СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-01-93/2022 г.
гр. София, 09.12.2022 г.

ОТНОСНО: *Искане за предварителна консултация относно използването на биометрични данни за контрол на достъпа чрез техническите системи за сигурност на ДП „РВД"*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов и Веселин Целков, на заседание, проведено на 30.11.2022 г., разгледа искане с рег. № ПНМД-01-93/31.10.2022 г. от генералния директор на Държавно предприятие „Ръководство на въздушното движение" (ДП РВД, BULATSA), в което се посочва, че в качеството си на администратор на лични данни, ДП РВД обработва лични данни съгласно Европейското и национално законодателство, като същевременно следи практиката и насоките на КЗЛД.

Повод за искането на ДП РВД е публикуваният на интернет страницата на КЗЛД, в раздел „Насоки", списък на операциите по обработване на лични данни, за които е задължителна предварителна консултация по чл. 65, ал. 3 от Закона за защита на личните данни *(Списък на операциите по обработване на лични данни. за които е задължителна предварителна консултация по чл. 65, ал. 3 от Закона за защита на личните данни).* Точка 4 от списъка включва следната операция по обработване на лични данни, за която е необходима предварителна консултация с КЗЛД: *„Осъществяване на систематично мащабно наблюдение на публично достъпни зони, когато това е свързано с автоматизирано вземане на решения, вкл. лицево разпознаване.".*

От ДП РВД считат, че попадат в тази хипотеза на списъка и отправят молба към КЗЛД за изразяване на становище относно използването на биометрични технологии за целите на контрол на физическия достъп на територията на обектите на ДП РВД.

Излагат се мотиви, че ДП РВД е стратегически обект от значение за националната сигурност (съгласно Постановление № 181 на Министерски съвет от 20 юли 2009 г. за определяне на стратегическите обекти и дейности, които са от значение за националната сигурност), като за целта прилага мерки за физическа защита и контрол на достъпа за всички обекти на цялата територия на предприятието.

Във връзка с реализиране на проект за модернизиране на техническите системи за сигурност на предприятието, ДП РВД планира изграждане на система за физически контрол на достъпа чрез биометрични данни, които могат да бъдат лицево разпознаване, пръстов отпечатък за служителите, или други подходящи способи, които използват биометрични технологии.

Към настоящия момент, една от мерките за защита и контрол на достъпа е използването на RFID карта за достъп със снимка на съответния служител. Прилагането на контрол на физическия достъп посредством обработка на биометрични данни ще ограничи риска от нерегламентиран достъп чрез неправомерно предоставяне на карта за достъп на трето лице, достъп с отнета/изгубена карта, превенция на клониране/копиране на карта.

От ДП РВД уточняват, че биометричните данни на служителите ще се съхраняват като хеш (hash) стойности в криптирана база данни, като ще бъдат приложени техническите мерки за защита, изброени в следващия параграф. Данните ще се съхраняват локално, на местата на които ще бъдат разположени устройствата за достъп – за предоставяне на безусловен достъп, както и на сървъра за снемане на биометричните данни.

Техническите мерки за защита на данните, които се предвиждат са:

• Предоставяне на логически достъп на базата на принципа „необходимо е да знае";

o На ограничен брой служители от отдел „Сигурност и защита" – за целите на администриране на логически достъп, както и за целите на снемане на дигитална репрезентация (hash) на биометричните данни и въвеждането на същите в защитена/криптирана база данни;

o На служители от отдел „Информационна инфраструктура", Дирекция „Информационни системи" – администраторски достъп за целите на мрежово осигуряване, както и за целите на обработка на събития от журнални файлове;

o Други служители от дирекция „Информационни системи" по компетентност с оглед поддръжката на техническите системи за сигурност.

• Съхранение на hash стойности на обработваните биометрични данни в криптирани бази данни;

• Регулярен преглед на правата за достъп (минимум на една година) и съхраняване на данните за не по-дълъг срок от срока на валидност на сертификатите на картата за достъп – 3 години;

• Изпращане на журнални файлове към платформата на „Оперативния център по информационна сигурност", дирекция „Информационни системи" на ДП РВД, за целите на управление на събития и инциденти, свързани със сигурността на информацията и предотвратяване на инциденти с изтичане на лични данни и нарушаване на правата на достъп.

