Комисия за Защита на Личните Данни

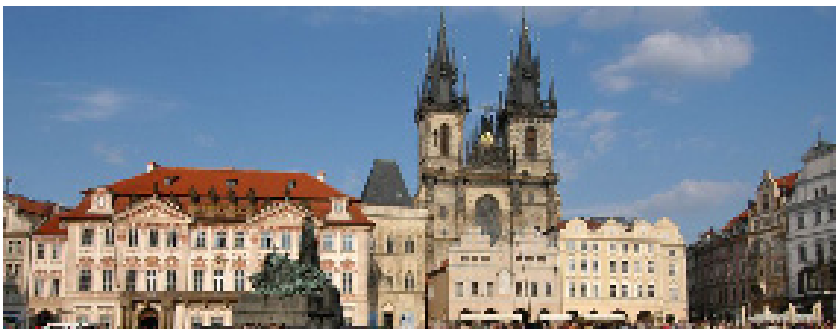
ИНФОРМАЦИОНЕН БЮЛЕТИН

брой 3 (24), май 2010 г.

ТЕМИТЕ В БРОЯ

СЪБИТИЯ И ИНИЦИАТИВИ

ГОДИШНА КОНФЕРЕНЦИЯ НА ОРГАНИТЕ ПО ЗАЩИТА НА ДАННИТЕ



Пражкият замък

На 29 и 30 април в Прага, Република Чехия, се проведе Годишната конференция на комисарите по защита на личните данни и личната неприкосновеност. Събитието бе организирано в Пражкия замък – резиденцията на Президента Вацлав Клаус. Присъстваха повече от сто представители от Европейската комисия, комисари по защита на личните данни на държавите-членки, както и представители на други органи и международни организации. От страна на Комисията за защита на лични данни участва г-н Красимир Димитров - член на КЗЛД, г-н Цветелин Софрониев- главен секретар и Десислава Борисова - юрисконсулт.

Логото на конференцията протече под надслова ”Преценка на миналото, поглед към бъдещето”.

Първият панел от дискусиите касаеше т.нар “Internet of things”. Терминът е въведен през 2005 год. и означава самоконфигуриращa се мрежа от обекти. Има се предвид вариант, при който всички заобикалящи ни предмети са оборудвани с миниатюрни устройства за разпознаване. По радио-честотни вълни ще може да се определи местоположението на абсолютно всичко. Това би могло да доведе до тотална трансформация на всекидневния ни живот. Като пример – няма да има вероятност определен продукт да свърши на пазара, тъй като компетентните органи постоянно ще са наясно с потреблението на стоките. Кражбата като престъпление също ще изчезне, тъй като по всяко време ще се знае кой предмет къде се намира. Изчислено е че човек е заобиколен от около 1000 до 5000 неща всекидневно. За да започне ефикасно да работи тази технология е необходимо да се сложат радио-честотни чипове на около 50 до 100 трилиона обекти. Всичко това обаче крие сериозни рискове пред защитата на личната неприкосновеност. Работната група по защита на данните, създадена въз основа на чл.29 от Директива 95/46 има консултативна роля при определяне на бъдещата законодателна рамка на радио-честотните чипове. На конференцията беше обсъдено и становището на Работната група по отношение на това как влияят радио-честотните чипове на защитата на личните данни.

По време на конференцията се дискутира нарастващата роля на Интернет в живота на хората. Логото на това обсъждане беше цитат на директора на Майкрософт, който гласи: „Когато си вкъщи и влезнеш в Интернет, твоето местоположение вече не е „вкъщи”, а е Интернет”. Въпреки всички положителни отзиви за Интернет, трябва да се има предвид и че с нарастването на потребителите, продължава увеличаването на компютърните престъпления и нарушения онлайн. Това налага да се търсят нови начини за предотвратяване на кражбата на самоличност, злоупотребата с лични данни и др.

Обсъди се системата за поставяне на чипове в колите, която ще се активира при пътен инцидент и необходимата законодателна рамка за това. Отбеляза се факта, че чрез безжична връзка се следи местоположението на превозните средства от публичния транспорт, а също така чрез сензорите на мобилните телефони може да се определи местоположението на хора. Обърна се специално внимание на Софийския меморандум, приет от Работната група по защита на личните данни в телекомуникациите и целящ да приложи принципите по защита на данните при предоставяне на информация за локацията на превозните средства. Изводът от презентацията е - ако не могат да бъдат анонимизирани данните на пътниците, поне да е възможно прилагането на принципа на пропорционалност при обработване на техните данни.

Беше обсъден и т.нар принцип "privacy by design" – това е защита на личната неприкосновеност в зависимост от източника на опасност. Този въпрос логично води до обсъждане на начините, по които може да се постигне повишаване на осведомеността на хората по отношение на защитата не техните права. Едно от вижданията е ,че при промяна в Директива 95/46 този принцип задължително трябва да е включен, тъй като е един от най-съществените. Широка дискусия предизвика евентуалната законодателна регламентация на " privacy by design". Обсъди се нарастваща потребност от регламентация на този принцип, както и практиките на отделните органи по защита на данните за въвеждането на единни изисквания към бизнеса.

Беше изнесена презентация от проф. Сарма от Масачузетския институт по технологии, който представи еволюцията на Интернет и на промените в разбиранията на гражданите. Както беше отбелязано, живеем в ерата на „технологично цунами", така че комисарите по защита на данните е наложително да вземат съвместно мерки за прилагане на принципите по защита на данните в новите технологии.

Специален панел на дискусии беше посветен на 12- годишнина от приемането на Конвенцията на ООН за правата на децата и по-специално за основната й цел – създаването на „свят, подходящ за децата". Беше приета Резолюция за започването на съвместни действия за повишаване на осведомеността и образованието на младите на европейско и международно ниво. На тези дискусии се обсъдиха инициативите на компетентните органи по защита на данните във връзка със защита на данните на децата онлайн. Португалският орган за защита на данните представи проекта DADUS, който е насочен към повишаване на осведомеността на децата при използването на Интернет. Опитът показва, че повишаване на осведомеността се постига най-лесно чрез създаването на Интернет форуми, дискусии, стартирането на конкурси с награди, състезания, семинари, които имат тема от областта на защита на данните.

Обсъди се бъдещето на защита на данните, като се отчете необходимостта от създаването на разбираема законодателна рамка, която ще направи възможно нормативното регламентира на новите принципи за "privacy by design"(защита на личната неприкосновеност съобразно източника на въздействие) и "accountability" (предприемането на адекватни технически и организационни мерки от администратора на лични данни); намирането на механизми, с които да се гарантира съответствието на администраторите на лични данни с принципите по защита на данните.

Във връзка с осъществяването на проверки от компетентните органи, бе споделено мнението, че трябва да се увеличи броя на последващите, за сметка на предварителните проверки. Голяма част от дейността на органите по защита на данните по предварителните проверки се припокрива с дейността на други разрешителни органи, докато при последващите проверки в най-голяма степен може да се прецени спазват ли се техническите и организационни мерки, които са били предвидени преди започване на дейността и по този начин да се реализира по най-ефикасен начин контролната функция на органите. До края на май тази година Работната група по чл.29 ще изготви становище относно принципа на отчетност. При евентуалното му бъдещо въвеждане, в много по-голяма степен ще се гарантира спазването на минималното ниво на технически и организационни мерки за защита на данните.

Представителите на България в конференцията - Цветелин Софрониев, Десислава Борисова и Красимир Димитров

Представиха се различни модели на публична администрация и принципите при функционирането й, като бе обърнато специално внимание на механизмите за осъществяване на връзката на гражданите с държавните структури. Важен въпрос, предмет на дискусии, е да се прецени дали е подходящ варианта базата данни на всички институции да бъде на един сървър, като всяка администрация достъпва данни от друга, или е необходима диференциация. Едно от обясненията за такава концентрация на информация е по-високата оперативност и ефективност на компетентните органи, но от гледна точка на защитата на лични данни, необходимо е да се дефинират нивата за достъп на потребителите. В обратния случай става възможно за едно лице да се получи информация относно физическата му идентичност, здравната му осигуровка, дължимите данъци и т.н, т.е съществува голяма опасност да се злоупотреби с личните му данни при един пробив в системата. Няколко са основните принципи за защита на данните в публичния сектор - обработването на данни да става само на нормативна основа, онлайн достъп да се осъществява само до собствени данни на потребителя, както и да се извършва постоянен мониторинг на системите. Беше отбелязано, че е много малка границата между това публичният сектор да е уважаван партньор на органа по защита на данните и това да е привилигирован обработващ данни. Естественият подход е компетентните институции да си сътрудничат ефективно с органите по защита на данните.

Обсъдиха се Обвързващите корпоративни правила и Обвързващите глобални кодекси. Един от основните проблеми на тези правила е фактът, че в момента има не повече от 30 компании, които са ги въвели, като много голямо е забавянето до завършване на процеса по приемането им, голям брой изисквания на компетентните органи по защита на данните, както и все още ниската степен на доверие на самите компании в тези правила. Статистически погледнато, съществуват около 63 000 мултинационални компании, в които работят приблизително 90 млн души. Всяка от тези компании осъществява трансфер на данни, а много минимална част от тях спазват такива обвързващи правила.

Направена бе презентация от г-жа Корадо (заместник началник на Отдел 5 по защита на данните в Европейската комисия) по отношение на законодателната рамка по защита на данните. Предизвикателствата пред нормотворците са свързани с въздействието на новите технологии, глобализацията, трансфера на данните, увеличаващата се роля на компетентните органи по защита на данните и др. При анализ на резултатите, получени от миналогодишната публична консултация за политиката по защита на личните данни, става ясно, че все още съществува правна несигурност в някои аспекти на приложение на Директива 95/46; има различни виждания при транспонирането й; голямо многообразие при тълкуване на определени текстове. Г-жа Корадо отбеляза важната роля на Групата по чл.29 при изясняването на нормативни понятия, изготвянето на становища по определени проблеми и опитите за провеждане на единна политика по защита на данните. Също така, беше изтъкната необходимостта от улесняване на административните процедури, тъй като в някои държави все още са много мудни и съществуват бюрократични пречки пред администраторите на лични данни.

Обсъди се проблемът с етническото профилиране на населението и наличието на два вида дискриминация – позитивна и негативна. Позитивната дискриминация представлява обработването на данни относно етнически произход, което предпоставя получаването на по-добър жизнен стандарт (напр. във връзка с получаването на помощи като малцинствена група, друг вид субсидии и т.н). При всички случаи, обработването на данни относно етнически произход е възможно да бъде осъществено при съгласие на лицето данните му да бъдат обработвани. Във всички останали случаи е възможно единствено обработването на такива данни за статистически цели.

По време на престоя в Прага, българската делегация се срещна с посланика на Република България в Република Чехия – г-н Здравко Попов и консула – г-н Данчо Мичев. По време на срещите бяха коментирани външнополитически въпроси и проблеми, свързани със защитата на личните данни, както в национален мащаб за двете страни, така и от гледна точка на работата на посолствата и консулствата.

47-МА СРЕЩА НА МЕЖДУНАРОДНАТА РАБОТНА ГРУПА ПО ЗАЩИТА НА ДАННИТЕ В ТЕЛЕКОМУНИКАЦИИТЕ

На 15 и 16 април 2010 г. в Гаранада, Испания се проведе 47-та среща на Международната работна група по защита на данните в телекомуникациите. България бе представена от членовете на Комисията за защита на личните данни Веселин Целков и Валентин Енев.

