща, наред с горните рискове от внедряването му, следва да бъдат отчетени и положителните ефекти от употребата на този кибер агент: неговото предназначение да служи като технологична/техническа мярка, която, съобразно нивото на текущото технологично развитие, може да осигури защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане. В този смисъл Треликс представлява не само технологично решение, което би могло сериозно да накърни личната сфера на физическите лица, но и мярка, която би следвало да осигури необходимото ниво на киберсигурност на съдилищата, вкл. при обработването на лични данни. Следва да се отбележи, че съобразно това предназначение на Треликс като средство за киберзащита би следвало да се извърши преценка дали предприетите мерки за сигурност са подходящи и в случай на настъпване на нарушение на сигурността на личните данни. Един от елементите, който подлежи на оценка при нарушение на сигурността, са обстоятелствата, свързани с нарушението, включително дали личните данни са били защитени чрез подходящи технически мерки за защита (в този смисъл са

съображение 88, чл. 33, пар. 3, б. „г“ и чл. 34, пар. 3, б. „а“). Затова, дефинирането на подходящи технически и организационни мерки за защита на личните данни съобразно критериите по чл. 25 и чл. 32 от Регламента е не само израз на формално спазване на неговите изисквания, но и доказателство за добросъвестността на администратора.

Поставено в по-широк контекст, изпълнението на задължението за предприемане на подходящи технически и организационни мерки с цел спазване изискванията на ОРЗД и защита на правата на субектите на данни следва да започне на най-ранен етап. Съгласно чл. 25, пар. 1 от Регламента, който установява принципа за защита на данните на етапа на проектирането, администраторът е длъжен да въведе такива мерки още към момента на определянето на средствата за обработване, като следва да ги прилага и към момента на самото обработване. Мерките по чл. 25, пар. 1 са пряко насочени към ефективното прилагане на принципите, свързани с обработването на лични данни по чл. 5, които принципи синтезират философията на Регламента. От своя страна, задължението за защита на данните по подразбиране по чл. 25, пар. 2 изисква, чрез подходящи технически и организационни мерки да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването.

Изискванията на чл. 25 за защита на данните на етапа на проектирането и по подразбиране, въпреки абстрактната им формулировка, имат практическо изражение във всички случаи на обработване на лични данни. Съгласно съображение 78 от Регламента при разработването, проектирането, подбора и използването на приложения, услуги и продукти, които се основават на обработване на лични данни или обработват лични данни, за да изпълнят функцията си, производителите на продукти, услуги и приложения следва да бъдат насърчавани да вземат предвид правото на защита на лични данни при разработването и проектирането на такива продукти, услуги и приложения и като отчитат надлежно достиженията на техническия прогрес, да се уверят, че администраторите и обработващите лични данни са в състояние да изпълняват своите задължения за защита на данните. Регламентът въвежда задължение принципите на защита на данните на етапа на проектирането и по подразбиране да се вземат предвид и в контекста на процедурите за възлагане на обществени поръчки. В изпълнение на това задължение, разпоредбата на чл. 48, ал. 7 от Закона за

обществените поръчки изисква, когато предметът на поръчката е разработване, проектиране и използване на услуги и продукти, които се основават на обработване на лични данни или обработват лични данни, и когато съответното обработване на лични данни попада в материалния обхват на Регламент (ЕС) 2016/679, техническите спецификации, които определят характеристиките на предмета на поръчката, да бъдат съобразени с правилата за защита на лични данни съгласно чл. 25 от същия Регламент.