В писмото се твърди, че биометрична категоризация на служители на предприятието няма да бъде извършвана. Данните ще бъдат използвани единствено за осигуряване на физически достъп до територията на предприятието. Контрол на достъпа следва да бъде упражняван само на територията на обектите на предприятието.

За пълнота на преписката КЗЛД изиска представянето на извършената оценка на въздействието върху защитата на личните данни, която се отнася за планираното обработване на биометрични данни. Направено е уточнение, че изложеният от ДП РВД казус не попада в хипотезата на чл. 65, ал. 3 от Закона за защита на личните данни (ЗЗЛД), а по-скоро в обхвата на общото правило на чл. 35, пар. 1 от Регламент (ЕС) 2016/679.

С писмо с вх. № ПНМД-01-93#4/10.11.2022 г. ДП РВД представят на вниманието на КЗЛД извършена оценка на въздействието върху защитата на личните данни (биометрични данни), които се планира да бъдат обработвани за осъществяване на контрол на физическия достъп на служители до съответните обекти на предприятието. Оценката на въздействието е изготвена на база утвърдената в ДП РВД „Методика за оценка на риска за сигурността на информацията".

Правен анализ:

Разпоредбата на чл. 65, ал. 3 от ЗЗЛД е част от Глава осма. *Правила за защита 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, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване (Загл. изм. ДВ, бр. 17 от 2019 г.)*, чрез която в българското законодателство се транспонират изискванията на Директива (ЕС) 2016/680. Въпросните правила се прилагат в областта на правоприлагането, когато администратор на личните данни е компетентен орган по смисъла на чл. 42, ал. 4 от ЗЗЛД и ги обработва за целите, изброени изчерпателно в чл. 42, ал. 1 от ЗЗЛД. Тъй като ДП РВД не притежава качествата, правомощията и функциите на компетентните органи по смисъла на чл. 42, ал. 4 от ЗЗЛД, за него като администратор на лични данни, не се прилага и изискването съгласно *Списъка на операциите по обработване на лични данни, за които е задължителна предварителна консултация по чл. 65, ал. 3 от ЗЗЛД.*

Процедурата по предварителна консултация с надзорния орган, в случая КЗЛД, е особено производство, което се развива по реда и условията на чл. 36 от Регламент (ЕС) 2016/679 или на чл. 65 от Закона за защита на личните данни (когато обработването на данни е за целите по чл. 42, ал. 1 от ЗЗЛД). По общо правило, за да се подобри спазването на нормативните изисквания за защита на личните данни, когато има вероятност операциите по обработване да доведат до висок риск за правата и свободите на физическите лица, администраторът е длъжен да изготви т.нар. оценка на въздействието върху защитата на данните, за да се оценят по-специално произходът, естеството, спецификата и степента на този риск. Резултатите от извършената оценка следва да бъдат взети предвид, когато се определят съответните мерки, за да се докаже, че обработването на лични данни отговаря на нормативните изисквания. Когато в оценката на въздействието върху защитата на данните е указано, че операциите по обработването водят до висок риск, който администраторът не може да ограничи с подходящи мерки от гледна точка на налични технологии и разходи за прилагане, преди началото на планираното обработване той следва да осъществи консултация с надзорния орган.