През двата дни бяха разгледани редица въпроси по защита на личните данни в сектор „Телекомуникации". Обсъдиха се проблеми по защита на данните в Пан-европейската система за осъществяване на спешни обаждания от превозни средства (E-call инициатива). За всички коли, произведени в Европа се очаква изграждането на такава система, което ще позволи обажданията при инциденти да бъдат препращани към европейския телефон за спешни случаи – 112. Обсъдиха се методите за съхранение и ползване на информацията от базата данни за транспортните произшествия

Разгледаха се т.нар. *Deep Packet Technologies* и тяхното използване за борба със съвременните мрежови атаки . Deep Packet Inspection (DPI) е основната технология, която се използва в съвременните защитни стени. Такива технологии вече са способни да наблюдават всяко действие на потребителя в Интернет, което пък от своя страна води до необходимостта за налагането на правила за събирането на данни за потребителите.

Представи се преработен вариант на Хартата за дигиталните права, като отново бе изтъкнато, че това е първият по рода си документ, който обединява правото на информация с правото на защита на личните данни.

Обсъди се работен документ за риска от повторното даване на ползван вече е-мейл адрес ("e-mail-heritage"). На 46-та среща на Международната работна група Луис Барозу (член на комисията за защита на данните на Португалия) предложи проектен документ по отношение на защита на данните в е-мейлl, SMS и социалните мрежи. Основният проблем касае случаите, в които служител напуска работа и неговите координати (е-майл, телефон и т.н.) получава друг служител. Подобен проблем съществува и при потребителите на Интернет при смяна на доставчика. Документът цели да регламентира възникващите правоотношения между различните потребители. Продължава неговото обсъждане и приемането на становища.

Повдигната бе темата за неприкосновеността и международните стандарти и в частност стандарта ISO/IEC CD 29100 - Information technology - Security techniques - Privacy framework (Информационни технологии - Методи за сигурност - Работна рамка за опазване на тайна на лични данни).

Един от постоянните въпроси, дискутирани на срещите на Международната група е този за личната неприкосновеност в социалните мрежи. Обърна се внимание на все по-широкото навлизане на възможностите за актуализация на информация в реално време и евентуалните мерки по опазване целостта и неприкосновенността на данните при извършването на тези актуализации. Припомни се Становището на Работна група по чл. 29 от 12 юни 2009 г., което бе отговор на зачестилите оплаквания от страна на потребителите на социалните мрежи в интернет. Тогава бе подчертано, че не само специалистите по маркетинг, но и дейността на ИТ специалистите, които се опитват да достигнат до потребителите трябва да са обект на Органите по интернет сигурността в Европа. В т.нар. „Римски меморандум"(от 43-тата Работна среща на Международната група по защита на данните в телекомуникациите) бяха издадени указания за запазване на неприкосновеността в социалните мрежи. Основната загриженост на Международната работна група е в това, че при ниско ниво на защитеност на личните данни се дава възможност за т.нар. "кражба на самоличност" или за неоторизиран достъп на трети лица.

Разгледаха се и други въпроси като проблемът с концентрацията на лични данни в многонационалните предприятия, работата с геопространствени данни за обектите и т.н.

Направи се презентация на тест за самооценка на риска от кражба на самоличност. В теста са представени 11 ситуации, в които физическо лице може да стане жертва на кражба на неговата самоличност – при използване на дебитни и кредитни карти, мобилен телефон, компютър, он-лайн пазаруване, при въвеждане на пароли и кодове и т.н .

Тестът е достъпен на интернет адрес http://www.idtyveri.info/id-theft/ .

България представи своя доклад за изминалия 6-месечен период. Засегнати са четири основни момента в развитието на защитата на данните в телекомуникациите:

1. Влизането в сила на поправките в Закона за електронните съобщения. С новите поправки се променя режимът на запазване и достъп до трафични данни. Предложените промени засягат предоставянето на трафични данни от мобилните оператори и доставчиците на интернет към компетентните органи при разследване на тежки и компютърни престъпления. Според промените, разрешенията за разпечатки вече ще се издават от председателите на районните съдилища в страната. Досега това се извършваше от окръжните съдилища, които са 5 пъти по-малко. В резултат на изключителния обществен интерес и широки дебати законът претърпя сериозно развитие спрямо първоначалния си вариант. Прие се да не се въвежда директния интерфейс, както бе предвидено в първоначалния вариант на измененията, а мобилните оператори и интернет доставчици да са задължени да предоставят данни на МВР до 72 часа след поискването им. Идеята на управляващите за постоянен достъп на службите до трафичните данни отпадна преди второ четене на закона заради силен обществен натиск. Предвижда се министърът на вътрешните работа да има право да поиска по-кратък или по-дълъг срок от 72 часа за получаване на информация от операторите. Глобите за мобилните оператори и интернет доставчиците в случай, че не предоставят исканата им информация в срок, ще варират от 15 000 до 50 000 лв. Личните данни, до които е осъществен достъп ще се съхраняват 6 месеца, след което ще бъдат унищожавани, в случай, че няма да се ползват по-нататък за целите на съдебно дело или разследване. За да се предотврати безконтролното и непропорционално навлизане в личното пространство на гражданите, законът предвижда Комисията за защита на личните данни да е наблюдаващ орган по сигурността на данните, които ще се проследяват, а комисия на Народното

събрание ще осъществява парламентарен контрол и наблюдение на процедурите по разрешаване и осъществяване на достъп до въпросните данни, както и по защита на правата и свободите на гражданите срещу незаконосъобразен достъп до тези данни. Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, ежегодно до 31 март предоставят на Комисията за защита на личните данни в качеството ѝ на наблюдаващ орган съответната статистическа информация, която в двумесечен срок от получаването ѝ се представя в ежегоден доклад до Народното събрание и Европейската комисия.

2. 2. Стартира на процесът по издаване на новите български документи за самоличност, които постепенно ще подменят старите при изтичането на срока им на валидност. От 29 март 2010 г. започна издаването на българските паспорти с биометрични данни. Живеещите в чужбина българи имат възможност да подадат своите заявления и да получат документите си в дипломатическите и консулските представителства на Република България в чужбина. Там, където има техническа възможност за заснемане с цифрови устройства на подписа, лицето и пръстовите отпечатъци на заявителя се приемат заявления за издаване на лична карта и паспорт. Там, където няма такава техническа възможност се приемат заявления за издаване само на лична карта.

3. В областта на електронното здравеопазване се отчита въвеждането на смарт карти за достъп до информацията за здравословното състояние на военнослужещите и техните семейства в базата данни на Военномедицинска академия. Подчертава се, че с така въведената информационна система и достъпа до информацията в нея се оптимизира медицинското обслужване, опростяват се и се модернизират процедурите за достъп и едновременно с това се увеличава сигурността на достъпа до здравна информация. Пациентите имат достъп до личните си данни онлайн по всяко време. Личният електронен здравен запис дава възможност на лекуващите специалисти за незабавен достъп до медицинските данни на пациента и поради това подпомагат решенията, особено в критични ситуации, за които има специален раздел в електронната здравна карта, съдържащ най-важната информация.

4. Отчита се напредък при изграждане на електронното правителство. На 1 февруари 2010 г. българското правителство официално започна тестване на интегрирана платформа за онлайн предоставяне на 13 общински и централни административни услуги. Основните предимства на тези интегрирана платформа са: едно място за достъп до обществените електронни услуги на всички нива на управление; унифицирано предоставяне на данните, предоставени от различни обществени администрации; спестяване на гражданите на необходимостта да представят едни и същи документи пред различни органи и т.н.

Към доклада на България нямаше въпроси и забележки.

ЗАСЕДАНИЯ НА ОБЩИ НАДЗОРНИ ОРГАНИ И РАБОТНИ ГРУПИ

От 7 до 11 март 2010 г. в Брюксел се проведоха заседания на Общите надзорни органи по Европол и Шенген, Работната група по полиция и правосъдие, Координационните групи по надзор на Евродак и по митническата информационна система. Присъстваха члновете на Комисията за защита на личните данни Мария Матева и Веселин Целков.

Общият надзорен орган по Европол одобри новата стратегия на Европол. Представи се доклад за срещата на председателя и заместник председателя на надзорния орган с новия директор на Европол. Разгледаха се новите правила за приемане на информация от частни източници. Обдъдиха се връзките на Европол с трети страни.

На заседанието на Координационната група по надзор на митническата информационна система се представиха презентации от Европейския надзорен орган по защита на данните и от дирекция „Оперативно и полицейско сътрудничество" на Европейската служба за борба с измамите (OLAF). Една от целите, с които е създадена Митническата информационна система е да улеснява сътрудничеството между европейските митнически власти в борбата им с митническите престъпления. Премахването на граничния контрол след формирането на единния пазар е бил

мотивиращ фактор за развитието на митническата информационна система като средство за борба с контрабандата. Централизираната митническа информационна система е в Брюксел. Тя е достъпна от страните членки-членки и тъй като включва обработване на лични данни, в нея са вградени редица средства за тяхната защита.

Координационната група на Евродак обсъди доклада на Евродак за 2008-2009 година. Разгледа се и се одобри работната програма на органа за 2010-2011 година. Обсъдиха се възможностите на страните за специални търсения в системата на Евродак. Предстои изготвянето на брошура за правата на бежанците за достъп до личните им данни. След изготвянето й, брошурата ще бъде предоставена официално на органите по защита на данните. На заседанието стана ясно, че КЗЛД следва да извърши проверка на системата Евродак в Република България през следващите две години и да докладва за резултатите от тази проверка на органа по Евродак. Според Мария Матева, представител на КЗЛД в Координационната група на Евродак е наложително тази проверка за залегне в плана на КЗЛД за планови проверки до края на 2010 година.

ЗАСЕДАНИЕ НА РАБОТНА ГРУПА „ОЦЕНКА ПО ШЕНГЕН”

На 16 март 2010 г. се проведе редовно заседание на Работна група „Оценка по Шенген”. От обсъдените теми, следните три са от специално значение за България:

- Проект на Решение на Съвета за прилагането от България и Румъния на разпоредбите на шенгенското законодателство, свързани с ШИС и проект на Заключения на Съвета относно защитата на личните данни в България и Румъния;
- Проект на Доклад от оценката на България в областта на въздушните граници;
- Актуализиран Компендиум от оценката на България в областта на полицейското сътрудничество.

Одобрени от работната група и изпратени за (незадължително) становище от Европейския парламент са следните два документа:

- Проект на Заключения на Съвета относно защитата на личните данни в България и Румъния;
- Решение на Съвета за прилагането от България и Румъния на разпоредбите на шенгенското законодателство, свързани с ШИС.

В проекта на доклад от оценката на България по въздушни граници се подчертава, че оценката е много добра и българската страна е напълно готова и отговаря на всички изисквания на Шенген в тази област. Изтъкнато е наличието на национална стратегия за интегрирано гранично управление, добрата професионална подготовка и работа на служителите на Гранична полиция, модерното техническо оборудване и много доброто решение и изпълнение на разделянето на потоците на летищата. Като най-добри практики се посочва продължаващото обучение на граничните служители и тактическият анализ на риска. Оценяващият екип е направил и някои конкретни предложения за подобряване на граничния контрол, които следва да бъдат изпълнени. Българската страна приема много сериозно препоръките, по някои от които вече се предприемат действия по изпълнението им, напр. доразвиването на стратегията за интегрирано гранично управление във връзка с борбата с незаконната миграция.

България представи накратко актуализирания Компендиум от оценката на България в областта на полицейското сътрудничество, като обърна внимание на последователните действия за изпълнение на препоръките.