Важна особеност по отношение съдебната система е обстоятелството, че ВСС е органът, който има нормативно задължение да осигурява съответните информационни системи, в които се обработват лични данни, както и да решава други организационни въпроси, които са общи за органите на съдебната власт. Той се явява и възложител на съответните обществени поръчки във връзка с това. ВСС обаче осъществява тези свои правомощия не в качеството си на администратор на лични данни по см. на ОРЗД по отношение на обработването на лични данни, което той осъществява, а в качеството си на постоянно действащ орган по чл. 130 и чл. 130а от КРБ и чл. 16 ЗСВ. На практика обаче, в изпълнение на тези свои нормативни задължения ВСС с решенията си влияе пряко върху определянето на (целите и) средствата за обработване на лични данни от органите на съдебната власт, респ. на техническите и организационни мерки за защита, които иначе Регламентът възлага като отговорност на съответния администратор (съответния орган на съдебната власт). Намирането на разумния баланс между тези две законодателни изисквания (чл. 25 от ОРЗД и чл. 30 от ЗСВ) при определянето на параметрите на информационните системи по чл. 30, ал. 2, т. 18 от ЗСВ и на други организационни въпроси (чл. 30, ал. 2, т. 20 от ЗСВ), имащи отношение към обработването на лични данни (напр. внедряването на Треликс агентите в конкретния случай), налага ВСС винаги да отчита изискванията на ОРЗД (по-специално съображение 78 и чл. 25) при изпълнение на тези свои задачи. Следователно, при изпълнение на задачите си по чл. 30 от ЗСВ, ВСС следва да съобразява техническите характеристики на продуктите или системите, чието разработване и/или внедряване възлага или одобрява, с принципите за защита на данните на етапа на проектирането и по подразбиране (чл. 25 от ОРЗД) още при изготвянето на съответните технически спецификации. Следва да се има предвид обаче че в цялостния процес по разработване, проектиране и използване на тези системи участват правни субекти, спрямо които надзор в

областта на защитата на личните данни осъществяват различни органи: ВСС е под надзора на КЗЛД; органите на съдебната власт, в зависимост от целите на обработването, което осъществяват, подлежат на надзор, както следва: съдилищата при изпълнение на функциите си на орган на съдебната власт - на ИВСС, а при изпълнение на административните си дейности - на КЗЛД; прокуратурата и следствените органи при изпълнение на функциите си на органи на съдебната власт за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания – на ИВСС, а извън тези цели – на КЗЛД. Предвид това, целесъобразно е в този процес да бъдат ангажирани всички участващи правни субекти по начин, който не накърнява независимостта на нито един от тях. Така, при необходимост, всяка от съответните ангажирани организации (ВСС и всеки орган на съдебната власт) би могла да проведе необходимите консултации с органа, компетентен да осъществи надзор спрямо нейните дейности по обработване (КЗЛД, респ. ИВСС) при наличие на нормативно основание за това – напр. провеждане на предварителна консултация по чл. 36 от ОРЗД като инструмент за управление на високия риск. Подобен подход ще гарантира съгласуваното прилагане на Регламента и на ЗСВ по начин, който гарантира законосъобразно изпълнение на задълженията на всички ангажирани страни (ВСС и органите на съдебната власт) при отчитане на законните цели на обработването и разделението на надзорната дейност съгласно чл. 6 (КЗЛД) и чл. 17, ал. 1 (ИВСС) от ЗЗЛД. Нещо повече, такъв съгласуван подход ще осигури законосъобразност на обработването в широк смисъл предвид обстоятелството, че ВСС формално определя целите и средствата за обработване на лични данни, а органите на съдебната власт носят отговорност за обработването. В този смисъл вземането на решения от ВСС по закона, който регулира неговата дейност (ЗСВ), свързани с целите и средствата за обработване на лични данни в съдебната система, по начин, който отчита задълженията на органите на съдебната власт като администратори на лични данни, ще гарантира изпълнение на ангажиментите на тези администратори по ОРЗД. Това се отнася в пълна степен и до договорните взаимоотношения, в които влиза ВСС и с които косвено създава предпоставки за изпълнение или за неизпълнение на нормативните задължения по ОРЗД на съответните администратори (напр. уреждане на отношенията с обработващ лични данни по чл. 28).