Анализ на представените документи показва, че ДП РВД е извършило оценка на риска, което е етап от извършването на оценката на въздействието върху защитата на личните данни (арг. чл. 35, пар. 7, б. в) от Регламент (ЕС) 2016/679). Приемливата оценка на въздействието върху защитата на личните данни по Регламент (ЕС) 2016/679 следва да съдържа:

• систематично описание на обработването (член 35, пар. 7, буква а)): взема се под внимание характерът, обхватът, контекстът и целите на обработката (съображение 90); личните данни, получателите и периодът, за който ще се съхраняват личните данни, се записват; функционално описание на операцията по обработване; идентифициране на активите, на които разчитат личните данни (хардуер, софтуер, мрежи, хора, хартия); отчита се евентуално спазването на одобрените кодекси за поведение (член 35, параграф 8);

• описание на техническите средства, с които се извършва обработването на лични данни – това е абсолютно необходимо при извършването на оценката на въздействието, като е свързано и с „мобилното приложение – мобилното здравно досие";

• необходимост и пропорционалност на обработването (член 35, параграф 7, буква б)): определени са мерките, предвидени за спазване на регламента (член 35, параграф 7, буква г) и съображение 90, като се вземат предвид: мерките, допринасящи за пропорционалност и необходимост на обработването на базата на: конкретни, изрични и законни цели (член 5, параграф 1, буква б); законосъобразност на обработването (член 6); адекватни, уместни и ограничени до необходимите данни (член 5, параграф 1, буква в); ограничена продължителност на съхранение (член 5, параграф 1, буква д)); мерки, допринасящи за правата на субектите на данни: информация, предоставена на субекта на данни (членове 12, 13 и 14); право на достъп и преносимост (членове 15 и 20); право на поправяне, заличаване, възражение, ограничаване на обработването (членове 16–19 и 21); получатели; обработващ (и) (член 28); гаранции, свързани с международния (те) трансфер (Глава V); предварително консултиране (член 36).

• управление на рисковете за правата и свободите на субектите на данни (член 35, параграф 7, буква в)): произходът, характерът, особеностите и тежестта на рисковете се оценяват (виж съображение 84) или по-конкретно за всеки риск (неправомерен достъп, нежелано изменение и изчезване на данни) от гледна точка на субектите на данни: вземат се предвид източниците на рискове (съображение 90); потенциалните въздействия върху правата и свободите на субектите на данни са идентифицирани в случай на незаконен достъп, нежелано изменение и изчезване на данни; заплахи, които могат да доведат до нелегален достъп, идентифициране на нежелани модификации и изчезване на данни; оценка на вероятността и тежестта (съображение 90); определят се мерките, предвидени за третиране на тези рискове (член 35, параграф 7, буква г) и съображение 90);

• участие на заинтересовани страни: консултация с длъжностното лице по защита на данните (член 35, параграф 2); иска се становището на субектите на данните или на техните представители (член 35, параграф 9).

Едва след като извърши оценката на въздействието върху защитата на личните данни и същата покаже висок остатъчен риск въпреки наложените технически и организационни мерки, администраторът следва да пристъпи към иницииране на производство по предварителна консултация по смисъла на чл. 36 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД).

Съгласно чл. 4, т. 14) от Регламент (ЕС) 2016/679 „биометрични данни" означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни. Биометричните данни са специални категории лични данни и по смисъла на чл. 9, пар. 1 от ОРЗД тяхното обработване **по принцип е забранено**, освен в изрично посочените в пар. 2 от същата разпоредба хипотези.

В съображение (51) от Регламент (ЕС) 2016/679 се посочва по-специално, че обработването на биометрични данни с цел идентификация е забранено. **Такова обработване е оправдано, само ако** съществува изрично съгласие на съответното лице, **прилагат се специфични правни задължения или ако обработването се изисква по съображения от обществен интерес, при наличие на правно задължение или е свързано с упражняването на официални правомощия.** В допълнение към посочените стриктни изисквания за такова обработване следва да се прилагат общите принципи и другите правила, залегнали в регламента.