Коментираха се предстоящите оценки в областта на ШИС и се реши по-стабилен график за бъдещите оценки да се се изготви след приключването на оценката по ШИС на Лихтенщайн, както и решаването на някои проблеми с пътната карта по ШИС1+ на България и Румъния.

Представен бе и актуализиран каталог на най-добри практики за защита на личните данни.

В рамките на заседанието бяха проведени неофициални контакти с представители на Холандия и Румъния във връзка с присъединяването ни към ШИС1+ чрез SISone4ALL.

СЪВМЕСТНИ ОЦЕНКИ В ОБЛАСТТА НА ЗАЩИТА НА ДАННИТЕ В ДЪРЖАВИТЕ – СТРАНИ ПО КОНВЕНЦИЯТА ЗА ПОЛИЦЕЙСКО СЪТРУДНИЧЕСТВО В ЮГОИЗТОЧНА ЕВРОПА

Конвенцията за полицейско сътрудничество в Югоизточна Европа е подписана във Виена на 5 май 2006 г. от Албания, Босна и Херцеговина, Македония, Молдова, Румъния, Сърбия и Черна гора. В сила е от 11 юли 2008 г. Предмет на Конвенцията е укрепването на сътрудничеството между Договарящите страни в борбата срещу заплахите за обществената сигурност и/или ред, както и за превенция, разкриване и разследване на престъпления.

България ратифицира Конвенцията с две резерви:

- обмен на класифицирана информация само с държавите - страни по Конвенцията, с които имаме влезли в сила международни договори за защита на класифицирана информация (в съответствие с чл.113, ал.1 от Закона за защита на класифицираната информация)
- трансфер на лични данни с държави - страни по Конвенцията, след надлежно разрешение от Комисията за защита на личните данни (в съответствие с чл.36 и чл.36а от Закона за защита на личните данни).

След осъществяването на необходимите процедури по нотификация, Конвенцията влезе в сила за България на 1 март 2009 г.

На 25 и 26 февруари 2010 в Любляна, Словения се състоя учредителна среща на Работната група по защита на данните, създадена от Комитета на министрите във връзка с започването на съвместни оценки в областта на защита на данните в държавите-страни по Конвенцията за полицейско сътрудничество. На учредителната среща в Любляна бяха поканени по двама представители от всяка държава-държава - един от Министерство на вътрешните работи и един от независимия национален орган за защита на данните.

През първата половина на 2010 г. България поема председателството на Работната група. Един от основните приоритети е старта на съвместните оценки, които ще се осъществяват по подобие на оценките по Шенген. Ръководител на Работната група в качеството на представител на настоящето българско представителство на Конвенцията е Снежана Малеева от Министерство на вътрешните работи на Република България.

България и Румъния ще участват с техни експерти в съвместните мисии, но няма да подлежат на оценка в рамките на Конвенцията, поради това, че вече са преминали оценките си по Шенген в тази област.

Основната цел на Конвенцията е укрепване на сътрудничеството между договарящите страни с оглед заплахите към обществената сигурност и /или обществения ред, както и по отношение на превенцията, разкриването полицейското разследване на престъпни деяния. Една от най-важните цели на групата е създаването на общество от висококвалифицирани специалисти в областта на личните данни.

Във връзка със защитата на данните по чл.31 от Конвенцията е предвидено, че по отношение на автоматичната обработка на лични данни, всяка от договарящите страни, не по-късно от датата на влизане в сила на Конвенцията предприема необходимите национални разпоредби,с цел постигане на ниво на защита на личните данни, съвместимо с принципите, изложени в Препоръка № R (87) 15 от 17 септември 1987г. на Комитета на министрите на Съвета от Европа относно използването на лични данни в полицейския сектор.Освен това, трябва да бъде постигнато ниво на защита на личните данни, най-малко еднакво с предвиденото в Конвенцията на Съветана Европа за защита на лицата във връзка с автоматичната обработка на лични данни от 28 януари 1981г. Предоставянето на лични данни, предвидено в Конвенцията, се осъществява след влизане в сила на гореизброените разпоредби.

Конвенцията за полицейско сътрудничество е отворена и за други държави, не само за тези от Югоизточна Европа. Австрия и Швейцария са заявили интереса си, в момента се обсъжда и в Словения присъединяването към Конвенцията. Всичко това показва, че към нея се подхожда с разбирането за

много важен правен инструмент в района, като високо се оценява нейната важност.

Първата стъпка, която всяка една държава предприема е процеса на вземане на решение за ратифициране на Конвенцията. Тук е важно да се отбележи, че за държавите-членки на Европейския съюз е задължително спазването на решенията на Комитета на министрите, т.е задължително е въвеждането на Препоръката относно използването на данни в полицейския сектор, което пък е условие за ратифициране на Конвенцията, съгласно чл.31.

Втората важна стъпка е гарантирането на защита на данните съобразно изискванията на Конвенцията. За да се осъществи предоставяне на данни към държавите-страни по нея,трябва да се гарантира определено ниво на защита на данните. България и Румъния са членки на Европейския съюз и като такива, са осигурили ниво на защита на данни съобразно европейските критерии.

Ролята на България като председателстващ на Конвенцията в първата половина на 2010г. е от голямо значение, тъй като се очаква тя да започне съответните мисии (оценки) на държавите- страни по Конвенцията. България ще трябва да докладва на 20 и 21 май в София пред Комитета на министрите напредъка на останалите държави при прилагане на изискванията на Конвенцията.

Работната група по защита на данните е създадена от Комитета на министрите, който е създал и процедурни правила за осъществяване на оценките в областта на защита на данните. В процедурните правила са определени и фазите, през които е задължително да премине всяка една оценка. Обмена на информация може да бъде осъществен единствено след позитивни отзиви от оценката. Договарящите страни, които вече са успешно преминали оценките по Шенген в областта на защита на данните, трябва да бъдат третирани като равностойни на държавите, които са преминали успешно оценките съобразно тези Процедурни правила. Въпреки че България и Румъния няма да бъдат обект на оценка по отношение на защита на данните, те са поканени да номинират техни експерти за членове на експертните екипи съобразно Конвенцията.

По предложение на г-жа Малеева „Наръчника за оценките по Шенген" във връзка със сферата на защита на личните данни ще се използва и за бъдещите оценки по линията на Конвенцията за полицейско сътрудничество. Доводите, които се изтъкнаха бяха, че целта на оценките по Шенген е същата като и на оценките по Конвенцията за полицейско сътрудничество – т.е да се констатира адекватно ниво на защита на данните. Наръчникът ще бъде изпратен до всички участници в Работната група и ще бъде използван като основа при бъдещите проверки. Той е приет на 25 май 2009 г. по предложение на екипите за оценка по Шенген.

Бяха обсъдени отговорите на въпросниците, получени от държавите-страни по Конвенцията. Във въпросниците държавите трябва да отговорят на въпросите дали са ратифицирали Конвенция №108, Препоръка 87/15; какви мерки са въвели за полагане на законодателните основи на защита на данните; дали има въведени мерки по защита на данните в полицейския сектор; има ли сключени двустранни споразумения за обмен на полицейски данни между държавите; по какъв начин се обезпечава сигурността на данните; какви са административно-наказателните разпоредби за неправомерно обработване и др.

Държавите трябва да подготвят план за действие, в който да отбележат информация по отношение на това кога считат, че ще бъдат готови за оценки.

ЗАСЕДАНИЕ НА ПОДГРУПАТА ПО " ПРИЛОЖИМО ПРАВО" КЪМ РАБОТНА ГРУПА ПО ЧЛ. 29

На 18 март 2010 г. в гр. Брюксел се проведе заседание на подгрупата по "Приложимо право" („Ключови разпоредби") към Работната група по защита на данните, създадена въз основа на чл.29 от Директива 95/46 на Европейския парламент и на Съвета за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни. На подгрупата присъстваха представители от Европейската комисия, от компетентните органи по защита на данните на Италия, Словакия, Великобритания, Белгия, Холандия, Франция, Люксембург и Испания. Председателстващ

заседанието на подгрупата беше г-н Питър Хъстингс, европейски надзорен орган по защита на данните. Представител на Комисията за защита на лични данни беше Десислава Борисова, мл. юрисконсулт от дирекция "Правни производства и надзор".

Поради необходимостта от ефективна защита на данните на физическите лица, както и за създаването на ясна правна рамка за администраторите на лични данни се изготвя документ по отношение на „Приложимо право". Една от целите е да се избегне припокриването на различни правни системи при решаването на определи казуси, т.е. да се избегне какъвто и да е конфликт между приложимите права. Разпоредбите на бъдещия документ относно Приложимо право ще представляват lex specialis по отношение на други сфери на правото.

Работният документ се обсъди по отношение на понятието "приложимо право". Важно уточнение в случая е, че документът и бъдещите нововъведения ще бъдат изготвяни съобразно Директива 95/46 и няма да се вземат предвид спецификите по отношение на съответните закони по защита на данните в различните държави. Взе се решение в началото на документа да се направи разграничение между приложимо право и юрисдикция. Обсъди се и задължението на администратора, когато обработването се извършва от негово име, да избере обработващ данните, който осигурява достатъчни гаранции по отношение на мерките за техническа безопасност и организационните мерки, регулиращи обработването, което следва да се извърши, както и да осигури спазването на тези мерки.

Законодателството на голяма част от държавите-членки предвижда налагането на административно-наказателна отговорност само за администратора на лични данни. Директива 95/46 не казва ясно дали обработващият също може да е субект на такава отговорност. „Държавите-членки предвиждат, че всяко лице, което е понесло вреди в резултат на неправомерна операция по обработката или на каквото и да е действие, което е несъвместимо с националните разпоредби, има право да получи обезщетение от администратора за понесените вреди. Администраторът може да бъде изцяло или частично освободен от такава отговорност, ако докаже, че не носи отговорност за събитието, довело до причиняване на вредите." Ако се окаже, че администратора не носи отговорност за настъпилите вреди, дали може да се приеме, че обработващият трябва да обезщети засегната страна. По този въпрос не се достигна до единно становище.

При предоставянето на данни се даде пример, ако фирма за набиране на персонал в страна А събира данни относно това дали работниците или служителите са болни от СПИН, обработващият данни се намира в старна В, където предоставяне на данни относно СПИН е забранено, няма правна пречка данните да се съхраняват в страна В и при необходимост да се предоставят в страна А. Случаят показва, че само ако в една от държавите-членки такова предоставяне на данните е разрешено, тогава е възможно да се осъществи.

Обсъди се дали критерият „ определя целите и средствата", който беше избран при изготвянето на документа „Администратор на лични данни/Обработващ", може да се използва и при определяне на приложимо право. В документа, изпратен до участниците, един от предложените критерий е "седалище на администратора". Този критерий лесно може да се приложи в случая, при който администраторът има седалище в една държава, а обработва данни в друга. Тогава се прилага правото на държавата, в която администраторът има седалище.

Великобритания обърна внимание на факта, че е добре да се има предвид изложения в примерния документ друг критерий, а именно „в контекста на осъществяваната дейност". Този критерий може да се приложи, ако например администраторът има седалище в държава-членка, но има и седалище в друга държава-членка, в която всъщност се осъществява обработването на данни в контекста на осъществяваната от администратора дейност. Разгледаха се няколко подобни казуса, за да се онагледи този критерий.

В края на май 2010 Европейският надзорен орган по защита на данните ще подготви нов документ по отношение на „Приложимо право", който ще бъде изпратен до всички участници в подгрупата за коментари и забележки.