Гореизложените съображения относно необходимостта от съблюдаване на изискванията на чл. 25 (защита на данните на етапа на проектирането и по подразбиране) са изцяло приложими в конкретния случай с Треликс агентите, предвид обстоятелството, че за да изпълни предназначението си този продукт, неговите функционалности предполагат обработване на лични данни. Следва да се отбележи обаче, че съдилищата не са имали възможност за пряко участие в процеса по избор на това конкретно техническо решение за сигурност на обработването, а само се явяват добросъвестен получател на въпросното средство за киберзащита (като техническа мярка за сигурност на обработването). Независимо от това, те като администратори на лични данни носят отговорност за обработването на лични данни чрез функционалностите на Треликс и това налага цялостното обработване да бъде реализирано под техен контрол. Затова, инкорпорирането на Треликс агентите в процесите по обработване на лични данни от съдилищата следва да бъде осъществено в съответствие с изискванията на ОРЗД.

Най-същественият аспект от това съответствие е необходимостта контролът върху обработването на лични данни чрез Треликс да бъде упражняван от съдилищата. Този контрол е израз на решаващото влияние, което администраторът на лични данни има върху целите и средствата за обработването. Администрирането на данните от съдилищата произтича от приложимото към дейността им материално и процесуално законодателство и това обстоятелство определя всички параметри на обработването.

Във връзка с възможността обработването на лични данни да бъде възложено на обработващ лични данни, в своите Насоки 07/2020 Европейският комитет по защита на данните отбелязва, че решението дали обработването да бъде поверено на конкретен доставчик на услуги изисква внимателна преценка дали този доставчик позволява на администраторите да упражняват достатъчна степен на контрол, като вземат предвид естеството, обхвата, същността и целите на обработването, както и потенциалните рискове за субектите на данни (т. 83). В конкретния казус това налага задълбочен преглед на фактическите отношения между съдилищата като администратори на лични данни и „Информационно обслужване“ АД като обработващ.

Запазването на подхода „централизирано управление“ на Треликс агентите от страна на „Информационно обслужване“ АД на практика

означава, че липсва контрол от страна на съдилищата върху обработването на лични данни, осъществявано чрез функционалностите на тези агенти. Такова централизирано управление представлява *de facto* упражняване на контрол върху обработването от външния изпълнител. Това би придало на обработващия качеството на администратор на лични данни въз основа на критерия „фактическо влияние“¹³ върху обработването при определянето на целите и средствата за обработването (чл. 28, пар. 10). Такова обработване обаче би било незаконосъобразно поради липса на легитимни цели и на правно основание за осъществяването му. Нещо повече, това би довело до незаконосъобразност на обработването и от страна на самите съдилища като администратори, поради това, че са лишени от контрол върху обработването, което са длъжни да осъществяват.

Ключов аспект, който да гарантира съответствие на обработването на лични данни чрез Треликс с изискванията на Регламента е спазването на принципа „ограничение на целите“ по чл. 5, пар. 1, б. „б“ от Регламент (ЕС) 2016/679. Този принцип въвежда изискването личните данни да бъдат събирани за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели. В случая данните, до които Треликс агентите биха имали достъп, са събрани от съдилищата за целите на правораздавателната им дейност и за целите на административната дейност, която осъществяват. Доколкото функционирането на Треликс обаче е свързано с обработване на някои набори от такива данни, то неговото приложение трябва да бъде строго ограничено до предназначението му на продукт за киберзащита. Както бе посочено по-горе, съображение 49 от Регламента изрично допуска такова обработване за целите на гарантирането на мрежовата и информационната сигурност. Европейският законодател обаче изрично ограничава това обработване до „степен, която е строго необходима и пропорционална“ на тези цели.

Важна гаранция, че обработването на лични данни с Треликс протича в съответствие с Регламента, е съблюдаването и на принципа „свеждане на данните до минимум“ (чл. 5, пар. 1, б. „в“ от ОРЗД). Този принцип изисква обработваните данни да бъдат подходящи, свързани със и ограничени до

¹³ Европейски комитет по защита на данните, Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, стр. 12.