Както се посочва в искането на ДП РВД, предприятието е стратегически обект от значение за националната сигурност съгласно Постановление № 181 на МС от 20.07.2009 за определяне на стратегическите обекти и дейности, които са от значение за националната сигурност. Съгласно чл. 41 от Правилника за прилагане на Закона за Държавна агенция „Национална сигурност" тези обекти са част от критичната инфраструктура на страната. Според чл. 41, ал. 2 от Правилника за прилагане на ЗДАНС защитата на стратегическите обекти и дейности от значение за националната сигурност включва:

1. контрол на организацията на физическа защита (охрана) на обектите, включително с оглед противодействие на заплахи от терористичен характер, който обхваща мерките за сигурност на стратегическите зони и режима на достъп до стратегическите зони и зоните, свързани с изпълнението на стратегическите дейности;

2. контрол на информационната защита, осъществявана чрез административни, организационни, технически и криптографски мерки;

3. оказване съдействие на ръководителите на стратегически обекти и на възлагащите или извършващите стратегически дейности при идентифициране и оценка на потенциални заплахи, насочени срещу стратегически обекти и дейности от значение за националната сигурност.

Доколкото контролът на организацията на физическата защита и достъпа до стратегическите обекти изисква чрез тях да се осъществи противодействие на заплахи от терористичен характер, обработването на биометрични данни в случая може да се обоснове с хипотезата на чл. 9, пар. 2, б. ж) от Регламент (ЕС) 2016/679 – когато обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните. Определянето на ограничен кръг от служители и конкретни зони за наблюдение могат да се разглеждат като подходящи мерки за защита правата и свободите на субектите на данни в конкретния случай.

Определянето на ДП РВД, като стратегически обект за националната сигурност – част от критичната инфраструктура, представлява важен обществен интерес, посочен в националното ни законодателство. Обработването на биометрични данни при осъществяване на достъпа до такъв тип обекти може да се разглежда като пропорционално на преследваната цел, а именно противодействието

на терористични заплахи. За да е законосъобразно обработването обаче, то следва да зачита същността на правото на защита на данните и да предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните – т.е. следва да се извърши оценка на въздействието върху защитата на данните.

На оценка подлежи съответната информационна система или приложението, като средство, чрез което се извършва обработването на биометрични данни. Анализът следва да се извършва още на етапа на проектирането (съобразно чл. 25 от Регламент (ЕС) 2016/679), както и да се прецени доколко чрез използването на такова приложение е възможно да се достигне до трансфер на данни по смисъла на глава V от Регламент (ЕС) 2016/679.

Съществено значение при предприемането на конкретно обработване на лични данни (в случая биометрични) има отговорността на администратора за гарантиране правата на засегнатите субекти на данни (в конкретния случай – определени служители със специфични функции) по смисъла на чл. 12–22 от Регламент (ЕС) 2016/679. Администраторът на лични данни има задължение предварително да уведоми лицата, чиито данни ще обработва за:

• данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;

• координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

• целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

• получателите или категориите получатели на личните данни, ако има такива;

• когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Европейската комисия относно адекватното ниво на защита или в случай на предаване на данни съгласно посоченото в членове 46 или 47, или член 49, параграф 1, втора алинея от ОРЗД позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.

• срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

• съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните;

• когато обработването се основава на член 6, параграф 1, буква а) или член 9, параграф 2, буква а) от ОРЗД, съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

• правото на жалба до надзорен орган;

• дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени;

• съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

Всяко засегнато лице може да упражнява правата по чл. 15–22, гарантирани му от Регламент (ЕС) 2016/679, чрез писмено искане до администратора на лични данни. Съгласно чл. 12, пар. 3 от Регламент (ЕС) 2016/679 администраторът предоставя на субекта на данни информация относно действията,

предприети във връзка с искане по членове 15–22, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

По тези съображения и на основание чл. 58, пар. 3, б. „б" от Регламент (ЕС) 2016/679 във вр. с чл. 10а, ал. 1 от Закона за защита на личните данни и чл. 51, т. 2 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

Доколкото от представените документи няма данни за извършена оценка на въздействието върху защитата на данните, на основание чл. 35, пар. 1 от Регламент (ЕС) 2016/679 ДП РВД следва задължително да извърши такава оценка и само ако същата покаже висок остатъчен риск за правата и свободите на засегнатите субекти на данни, може да пристъпи към предварителна консултация с надзорния орган съгласно чл. 36 от Регламент (ЕС) 2016/679.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Веселин Целков /п/