УЧАСТИЕ В СЪВМЕСТНИЯ ПРИНОС НА ЕВРОПЕЙСКИТЕ ОРГАНИ ПО ЗАЩИТА НА ДАННИТЕ КЪМ ПУБЛИЧНА КОНСУЛТАЦИЯ

През март 2010 г. Комисията за защита на личните данни подкрепи проекта на съвместен принос на европейските органи за защита на данните, участващи в Работна група по чл. 29 и Работна група по полиция и правосъдие към публичната консултация по съдържанието на споразумението между ЕС и САЩ за защита на данните и обмен на информация при сътрудничеството по въпроси на правоприлагането.

Направленията и основните принципни положения, които се предлага да залегнат в споразумението са следните:

1. Целта на споразумението е създаването на задължителни правила за защита на данните, които да гарантират постигането на висок стандарт в защитата на информацията в сферата на правоприлагането и които да бъдат включени във всяко последващо споразумение между ЕС и САЩ, свързано с трансфер или обмен на данни за целите на правоприлагането или съдебното сътрудничество по криминални въпроси. В тази връзка е необходимо изясняване на понятията "правоприлагане" и "сътрудничество по въпросите на правоприлагането" и спазването на принципите на реципрочност при обмена на данни и на минимизация на предоставяната информация.

2. Необходимо е в споразумението да бъдат включени полицейското и съдебното сътрудничество по криминални въпроси като основни елементи в трансатлантическото взаимодействие, като стандартите за защита на данните да се отнасят и за тях. Обръща се внимание, че споразумението не може да служи като правно основание за обмен на информация и данни. Предлага се неговият обхват на действие да е по-широк с цел постигане на правна яснота относно условията за прилагането на принципите за защита на данните и стриктното спазване на принципа на ограничение на целта. Преди извършването на трансфер е необходимо да бъде показана нуждата и пропорционалността на такова прехвърляне на данни. Споразумението трябва да се прилага и за трансатлантически трансфери на лични данни, свързани с частни фирми, като не се насърчава директният трансфер от частна компания в страна А до правоприлагащи органи в страна Б. Счита се, че определени въпроси, свързани с трансфери от частни към държавни органи могат да се решават по-адекватно със специални споразумения, в които да се вземат предвид конкретните обстоятелства по събирането на данните.

3. Съществува ясна нужда от въвеждане на подходящи вътрешни и външни механизми за осигуряване, преценка и спазване на съответствието. Необходимо е компетентните органи за защита на данни да участват във външните, а където е необходимо във вътрешните процедури по преценка. В споразумението трябва да се заложи възможността на субекта на данни за упражняване на правата му на достъп, промяна и изтриване на личните данни по лесен и ефективен начин. Съгласно европейското или национално право, правото на достъп може да бъде упражнявано или директно чрез администратора на данни или непряко, като то да се гарантира за всички, независимо от националността или страната на пребиваване. Споразумението трябва да осигури ефективни административни и правни механизми за упражняване на правото на обжалване на действията на администратора на данни.

4. Принципите на споразумението да са задължителни за страните по него, както и за всички настоящи и бъдещи договорености между ЕС и САЩ в тази връзка. Всички външни трансфери до трети страни да се извършват след предварително изразено и писмено съгласие на страната по произход като се спазват целите, за които първоначално са прехвърлени данните и ако третата страна предостави адекватно ниво на защита. В споразумението трябва да е заложена компетентността на органите за защита на данните да преглеждат, преценяват и проверяват съответствието и на двете страни с принципите за защита на данните, които да бъдат вкарани в бъдещите двустранни споразумения между ЕС и САЩ, свързани с трансфер и обмен на данни. Периодите за задържане на данни трябва да бъдат пропорционални и не прекалено дълги по отношение на целта на събиране и допълнителна обработка на данните.

Споразумението трябва да е с дълъг срок на действие и с възможност за ревизия през определен период.

ЕВРОПЕЙСКАТА АГЕНЦИЯ ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ (ENISA) ПРАВИ ПРЕГЛЕД НА ОПИТА В ОБРАБОТКАТА НА СЪОБЩЕНИЯ ЗА ПРОБИВ В ДАННИТЕ

Въвеждането на европейските изисквания за уведомяване при пробив в данните в сектора на електронните комуникации представлява съществено развитие, планирано с промените на Директива 2002/58/ЕС („the Eprivacy Directive"). Това ще доведе както до повишаване както на нивото на сигурност на данните в Европа, така и до увереност гражданите, че техните лични данни в комуникационния сектор са защитени. Европейската агенция за мрежова и информационна сигурност (ENISA) прави преглед на настоящата ситуация с цел да бъде разработен последователен набор от насоки за подобряване на прилагането на мерките и процедурите, описани в член 4 от Директива 2002/58/ЕС. Освен това, ENISA има за цел да изясни дали разпоредбите на директивата са приложими и за други сектори извън този на електронните комуникации.

ENISA започна проучване на политиките на страните-членки във връзка с уведомяване при настъпване на пробив в данните. Резултатите от изследванията ще послужат за сравняване на процедурите по уведомяване в различните сектори и страни. Ще се обобщи и анализира опита на националните органи за защита на данните и телекомуникационни оператори и други компании от цяла Европа. Изследването има за цел да събере информация от всички заинтересовани страни - както тези с богат опит в съобщенията за пробив на данни, така и тези, които са в ранен етап в това отношение.

Като първа стъпка целта на ENISA е да добие представа за опита на заинтересованите страни в частния и публичния сектор и препоръките за въвеждане на механизми за уведомяване при нарушения в сигурността на данните. Тази дейност се осъществява в сътрудничество с IDC, световна фирма за проучване и консултации в телекомуникациите и ИТ пазара. Проучването се извърши чрез въпросници и интервюта в рамките на първото тримесечие на 2010 година. Въпросите касаят както общи, така и конкретни стъпки по механизмите за уведомяване - има ли съответната организация ръководства или препоръчителни процедури, има ли проблеми при разграничаването на личните данни от други видове данни като корпоративни/ професионални/ трафични, кои обстоятелства се квалифицират като пробив в данните, как се определя рискът от пробив, кой изготвя доклада за извършен пробив в данните, кой взема решение за уведомяване на засегнатите лица, каква информация се включва в уведомлението, налагат ли се санкции и т.н.

Като резултат се очаква да се получи изследване и разработка по този критичен компонент, свързан с гарантиране на личната неприкосновеност – информиране при извършване на нарушение в сигурността на данните.

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА ИЗВЪРШЕНИТЕ ПРОВЕРКИ ЗА ПЕРИОДА МАРТ – АПРИЛ 2010

На основание чл. 12 от Закона за защита на личните данни (ЗЗЛД) през март и април са извършени общо 202 проверки.

Най-голям е делът на предварителните проверки, извършвани на основание чл.17б от ЗЗЛД (когато администраторът е заявил обработване на данни по чл. 5, ал. 1 от ЗЗЛД или на данни, чието обработване съгласно решение на комисията застрашава правата и законните интереси на физическите лица). За януари и февруари извършените предварителните проверки са 196 бр. В резултат на проведената кампания за актуализация на регистрите на администраторите на лични данни, броят на предварителните проверки значително ще се увеличава през следващите месеци.

На основание изготвените констативни актове от тези проверки в регистъра по чл. 10, ал. 1 т. 2 от ЗЗЛД са вписани 195 администратора след извършена предварителна проверка. За 2 администратори процедурата по вписване е прекратена на различни основания.

По административни производства по жалби пред КЗЛД са извършени 2 текущи проверки. Констативните актове от проверките са внесени за разглеждане от колегиалния орган на КЗЛД. Съгласно утвърдения "План за извършване на текущи проверки по инициатива на Комисията за защита на личните данни (КЗЛД) за 2010 г." са приключили проверките на "България Ер" АД и Медицински университет – София без констатирани нарушения.

В процес на приключване са проверките на "Уиз Еър България Еърлайнс" ЕАД, "Хели Ер – САУ" АД и "Авиокомпания Хемус Ер" ЕАД. Предстоят още проверки на няколко големи дружества авиопревозвачи.

През месец март са съставени два акта за установяване на административни нарушения (АУАН), като в първия случай актът е съставен на дружество, за което е установено, че обработва лични данни, без да е подало Заявление за регистрация в КЗЛД и без да е вписано в Регистъра по чл. 10, ал. 1, т. 2 от ЗЗЛД. Вторият АУАН е връчен на дружество, за което е установено, че обработва лични данни, свързани със здравето на физически лица, без да е уведомена за това обстоятелство КЗЛД.

РЕГИСТРАЦИЯ НА АЛД

СТАТИСТИКА НА ИНФОРМАЦИЯТА ОТ ОТДЕЛ “РЕГИСТЪР И АРХИВ”

През месеците март и април цялостната дейност на отдел „Регистър и Архив”, подпомогнат от служители на отдел „Комуникационни и информационни системи” бе насочена към обработката на постъпилите на хартиен носител заявления и молби за освобождаване.

Използването на автоматизираната информационн асистема еРАЛД през интернет позволява на администраторите да подадат документи по електронен път, да получат свое потребителско име и парола за системата и да имат пълен достъп до информацията, която се съхранява за тях в Комисията за защита на личните данни. Тъй като по ЗЗЛД всяка промяна в декларираните обстоятелства трябва да се отразява, то в интерес на всеки администратор е да може бързо и удобно да извършва необходимите корекции в своите данни. За целта сме се постарали да предоставим кратка и според нас ясна инструкция за работа със системата, като целта е колкото може повече администратори да се справят по интернет със своята регистрация и поддържането на данните в актуален вид.

На графиката е илюстриран броят въведени в автоматизираната информационна система заявления на администратори на лични данни:

До приключването в средата на февруари на кампанията по актуализация и регистрация на администраторите на лични данни в КЗЛД по електронен път постъпиха заявленията на 195924 администратори на лични данни, а на хартиен носител – 101 403. От постъпилите по електронен път заявления, 16% са подадени с електронен подпис, т.е. напълно автоматизирано.

Заявленията, подадени по електронен път представляват въвеждане директно в базата данни на информационнта система. Заявленията, подадени на хартиен носител трябва да бъдат въведени в същата база данни от наши служители. Към момента за изтеклите два месеца са въведени 23 688 зявления за вписване или актуализиране на данни.

След въвеждането се извършва проверка за коректност съответствие на данните и одобрение от проверяващ служител. Тези администратори, които извършват първоначална регистрация след одобрение от проверяващия служител биват включен в един от двата списъка:

- за гласуване от комисията – когато не обработва данни по смисъла на чл.5 от ЗЗЛД;
- за проверка по 17б - когато обработва данни по смисъла на чл.5 от ЗЗЛД.

Големият брой обработени заявления съответно доведе до необходимостта от извършване на голям брой предварителни проверки по чл. 17б.

Сравнението на броя необходими проверки по 17б само за първите четири месеца на 2010 г. с предходните две години е илюстрирано на графиката:

Администраторите, които са включени в списъка на предложените за вписване, се предлагат се на заседание на комисията и им се издава на уникален идентификационен номер. Веднага след вземане на решението администраторът бива вписан в "Регистъра на АЛД и на водените от тях регистри с лични данни". През изтеклите два месеца в регистъра са вписани над 16 000 АЛД. Освободените от регистрация с решение на комисията администратори на лични данни към момента са 1810, като 95 % са освободени с решение на комисията през последните два месеца.