необходимото във връзка с целите на обработването. Това налага администраторът на личните данни да предприема мерки за ограничаване на категориите лични данни, предмет на обработване във всяка конкретна операция по обработване. Отговорност на съдилищата в конкретния случай е да определят мерките, които да сведат до минимум засягането на правата на физическите лица чрез ограничаване на категориите лични данни, които функционалностите на Треликс могат да достъпят.

Друг съществен елемент от съответствието с ОРЗД е изискването на чл. 5, пар. 1, б. „д“ личните данни да бъдат съхранявани във форма, която позволява идентифицирането на субектите на данни за период, не по-дълъг от необходимото за целите, за които се обработват данните (принцип „ограничение на съхранението“). В конкретния случай това налага предприемането на мерки, които гарантират, че данните, достъпени в хода на дейностите по мониторинг и контрол на зловредни действия чрез Треликс, се съхраняват за същите тези цели само за времето, необходимо за засичане, анализ и ответна реакция, респ. за спазването на изискванията на Закона за киберсигурност. В този срок на съхранение на данните евентуално ще намери проявление и принципът за „точност“ по чл. 5, пар.1, б. „г“ от Регламента. Анализът и преценката дали личните данни са точни и дали има необходимост от тяхната актуализация следва да бъде направена от гл.т. на целите на обработването с Треликс. Точността на личните данни в случая би следвало да се преценява през изискванията за надеждност и ефективност на мерките за киберсигурност, по-специално за гарантирането на мрежовата и информационната сигурност (арг. съображение 49 от ОРЗД).

Относим към конкретния казус е и принципът на отчетност по чл. 5, пар. 2 от ОРЗД. Този принцип изисква от всеки администратор да спазва на практика останалите принципи, свързани с обработването на лични данни и да доказва, че обработването под негов контрол е в съответствие с тях. Принципът е доразвит с разпоредбата на чл. 24 (отговорност на администратора), съгласно която администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с Регламента. Европейският комитет по защита на данните приема, че „принципът на отчетност е отразен и в член 28 от ОРЗД, в който се определят задълженията на администратора при включване на обработващ лични данни“ (Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в

ОРЗД, т. 8). Общият регламент относно защитата на данните не въвежда изчерпателен списък с мерки, а оставя правото на избор на администраторите. Спазването на практика на всички изисквания, коментирани в настоящото становище и надлежното им документиране може да се използва като елемент за доказване отчетността от страна на съдилищата.

При отчитане на всички изложени съображения е необходимо привеждане в съответствие с ОРЗД на фактическите действия по обработване и на степента на влияние на различните участници при вземането на решения във връзка с възникването на възможност за обработване на лични данни с Треликс по начин, който гарантира изпълнение на задълженията на съдилищата като администратори на лични данни и който осигурява висока степен на защита на основните права и свободи на физическите лица при обработването на данните (чл. 1, съображения 1 и 10).

При централизирано внедряване на платформа за сигурност на крайни точки като Треликс в среда, в която множество организации използват обща инфраструктура за киберсигурност, се разграничават следните основни дейности:

- техническа/системна администрация и конфигуриране на платформата;
- оперативни дейности по наблюдение на средата и анализ на събития по информационна сигурност;
- анализ/реакция/разследване на инциденти по информационна сигурност, които могат да доведат до обработване на лични данни.

В тази връзка е необходимо да се съобразят функциите, които изпълняват участниците в платформата, с правните им качества по ОРЗД. За тази цел:

1. Дейността на външния изпълнител следва да бъде регламентирана в договор между ВСС и „Информационно обслужване“ АД със задължителното минимално съдържание по чл. 28, пар. 3, при спазване на изискванията за формата му по чл. 28, пар. 9 (писмена, вкл. в електронен формат) от ОРЗД.