Регистърът на вписаните администратори на лични данни и **Списъкът на освободените от регистрация с решение на КЗЛД** са публични и са достъпни от интернет страницата на комисията.

РЕШЕНИЯ НА КЗЛД

РЕШЕНИЯ ПО ЖАЛБИ

РЕШЕНИЕ
№ 954/24.02.2010 г.

Комисията за защита на личните данни /КЗЛД/ в състав: Венета Шопова, Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков, на открито заседание, проведено на 24.02.2010 г., на основание чл. 10, ал. 1, т. 7 от Закона за защита на личните данни /ЗЗЛД/, разгледа по същество жалба с рег. № В- 954/ 15.01.2009 г. от Р.Ц.Ш. срещу Агенция по вписванията.

Страните са редовно уведомени за разглеждане на жалбата по същество.

За жалбоподателя Р.Ш. се явява адв. Славена Атанасова с нотариално заверено изрично пълномощно.

За Агенцията по вписванията се явява юрисконсулт Десислава Иванова с пълномощно изх. № 91-00-58/20.10.2009 г.

В деловодството на КЗЛД е постъпила жалба с рег. № В- 954/ 15.01.2009 г. от Р.Ц.Ш.- акционер в "А.М." АД- гр. П., срещу действия на Агенцията па вписванията, свързани с поддържане на Търговския регистър, които засягат правния интерес на жалбоподателя в качеството му на физическо лице.

В жалбата се твърди, че на 15.09.2009 г. след извършена справка в електронната интернет-база данни на Търговския регистър по партидата на "А.М." АД е публикуван списък на акционерите, придобиващи акции в приемащото дружество в резултат на извършено през 2008 г. вливане на "А.И." АД в "А.М." АД. В приложения списък фигурират трите имена, ЕГН, постоянен и настоящ адрес на жалбоподателя, както и точния брой на придобитите акции. Жалбоподателят счита това за незаконосъобразно, тъй като никога не е изразявал съгласие за свободен достъп на трети лица до неговите лични данни. На 26.10.2010 г. на основание чл. 28 а, т. 1 и във връзка с чл. 32, ал. 4 от ЗЗЛД Р.Ш. е поискал от Агенцията по вписванията заличаването на данните му от сайта на Търговския регистър, за което е получил отказ.

Отправено е искане до КЗЛД за предприемане на действия, с които да се задължи Агенцията по вписванията да заличи личните данни на жалбоподателя, както и на останалите акционери в "А.М." АД от списък на акционерите, приложен в електронния вариант на Търговския регистър по партида на посоченото дружество

Към жалбата не се прилагат писмени доказателства.

При служебно направена справка в Търговския регистър се потвърждават твърденията на жалбоподателя, във връзка с което към преписката се прилага копие-извадка от електронния вариант на Търговския регистър "Списък на новите акционери в " А.М ." АД в резултат на АИ в АМ след 02.07.2008 г.".

Процесуалният представител на жалбоподателя заявява, че така отразената информация е прекомерна, надхвърляща целите с оглед на които е необходима и настоява за заличаване на единните граждански номера и адреси на акционерите от електронния образ на "Списък на новите акционери в " А.М ." АД в резултат на АИ в АМ след 02.07.2008 г." в Търговския регистър.

От страна на Агенцията по вписванията се застъпва становище за неоснователност на жалбата, позовавайки се на разпоредбата на чл. 13, ал. 9 от Закона за търговския регистър, съгласно която в случаите при които в заявлението или в приложените към него документи са посочени лични данни, които не се изискват по закон, се смята, че предоставилите ги лица са дали съгласието си за тяхното обработване от агенцията и за предоставянето на публичен достъп до тях.

В чл. 27, ал. 2, т. 6 от АПК законодателят обвързва преценката на допустимостта на искането с наличие на специални изисквания, установени със закон. Приложимостта на Закона за защита на личните данни е свързана със защита на физическите лица във връзка с обработването на техните лични данни от лица, имащи качество на администратори на лични данни по смисъла на легалната

дефиниция на чл. 3. Тоест, това изискване се явява абсолютна процесуална предпоставка, с оглед на която следва да се прецени допустимостта на жалбата. В конкретния случай, Р.Ш. сезира комисията с жалба в качеството си на физическо лице срещу Агенцията по вписванията- администратор на лични данни по смисъла на чл. 3, ал. 2 от ЗЗЛД, поради което КЗЛД следва да упражни правата си по чл. 10, ал. 1 т. 7 от закона, който регламентира правомощието й по разглеждане на жалби срещу актове и действия на администратори на лични данни, с които се нарушават правата на физическите лица по ЗЗЛД.

От друга страна, приложението на закона за защита на личните данни се обвързва с обработването на информация, представляваща "лични данни" по смисъла на легалната дефиниция на чл. 2, ал. 1, съгласно която тя трябва да е в такъв обем, чрез който физическото лице да може да бъде идентифицирано.

Чрез информацията, отразена в сканираните документи, жалбоподателят може да бъде еднозначно идентифициран и в този смисъл правото му на лична неприкосновеност попада под закрилата на ЗЗЛД.

Приложимостта на ЗЗЛД е обвързана и с изискването обработването на лични данни да се извършва с автоматични средства. Съгласно дефиницията в §1, т. 2 от ДР на ЗЗЛД относно понятието "регистър на лични данни"- Търговският регистър като единна централизирана електронна база данни, управлявана от информационна система отговаря на изискванията на чл. 1, ал. 3, т. 1 от ЗЗЛД относно приложимостта на закона.

Видно от сканираните и приложени към Търговския регистър документи се налага изводът, че жалбоподателят е спазила законоустановения срок, в който може да сезира с жалба комисията.

От гореизложеното следва, че жалбата е подадена в законоустановения срок, при наличие на правен интерес, от надлежна страна, при спазени специални изисквания на закона, поради което е обявена от Комисията за процесуално допустима с Решение от 03.02.2010 г.

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в процесуалното производство, съгласно чл. 7 от АПК, изискващ наличието на установени действителни факти от значение за случая, имайки предвид представените писмени доказателства и изразени становища, Комисията приема, че разгледана по същество жалбата е неоснователна.

Комисията за защита на личните данни е независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Закона за защита на личните данни, чиято цел е да е гарантира неприкосновеността на личността и личния живот на физическите лица чрез осигуряване на защита при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните. Обработването на личните данни от страна на администраторите на лични данни съгласно чл. 2, ал. 2, т. 1 от ЗЗЛД, следва да бъде законосъобразно и добросъвестно, при наличието на условията на чл. 4, ал. 1, едно от които е изпълнение на нормативно установено задължение на администратора на лични данни.

Воденето и съхраняването на данни от Търговския регистър, което представлява обработване на лични данни по смисъла на §1, т. 1 от ДР на ЗЗЛД, е правомощие на Агенцията по вписванията съгласно чл. 3, ал. 1 от ЗТР. Правомощията й по отношение неговото поддържане са регламентирани със ЗТР, който прогласява неговата публичност. Тази публичност законодателят обвързва с възможността на всеки гражданин да има право на свободен и безплатен достъп до него и до електронния образ на документите, въз основа на които са извършени вписванията, заличаванията и обявяванията, както и до електронния образ на фирмените дела на преерегистрирани търговци- чл. 11 от ЗТР. Задължение на всеки търговец е а поиска да бъде вписан в търговския регистър, като заяви подлежащите на вписване обстоятелства и представи подлежащите на обявяване актове. Вписване, заличаване и обявяване се извършват въз основа на заявление по образец, чиито реквизити, начин и ред за попълване са детайлно регламентирани в глава II на Наредба № 1 от 14 февруари 2007 г. за водене, съхраняване и достъп до търговския регистър, издадена от Министерство на правосъдието.

Достъпът до Регистъра се оказва на практика неограничен, тъй като справките по него могат да се правят чрез множество критерии, посочени в чл. 32 от ЗТР.

Допустимостта на обработването на лични данни съгласно чл. 4, ал. 1, т. 2 от ЗЗЛД от друга страна е обвързано с наличие на изпълнение на нормативно установено задължение на администратора на лични данни. В този смисъл обработването на лични данни на физически лица чрез Търговския регистър от страна на Агенцията по вписванията се явява нейно вменено задължение по силата на закона. А по отношение на прекомерно отразената информация относно личните данни, съгласието за тяхното отразяване отново намира легална уредба в разпоредбата на чл. 13, ал. 9 от ЗТР.

Въпреки установената законосъобразност на обработването, Комисията винаги е считала, че регламентираната по този начин в ЗТР публичност на Търговския регистър не осигурява достатъчна организационна и техническа защита на съдържащите се в него лични данни на физическите лица и законодателят не е предвидил гаранции за неправомерен достъп до тях, каквото е императивното изискване на чл. 23, ал. 2 от ЗЗЛД. В този смисъл, макар и данните на жалбоподателя да са обработвани законосъобразно от страна на Агенцията по вписванията като администратор на лични данни с нормативно определени правомощия, в съответствие със специално действащата уредба, регулираща действията във връзка с поддържане на Търговския регистър, то предоставянето на неограничен достъп до такъв обем данни е в противоречие с идеята и целта на ЗЗЛД за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при обработване на свързаните с тях лични данни в процеса на свободното движение на момента начин за достъп до значителен обем от лични данни, осигурява свободен достъп до него, без да е необходимо изрично разрешение на държавен или друг орган за това, но не гарантира неприкосновеността на личността и личния живот на физическите лица, както прокламира ЗЗЛД.

Колизия на двата закона и преследваните с тях цели е проблем, който следва да бъде предмет на бъдеща законодателна промяна, чрез която да се намери баланса между обществения и личен интерес, което е от компетентността на Народното събрание.

С оглед гореизложеното и на основание чл. 10, ал. 1, т. 7 от ЗЗЛД, Комисията:

РЕШИ :

Оставя без уважение жалба с рег. В- 954/ 15.01.2009 г. от Р.Ц.Ш. срещу Агенция по вписванията.

Решението на Комисията може да се обжалва пред Върховния административен съд в 14-дневен срок от получаването му.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
ОМ Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
№ 2469/24.02.2010 г.

Комисията за защита на личните данни /КЗЛД/ в състав: Венета Шопова, Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков, на открито заседание, проведено на 24.02.2010 г., на основание чл. 10, ал. 1, т. 7 от Закона за защита на личните данни /ЗЗЛД/, разгледа по същество жалба с рег. № Ж-2469/30.11.2009 г. от П.П. срещу Виваком /новата търговска марка на обединението на БТК АД и Вивател/.

Страните са редовно уведомени за разглеждане на жалбата по същество. Не се явяват, не изпращат процесуални представители, не ангажират нови доказателства по случая.

С жалба рег. № Ж-2469/30.11.2009 г. П.П. сезира Комисията за злоупотреба с личните му данни от страна на Виваком.

Жалбоподателят информира, че сим-картата му е била блокирана чрез последователно въвеждане на три погрешни пин-кода.

След проведен разговор с оператор на Виваком става ясно, че картата ще остане блокирана, но клиентът няма да загуби номера си.

След като регистрирал въпросната сим-карта на свое име, г-н П. започнал да получава непознати обаждания на всичките си номера към Виваком.

В тази връзка г-н П. проверил, че картата вече не е регистрирана, а операторът е отказал съдействие за преиздаване на същата.

Жалбоподателят счита, че описаното "само може да означава, че служител на Виваком се е възползвал от правомощията си, преиздал е картата за лична облага и дори е злоупотребил със съхранението на лични данни като ги разпространява на трети лица или ползва не служебно".