2. Използването на платформата да се осъществява при подходящи технически и организационни мерки, които гарантират контрол,

проследимост и отчетност на действията, извършвани чрез нея, включително:

- определяне и разграничаване на ролите за управление и използване на платформата Треликс. В този контекст може да бъде предвидено разграничаване на нивата на достъп и правомощията при използването на платформата;
- регламентиране на действията на външния изпълнител по разследване на инциденти в платформата, свързани с извличане на данни от крайни устройства или с достъп до съдържание на файлове. Например, техническо ограничаване на функционалности, позволяващи масово или неизбирателно извличане на данни от крайни точки, въвеждане на механизми за предварителен и/или последващ контрол, вътрешни процедури за одобрение или други, които осигуряват връзка между конкретно действие и възникнал инцидент по информационна сигурност, както и неговото документиране;
- осигуряване на одитна проследимост на действия, извършвани чрез платформата. Подобна проследимост може да включва регистриране на действията на администраторите на Треликс и на операторите, извършващи дейности по наблюдение, анализ, реакция и разследване на инциденти, както и възможност за текущ и последващ преглед на тези действия.

3. Всеки съд в качеството си на администратор на лични данни да:

3.1. актуализира вътрешните си правила или политики за защита на личните данни (политика за поверителност) в частта относно предприети технически и организационни мерки за защита на данните, като включи обща информация относно средството за киберзащита Треликс;

3.2. актуализира информацията по чл. 13 и чл. 14 от ОРЗД, която дължи на субектите на данни в изпълнение на задължението за прозрачност на обработването с включването на информация относно операциите по обработване, които могат да се извършват чрез функционалностите на Треликс и тяхното правно основание; доколкото внедряването на това средство за защита би съставлявало ограничение при използване на вътрешнофирмените ресурси, които използват съдилищата, е необходимо да бъдат актуализирани и относимите към това правила и процедури, за което да бъдат уведомени съдиите и съдебните служители (чл. 25и, ал. 1, т. 2 от

33ЛД) - задължението за информираност в този случай се отнася най-малкото до обхвата, целите и ограниченията на използваните средства.

Предвид горното, на основание чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679 във вр. с чл. 17а, ал.1, т. 2 от Закона за защита на личните данни и чл. 94г, ал. 2 от Правилника за организацията на дейността на Инспектората към Висшия съдебен съвет и за дейността на администрацията и на експертите, ИВСС на свое заседание, проведено на 10.03.2026 г. взе решение съгласно Протокол № 5/10.03.2026 г. с 7 (седем) гласа „за“ от 7 (седем) присъстващи инспектори за изразяване на следното

СТАНОВИЩЕ:

Обработването на лични данни чрез платформата Треликс в съдебната система е допустимо на основание чл. 6, пар. 1, б. „в“ от Регламент (ЕС) 2016/679 (*необходимост от спазване на законово задължение, което се прилага спрямо администратора*) във вр. с чл. 30, ал. 2, т. 24 от Закона за съдебната власт и чл. 4, т. 9 от Закона за киберсигурност, при едновременното наличие и прилагане на най-малко следните гаранции за правата и свободите на физическите лица:

1. Обработването с включване на обработващ лични данни – „Информационно обслужване“ АД, да се осъществява при условията на чл. 28 от Регламент (ЕС) 2016/679.

2. Обработването от обработващия лични данни по т. 1 да е съпроводено с въвеждане и прилагане на подходящи технически и организационни мерки и изисквания, които гарантират контрол, проследимост и отчетност на действията, извършвани в платформата.

3. Обработването на лични данни чрез Треликс в съответствие с т. 1 и т. 2 не освобождава съдилищата от задълженията им по Регламент (ЕС) 2016/679, които те имат в качеството си на администратори на лични данни.

ИНСПЕКТОР:

Заличено на
осн. 33ЛД

ИГНАТИЕВ