С писмо изх. № И-5885/11.12.2009 г. жалбоподателят е уведомен, че във връзка с твърдените от негова страна некоректни действия на служителите на Виваком, следва да се обърне със запитване към оператора, с който се намира в договорни отношения.

В отговор на уведомителното писмо г-н П. допълнително прилага своя жалба да Виваком от 30.11.2009 г., като твърди, че към момента не е получил отговор на поставените от него въпроси. За пореден път изразява опасения за злоупотреба от страна на служител на Виваком с неговите лични данни, които счита, че са били предоставени на трето лице, което му оказвало тормоз по телефона на номерата на всички притежавани от него сим-карти от същия оператор.

С Решение от 20.02.2010 г. Комисията приема жалбата за допустима и изисква становище по случая от Виваком.

С писмо вх. № В-2496/16.02.2010 г. от страна на Виваком представят писмено становище по визираните в жалбата факти, с които навеждат мотиви в подкрепа на твърденията си за неоснователност на жалбата. Посочва се, че казусът има за предмет спор за собственост на сим-карта, чието разрешаване е извършено и приключило по установения ред, като за ползвател на същата е определено лицето Е.Н., тъй като последната е предоставила в пълнота нужната информация.

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в процесуалното производство, съгласно чл. 7 от АПК, изискващ наличието на установени действителни факти от значение за случая, имайки предвид представените писмени доказателства и изразени становища, Комисията приема, че разгледана по същество жалбата е неоснователна.

Комисията за защита на личните данни е независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Закона за защита на личните данни, чиято цел е да е гарантира неприкосновеността на личността и личния живот на физическите лица чрез осигуряване на защита при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните. Обработването на личните данни от страна на администраторите на лични данни съгласно чл. 2, ал. 2, т. 1 от ЗЗЛД, следва да бъде законосъобразно и добросъвестно, при наличието на условията на чл. 4, ал. 1, едно от които е изпълнение на нормативно установено задължение на администратора на лични данни.

С промените в Закона за електронните съобщения от 2009 г. (§80 от ПЗР) и приемането на Правилата за събиране на данни, необходими за идентифициране на потребители на предплатени услуги преди 01.01.2010 г. от Комисията за регулиране на съобщенията, като потребители на спорната сим-карта се регистрират жалбоподателят П.П. на 23.11.2009 г. и Е.Н. на 29.11.2009 г. Поради възникнал спор относно собствеността на сим картата от така посочените лица е било необходимо изискването на допълнително информация от страна на Виваком, която касае модели апарати, в които е използвана картата, сериен номер на мобилния апарат, в който тя е била поставяна, допълнително информация, относима към доказването собствеността на картата. Тъй като Е.Н. предоставя посочената информация, спорната сим-карта се регистрира на нейно име. От страна на П.П. не са пред-

приети указаните му от страна на мобилния оператор действия относно доказване собствеността на сим картата.

От така изложената фактическа обстановка е видно, че данните на П.П. се обработват от Виваком в качеството му на клиент на дружеството във връзка с използвани от него услуги. Договорния характер на отношенията между страните предполагат наличието на законоустановени предпоставки за законосъобразното обработване на личните данни на жалбоподателя, свързани с наличието на неговото изрично съгласие като основание за допустимостта на обработване на лични данни- чл. 4, ал.1, т. 2 от ЗЗЛД, както и с правото на обработването от страна на администратора на лични данни необходимо за изпълнение на задължения по договор- чл. 2, ал. 1, т. 3 от ЗЗЛД. В този смисъл, предприетите действия от страна на Виваком във връзка с доказване на собствеността на оспорената сим карта са законосъобразни. От представените по жалбата доказателства и становища не се установява наличие на факти, които да индикират наличие на неправомерно обработване и по-конкретно – неправомерно разпространение на личните данни на П.П. от страна на Виваком.

С оглед гореизложеното и на основание чл. 10, ал. 1, т. 7 от ЗЗЛД, Комисията:

РЕШИ :

Оставя без уважение жалба с рег. № Ж-2469/30.11.2009 г. П.П. срещу Виваком /новата търговска марка на обединението на БТК АД и Вивател/.

Решението на Комисията може да се обжалва пред Върховния административен съд в 14-дневен срок от получаването му.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
№ 10/17.03.2010 г.

Комисията за защита на личните данни /КЗЛД/ в състав: Венета Шопова, Красимир Димитров, Мария Матева, Валентин Енев и Веселин Целков, на открито заседание, проведено на 17.03.2010 г., на основание чл. 10, ал. 1, т. 7 от Закона за защита на личните данни /ЗЗЛД/, разгледа по същество жалба с рег. № Ж- 10/21.01.2010 г. от Й.Х. срещу МВР.

Жалбоподателката Й.Х. сезира КЗЛД с жалба, в която твърди, че органите на МВР-ОД МВР-Ш. неправомерно обработват нейни лични данни, изразяващо се в неправомерно разпространение на единния й граждански номер, в нарушение на разпоредбите на чл. 2, ал. 2, т. 1 и чл. 4, ал. 1, т. 1 от ЗЗЛД, излагайки следната фактическата обстановка:

По гр.д. № 601/2008 г. по описа на Районен съд- Ш., жалбоподателката е упълномощена от сина си да го представлява на основание чл. 20, ал. 1, б. “б” ГПК /отм./.

На 09.12.2009 г. в провелото се открито съдебно заседание по делото процесуалният представител на ищеца- МВР депозира по делото писмо от Висшия адвокатски съвет /ВАдвС/, което представлява отговор на запитване от страна на ОД МВР- Ш. относно правоспособността на г-жа Х. на действащ адвокат. В писмото се съдържат нейните три имена и ЕГН.

Жалбоподателката счита, че е налице неправомерно предоставяне на нейни лични данни от страна на ОДМВР- Ш. на Висшия адвокатски съвет, респ. на Районен съд- Ш. Посочва, че нужната информация би могла да бъде получена от Единния регистър на ВАдвС, който е публичен и достъпът до него е свободен и не изисква посочване на ЕГН.

Към жалбата се прилагат копия от – писмо изх. № 522 от 16.6.2009 г. на ВАдвС, извадка от

Протокол от открито съдебно заседание по гр. д. № 601/2008 г. по описа на РС- Ш., разпечатка от базата данни от електронния вариант на Единния регистър на ВадвС, както и решения от практиката на КЗЛД.

С Решение от 17.02.2010 г. (Протокол № 6) Комисията конституира министъра на вътрешните работи като ответник по жалбата в качеството му на администратор на лични данни, и като заинтересована страна- ОДМВР-Ш. От тях, както и от председателя на ВАдвС са изискани становища по случая, респ. и представянето на относимите към случая писмени доказателства.

С писмо изх. № 225/08.03.2010 г. от страна ВАдвС се заявява, че информацията относно Й.Х. е предоставено на ОДМВР- Ш. в отговор на тяхно запитване на базата на идентификацията, представена от самия орган. За целта прилагат копие от искането на ОДМВР- Ш. до ВАдвС, респ. и дадената справка.

От страна на министъра на вътрешните работи е депозирано становище по жалбата, в което се навеждат доводи за нейната недопустимост и неоснователност. По отношение на обстоятелствата, имащи отношение към допустимостта на жалбата се изтъква, че последната е насочена срещу конкретни действия на директора на ОДМВР- Ш., които не следва да бъдат отнесени към отговорността на министъра на вътрешните работи в качеството му на администратор на лични данни. С подробно изложени съображения по основателността на жалбата се сочи, че са налице предпоставки, допускащи обработването на личните данни на жалбоподателката в хипотезите на чл. 4, ал. 1, т. 6 и т. 7 от ЗЗЛД.

От страна на ОДМВР- Ш. се представя становище, в което се твърди, че личните данни на жалбоподателката са обработени законосъобразно, използвани единствено за нуждите на гражданско дело № 601/2008 г. по описа на Районен съд- Ш. за защита интересите на МВР, с което не е засегната личната й неприкосновеност и не е налице нарушение на ЗЗЛД.

Жалбата е насрочена за разглеждане по същество на 17.03.2010 г., за което страните са редовно уведомени, като единствено за МВР се явява юрисконсулт Благой Иванов с надлежно пълномощно.

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в процесуалното производство, съгласно чл. 7 от АПК, изискващ наличието на установени действителни факти от значение за случая, имайки предвид представените писмени доказателства и изразени становища, Комисията приема, че разгледана по същество жалбата е неоснователна.

Основателността на жалбата следва да се прецени с оглед обстоятелствата, при които е предоставена информация за ЕГН на жалбоподателката от страна на ОДМВР-Ш. на ВАС и Районен съд- Ш.

Според чл. 148, ал. 2 от Закона за съдебната власт ВАС води единни адвокатски регистри за адвокати, младши адвокати, за адвокатски дружества и за чуждестранни адвокати. Правилата за водене на регистрите се определят с Наредба № 3 от 29 октомври 2004 на ВАдвС. В единните регистри се вписват предвидените в закона обстоятелства въз основа на данни от регистрите на адвокатските съвети. В чл. 6, ал. 1, т. 2 от тази наредба е посочено, че информацията за подлежащите на вписване обстоятелства в регистъра на адвокатите се посочва в заявление съгласно приложение № 1 в полета, обединени в групи, включително в поле № 4 "ЕИН" се посочва единният граждански номер на адвоката. Според чл. 24, ал. 1 и ал. 2 от същата наредба ВАдвС издава удостоверения за вписаните обстоятелства в регистрите и преписи от документите, въз основа на които са извършени вписванията. ВАдвС издава и справки със съдържанието на удостоверенията по ал. 1, както и незаверени преписи от документите по ал. 1. Справките се предоставят устно, писмено или по електронен път. В случая точно такава справка е изискана от ОДМВР- Ш. от ВАдвС- относно правоспособността на жалбоподателката като действащ адвокат. Касае се за представено и прието от РС-Ш. доказателство-официален документ по съответното гражданско дело, каквото не може да бъде според твърденията в жалбата разпечатка от интернет. Информацията за вписаните адвокати по колегии, която се публикува всяка година в ДВ е официална, а в регистрите настъпват промени /вписват се нови адвокати, някои се отказват, други се наказват с лишаване от адвокатски права/. Тъй като по съответното гражданско

дело е била необходима актуална информация, изисканата справка е включвала като информация ЕГН на жалбоподателката, тъй като по този начин тя би могла да бъде идентифицирана еднозначно като се избегне възможността за дублиране на имената.

Видно от представените доказателства, така сочените действия по обработване на личните данни на Й.Х. не представляват разпространение на лични данни, дотолкова доколкото достъпът до тях не е неограничен, а се касае за действия, предприети във връзка с нуждите по гр. дело за упражняване на законните интереси и права на ищеца по образуваното съдебно производство.

Чл. 4, ал. 1, т. 6 от ЗЗЛД допуска обработването на лични данни, когато то е необходимо за упражняване на правомощия, предоставени със закон на администратора на лични данни. В случая министърът на вътрешните работи, който е администратор на лични данни, е задължен и оправомощен от ЗМВР да представлява МВР и да ръководи финансовото осигуряване. В рамките на тези свои задължения той е осъществявал функции по защита на икономическия интерес на МВР в производството по гр.д. 601/2008 г. на РС Ш.

При изпълнението на тези законово определени задължения за него е налице и друго условия по чл. 4, ал. 1, т. 7 от ЗЗЛД, което допуска обработване на лични данни. Като страна в съдебното производство, законовият интерес е да осъществи своята защита, като събере и предостави на съда всички необходими доказателства. Тази необходимост за реализиране на законните интереси определя и допустимостта на извършената обработка на ЕГН на жалбоподателката.

С оглед гореизложеното, Комисията

РЕШИ :

Оставя без уважение жалба с рег. № Ж- 10/21.01.2010 г. от Й.Х. срещу МВР.

Решението на Комисията може да се обжалва пред Върховния административен съд в 14-дневен срок от получаването му.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
е-В-80/17.03.2010 г.

Комисията за защита на личните данни в състав: Председател: Венета Шопова и членове Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков на заседание, проведено на 17.03.2010 г. /Протокол №9/ разгледа искане вх.№ е-В-80/13.01.2010г. получено по електронната поща от Д.С.Й.

С искането от госпожа Й. се уведомява Комисията, че в интернет сайт има качена нейна снимка, без да е изразила изричното си съгласие за публикуването й и моли Комисията да бъде заличена от там.

В чл.38, ал.1 от Закона за защита на личните данни е определен преклузивен срок, в който физическото лице има право да сезира Комисията за защита на личните данни. В искането не е посочено, кога е извършено твърдяното от госпожа Й. неправомерно обработване на личните й данни, за да се направи извод, че жалбата е подадена в срок. В искането не е посочен и адреса на сайта, в който е качена снимката й, поради което не може да се определи срещу кого е насочена жалбата и дали той има качеството администратор на лични данни.

Формата на искането, с което се сезира Комисията за защита на личните данни и реквизитите, които трябва да съдържа, са определени в чл.30, ал.1 от Правилника за дейността на Комисията за

защита на личните данни и нейната администрация.

Постъпилото искане не съдържа тези реквизити.

В изпълнение на чл.30, ал.1 и ал.2 от Административно-процесуалния кодекс са дадени указания на искателя с писмо изх.№ И-179/21.01.2010 г., в което й е указано, че искането страда от пороци и на основание чл.30, ал.2 от АПК следва да ги отстрани в тридневен срок от получаване на съобщението за това. Указано е също така, че при неизпълнение на дадените указания образуваното административно производство ще бъде прекратено. Писмото е изпратено на посочения в искането адрес. Видно от известие за доставка /обратна разписка/ молителката го е получила на 27.01.2010 г. Срокът за изпълнение на дадените указания е изтекъл на 30.01.2010 г. и нередностите в искането не са отстранени.

Искането няма да бъде разгледано по същество, поради факта, че не съдържа изискуемите се от закона реквизити. С оглед дадените в чл.10, ал.1, т.1 от Закона за защита на личните данни /ЗЗЛД/ правомощия на Комисията, за осъществяване на цялостен контрол за спазване на нормативните актове в областта на личните данни, Комисията счита, че следва да укаже на Д.Й. правните възможности дадени й по ЗЗЛД.

Текстът на чл. 4, ал. 1 от ЗЗЛД изрично урежда хипотезите, при наличието на които се допуска обработването на лични данни. Обработването на лични данни е допустимо само в случаите, когато е налице поне едно от следните условия:

1. обработването е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни;

2. физическото лице, за което се отнасят данните, е дало изрично своето съгласие;

3. обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по негово искане;

4. обработването е необходимо, за да се защитят животът и здравето на физическото лице, за което се отнасят данните;

5. обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес;

6. обработването е необходимо за упражняване на правомощия, предоставени със закон на администратора или на трето лице, на което се разкриват данните;

7. обработването е необходимо за реализиране на законните интереси на администратора на лични данни или на трето лице, на което се разкриват данните, освен когато пред тези интереси преимущество имат интересите на физическото лице, за което се отнасят данните.

Всеки един администратор на лични данни следва да обработва личните данни на г-жа Й. при спазване на разпоредбата на чл. 2, ал. 2 от Закона за защита на личните данни: законосъобразно и добросъвестно (чл.2, ал.2, т. 1 ЗЗЛД); да ги събира за конкретни, точно определени и законни цели и да не се обработват допълнително по начин несъвместим с целите (чл.2, ал.2, т. 2 ЗЗЛД); да бъдат съотносими, свързани с и ненадхвърлящи целите, за които се обработват (чл.2, ал.2, т. 3 ЗЗЛД); не на последно място те трябва да се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват (чл.2, ал.2, т. 5 ЗЗЛД).

В чл.28а от ЗЗЛД е предвидено, че всяко физическо лице има право по всяко време да поиска от администратора да:

1. заличи, коригира или блокира негови лични данни, обработването на които не отговаря на изискванията на този закон;

2. уведоми третите лица, на които са били разкрити личните му данни, за всяко заличаване, коригиране или блокиране, извършено в съответствие с т. 1, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

На свое заседание, проведено на 17.03.2010 год. (Протокол № 9), Комисията прие разглежданото искане за недопустимо.

С оглед на изложеното и на основание чл.10, ал.1, т.1 от ЗЗЛД, във връзка с чл.30, ал.3 от

Правилника за дейността на Комисията за защита на личните данни и нейната администрация, Комисията

РЕШИ:

Оставя без разглеждане искане с вх. № е-В-80/13.01.2009 г. от Д.С.Й. като недопустимо и прекратява административното производство.

Решението да се съобщи на заинтересованата страна по реда на АПК.

Настоящето решение подлежи на обжалване, в 14-дневен срок от връчването му, чрез Комисията за защита на личните данни пред Върховен административен съд на Република България.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
№ 5686/17.03.2010 г.

Комисията за защита на личните данни /КЗЛД/ в състав: Венета Шопова, Красимир Д., Валентин Енев, Мария Матева и Веселин Целков на открито заседание, проведено на 17.03.2010 г., на основание чл. 10 ал. 1 т. 7 от Закона за защита на личните данни /ЗЗЛД/ и във връзка с изискването на чл. 27, ал. 2 от АПК към административните органи за проверка на предпоставките за допустимост на искането, разгледа по допустимост жалба с вх. № 5686/01.03.2010 г. от Е.Н. от гр. С. срещу Д.Д. от гр. С.

Е.Н. сезира КЗЛД с жалба, в която протестира срещу неправомерното обработване на личните й данни от страна на Д.Д., като за целта излага следните факти:

На 18.02.2010 г. в качеството си на физическо лице ответникът по жалбата поставя в пощенските кутии на живущите в неговия и този на жалбоподателката и съседен вход извадка от писмен отговор на Е.Н. до СРС във връзка с гр.д. № 35277/2009 по описа на СРС, 37-ми състав. Към извадката от него Д.Д. е добавил и свой коментар във връзка с предмета на съдебния спор. Листове с тази информация били залепени във фоайетата и на двата входа. Съдебният спор между страните се води в качеството им на председател и управител на ЖСК "А." по повод установяване истинността на протокол от проведено Общо събрание на кооператорите на ЖСК "А.".

В така разпространената информация фигурират трите имена и ЕГН на жалбоподателката.

Е.Н. счита, че с действията си Д.Д. освен че цели нейното злепоставяне, но и нарушава разпоредбите на ЗЗЛД, като разпространява без нейно съгласие нейни лични данни.

В жалбата си г-жа Н. настоява ответникът Д.Д. да бъде санкциониран по реда на гл. VIII от ЗЗЛД, както и да бъдат допуснати двама свидетели за установяване истинността на нейните твърдения.

Към жалбата се прилагат листа с изнесената от Д.Д. информация, както и Отговор от жалбоподателката от 08.10.2009 г. по гр.д. № 35277/2009 г. по описа на СРС 27-ми състав в неговата цялост.

Жалбата се явява процесуално недопустима по следните съображения:

В чл. 27, ал. 2, т. 6 от АПК законодателят обвързва преценката на допустимостта на искането с наличие на специални изисквания, установени със закон. Приложимостта на Закона за защита на личните данни е свързана със защита на физическите лица във връзка с обработването на техните лични данни от лица, имащи качество на администратори на лични данни по смисъла на легалната дефиниция на чл. 3. Тоест, това изискване се явява абсолютна процесуална предпоставка, с оглед на която следва да се прецени допустимостта на жалбата. В конкретния случай, жалбата е насочена

срещу физическо лице, което не е администратор на лични данни по смисъла на закона, поради което комисията не може да упражни правата си по чл. 10, ал. 1 т. 7 от ЗЗЛД, съгласно който комисията разглежда жалби срещу актове и действия на администратори на лични данни, с които се нарушават правата на физическите лица по този закон, както и жалби на трети лица във връзка с правата им по този закон.

С оглед гореизложеното, поради невъзможността да се конституира ответна страна- администратор на лични данни по смисъла на чл. 3 от ЗЗЛД и в съответствие с чл. 27, ал. 2, т. 6 от АПК, на основание с чл. 10, ал. 1, т. 7 от ЗЗЛД, Комисията

РЕШИ :

Прекратява административното производство по жалба с рег. № 5686/01.03.2010 г. от Е.Н. от гр. С. срещу Д.Д.

Решението на Комисията може да се обжалва пред Върховния административен съд в 14-дневен срок от получаването му.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
№12/24.03.2010 г.

Комисията за защита на личните данни в състав: Председател: Венета Шопова и членове Валентин Енев, Мария Матева и Веселин Целков на заседание, проведено на 24.03.2010 г. /Протокол №10/ разгледа жалба вх.№ Ж-12/28.01.2010 г. от И.К.И. срещу "Евроком Кабел мениджмънт България" ЕООД.

На основание чл.25, ал.1 от Административно-процесуалния кодекс /АПК/ във връзка с чл.38, ал.1 от Закона за защита на личните данни /ЗЗЛД/ е образувано административно производство.

Жалба рег.№ Ж-12/28.01.2010г. е подадена от И.К.И. чрез адв. Бистра Спасова срещу "Евроком Кабел Мениджмънт България" ЕООД.

Жалбата, с която е сезирана Комисията е адресирана до "Евроком Кабел Мениджмънт България" ЕООД, Комисия за защита на потребителите и "ЕОС Матрикс" ООД.

В жалбата е описано, че имало сключен договор между "Евроком Кабел мениджмънт България" ЕООД и жалбоподателката, за предоставяне на услуга-кабелна телевизия. Жалбоподателката е отправила покана на 12.04.2009г. до фирмата, като я е уведомила, че сключения между тях договор е прекратен, считано от 20.04.2009г.

На 08.01.2010г. с адвокат Спасова се е свързал служител от "ЕОС Материкс" ООД, който я е уведомил, че дружеството е натоварено да събира вземания на Евроком кабел. Адвокат Спасова била информирана, че клиентката й И.И. дължи сума за цифрова телевизия за периода 01.02.2009г. до 31.04.2009г. в размер на 95.70 лв. В жалбата се сочи, че разпространяването на личните данни на доверителката й от страна на Евроком кабел на трето лице, което в случая се явява "ЕОС Матрикс" ООД, без нейното съгласие е извършено в противоречие на чл.4, ал.1 от Закона за защита на личните данни. Твърди се, че не е налице, нито едно от условията визирани в чл.4 от ЗЗЛД, за допустимост на обработване на личните данни на жалбоподателката.

С жалбата се иска КЗЛД да установи, че "Евроком Кабел Мениджмънт България" ЕООД е предоставил личните данни на И.И. без нейно съгласие на трето лице, което е в нарушение на ЗЗЛД.

Към жалбата, като доказателства са приложени следните документи: покана от И.И. до "Евроком Кабел" ЕАД от 12.04.2009г.; преводно нареждане от 27.11.2007г.; вносна бележка към банкова сметка от 29.11.2009г. и преводно нареждане /без дата/.

В чл.30 от Правилника за дейността на Комисия за защита на личните данни и на нейната администрация /ПДКЗЛДНА/ са посочени реквизитите, които трябва да съдържа искането оправено до Комисията за защита на личните данни. Формата на искането за откриване на административно производство е определена и в чл.29, ал.2 от Административно-процесуалния кодекс. Писменото искане трябва да съдържа пълното име и адреса на лицето, от което изхожда, естеството на искането дата и подпис.

При извършената проверка на редовността на жалбата се установи, че същата не е подписана. Посочено е, че жалбата е подадена от адв. Бистра Спасова, но към нея не е приложено пълномощно, от което да се установи по безспорен начин, че адв. Спасова е упълномощена от И.И.

Във връзка с констатираните нередности в жалбата, на основание чл.30, ал.2 от ПДКЗЛДНА са изпратени писма до адв. Спасова и до И.И., с които са уведомени, че жалбата не съдържа законово изискуемите се реквизити и приложенията към нея, съгласно чл.86, ал.1 от АПК. Уведомени са също така, че при неизпълнение на дадените указания образуваното административно производство ще бъде прекратено.

Писмото, с което адв. Спасова е уведомена за пороците, от които страда жалбата е получено от нея на 09.02.2010г., видно от известие за доставка. Срокът, в който е следвало да ги отстрани е изтекъл на 12.02.2010г.

Писмото, с което жалбоподателката И.И. е уведомена, че жалбата не отговаря на изискванията на закона се е върнало в цялост с отбелязване от пощата, че писмото е "непотърсено". Комисията приема, че на основание чл.144 от АПК следва да се приложи разпоредбата на чл.41 от ГПК. В алинея първа от цитирания текст се вменява в задължение на страната, която отсъства повече от един месец от адреса, който е съобщила, или на който веднъж й е връчено съобщение, да уведоми за това обстоятелство органа, който е сезиран. В разпоредбата са предвидени алтернативно две хипотези и в конкретния случай е налице първата. В алинея втора е предвидено, че при не изпълнение на това задължение, всички съобщения се прилагат към преписката и се смятат за връчени.

На основание изложеното, Комисията приема, че жалбоподателката и адв. Спасова са редовно уведомени за липсата на законовите реквизити на жалбата и е спазено изискването на чл.30, ал.2 от ПДКЗЛДНА.

В законово определения срок, нередностите на жалбата не са отстранени, поради което на основание чл.30, ал.3 от ПДКЗЛДНА, жалбата е недопустима, следва да се остави без разглеждани и административното производство да се прекрати.

С оглед на изложеното и на основание чл.10, ал.1, т.1 от ЗЗЛД, във връзка с чл.30, ал.3 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация, Комисията,

РЕШИ:

Оставя без разглеждане жалба рег. №Ж-12/28.01.2001г. от И.К.И. срещу "Евроком Кабел Мениджмънт България" ЕООД.

Решението да се съобщи на заинтересованата страна по реда на АПК.

Настоящето решение подлежи на обжалване, в 14-дневен срок от връчването му, чрез Комисията за защита на личните данни пред Върховен административен съд на Република България.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
№3638/24.03.2010 г.

Комисията за защита на личните данни в състав: Председател: Венета Шопова и членове Валентин Енев, Мария Матева и Веселин Целков на заседание, проведено на 24.03.2010 г. /Протокол №10/ разгледа жалба вх.№3638/09.02.2010г. получено по електронната поща от Т.Х.Г. срещу "Юробанк И Еф Джи България" АД.

С жалбата се уведомява Комисията, че при посещение в клон на "Юробанк И Еф Джи България" АД във Велико Търново и при извършване на банкова операция – касово теглене, служител на банката е изискал да преснеме личната карта на жалбоподателя. Мотивът на служителят бил, че досието на господин Г. е непълно и според вътрешните правила на банката следва да се извърши това преснемане. Жалбоподателят категорично отказал документа му за самоличност да бъде ксерокопиран. Господин Г. иска Комисията да изрази становище по изнесения от него случай.

В чл.30 от Правилника за дейността на Комисия за защита на личните данни и на нейната администрация /ПДКЗЛДНА/ са посочени реквизитите, които трябва да съдържа искането отправено до Комисията за защита на личните данни. Формата на искането за откриване на административно производство е определена и в чл.29, ал.2 от Административно-процесуалния кодекс /АПК/. Писменото искане трябва да съдържа пълното име и адреса на лицето, от което изхожда, естеството на искането дата и подпис.

Жалбата не съдържа всички законово изискуеми реквизити – не е подписана с електронен подпис и текста й е изписан на латиница.

Изготвено е писмо до жалбоподателя изх.№3638/22.02.2010г., в което му е указано, че искането страда от пороци и на основание чл.30, ал.2 от АПК следва да ги отстрани в тридневен срок от получаване на съобщението за това. Указано му е също така, че при неизпълнение на дадените указания образуваното административно производство ще бъде прекратено. Писмото е препратено на 22.02.2010г. на посочения имейл адрес. Срокът за изпълнение на дадените указания е изтекъл на 25.02.2010г.

На 19.03.2010г. е постъпила молба по електронната поща от Т.Г. С нея той уведомява Комисията, че е закрил разплащателната сметка в "Пощенска банка" /" Юробанк И Еф Джи България" АД/ и моли жалбата му да се счита за оттеглена.

Комисия за защита на личните данни, счита молбата за оттегляне на жалбата за нередовна, тя не може да породи правни последици, поради което я оставя без уважение. В чл.56, ал.1 от АПК е предвидена правната възможност, административния орган, пред който има висящо административно производство по искане на страната, по чиято инициатива е започнало да го прекрати. В цитираната разпоредба, законодателят е възприел, че трябва да има искане. По аналогия, след като са определени реквизитите, които трябва да съдържа искането за откриване на производство, то искането, с което се оттегля жалбата следва да има същите реквизити. Молбата, с която господин Г. оттегля жалбата си не е подписана и страда от същия порок, от който страда жалбата му.

В законово определения срок, нередностите на жалбата не са отстранени, поради което на основание чл.30, ал.3 от ПДКЗЛДНА, жалбата е недопустима, следва да се остави без разглеждане и административното производство да се прекрати.

С оглед на изложеното и на основание чл.10, ал.1, т.1 от ЗЗЛД, във връзка с чл.30, ал.3 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация, Комисията

РЕШИ:

Оставя без разглеждане жалба с вх. № 3638/09.02.2010г. от Т.Х.Г. срещу "Юробанк И Еф Джи България" АД.

Решението да се съобщи на заинтересованата страна по реда на АПК.

Настоящето решение подлежи на обжалване, в 14-дневен срок от връчването му, чрез Комисията за защита на личните данни пред Върховен административен съд на Република България.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
№5540/07.04.2010 г.

Комисията за защита на личните данни в състав: Председател: Венета Шопова и членове Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков на заседание, проведено на 07.04.2010 г. /Протокол №12/ разгледа искане рег.№5540/25.02.2010г. получено по електронната поща от С.С.

На основание чл.25, ал.1 от Административно-процесуалния кодекс /АПК/ във връзка с чл.38, ал.1 от Закона за защита на личните данни /ЗЗЛД/ е образувано административно производство.

С искането от С.С. се уведомява Комисията, че има изтичане на нейни лични данни /имена, адрес, домашни и мобилни телефони/ от "Първа Инвестиционна банка" АД. В искането е посочено, че молителката е открила сметка в посочената банка и в края на 2009г. година я е закрила. Няколко лица са "захранвали" сметката, като в последствие са се възползвали, от това, че банката им е предоставила информация, по отношение на личните й данни. Тези лица са търсили контакт с молителката и със семейството й, за да си искат сумите, които са превели по сметката. Позвъняванията са били от скрити номера. С искането се информира комисията, че сметката е закрита, като се посочва намерението на госпожица С. да закрие и сметката си в ОББ. Споделя, че не се чувства защитена като дава данните си на тези институции. Иска от Комисията да има развитие по изнесения от нея случай.

В чл.38, ал.1 от Закона за защита на личните данни е определен преклузивен срок, в който физическото лице има право да сезира Комисията за защита на личните данни. В искането не е посочено, кога е извършено твърдяното от С.С. неправомерно обработване на личните й данни, за да се направи извод, че искането е подадено в срок.

Формата на искането, с което се сезира Комисията за защита на личните данни и реквизитите, които трябва да съдържа, са определени в чл.30, ал.1 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация.

Постъпилото искане не съдържа тези реквизити и от него не може да се установи подателят му, тъй като същия не е индивидуализиран с три имена. По имейла, от който е направено искането не може да индивидуализира подателя. Искането не е подписано и не може да се установи, от кого изхожда.

В изпълнение на чл.30, ал.1 и ал.2 от Административно-процесуалния кодекс са дадени указания на искателя с писмо изх.№5540/09.03.2010г., в което й е указано, че искането страда от пороци и на основание чл.30, ал.2 от АПК следва да ги отстрани в тридневен срок от получаване на съобщението за това. Указано е също така, че при неизпълнение на дадените указания образуваното административно производство ще бъде прекратено. Писмото е препратено на 10.03.2010г. на посочения в искането имейл адрес. Срокът за изпълнение на дадените указания е изтекъл на 13.03.2010г. и нередностите в искането не са отстранени.

В законово определения срок, нередностите на жалбата не са отстранени, поради което на основание чл.30, ал.3 от ПДКЗЛДНА, жалбата е недопустима, следва да се остави без разглеждани и административното производство да се прекрати.

С оглед на изложеното и на основание чл.10, ал.1, т.1 от ЗЗЛД, във връзка с чл.30, ал.3 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация, Комисията

РЕШИ:

Оставя без разглеждане искане рег. №5540/25.02.2010г. от С.С.

Решението да се съобщи на заинтересованата страна по реда на АПК.

Настоящето решение подлежи на обжалване, в 14-дневен срок от връчването му, чрез Комисията за защита на личните данни пред Върховен административен съд на Република България.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЯ ПО СИГНАЛИ

РЕШЕНИЕ
от 17.03.2010г.

Комисията за защита на личните данни (КЗЛД), в състав: председател Венета Шопова и членове : Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков, на редовно заседание, проведено на 17.03.2010 год. (Протокол № 9), разгледа молба с вх. № в-3274/05.02.2010г. от „АМДЖЕН БЪЛГАРИЯ" ЕООД, представлявано от адв. Павлин Стоянов, в качеството му на пълномощник, за получаване на разрешение за трансфер на лични данни към дружество „Кенекса Технолъджи Инк." в САЩ на основание чл. 36а, ал. 4 във връзка с чл.36а, ал. 2 от Закона за защита на личните данни (ЗЗЛД).

В писменото си искане пълномощникът на „АМДЖЕН БЪЛГАРИЯ" ЕООД се обръща с молба към КЗЛД за даване на разрешение, на основание чл. 36а, ал. 4, т.1 от ЗЗЛД, да бъдат предоставени лични данни на физически лица към дружество „Кенекса Технолъджи Инк."в САЩ.

Съгласно информацията в искането промяната на мястото на обработване на тези данни е във връзка с получаването на консултантски услуги, които ще бъдат предоставяни от Кенекса чрез продукта „Kenexa Recruiter Brass Ring". Към молбата са приложени договор за предоставяне на услуги между Амджен Инк. и Кенекса Технолъджи Инк., Общи условия за регистрация като кандидати за работа на Амджен Инк., Политика за поверителност на Амджен, Сертификат за регистрация на Кенекса към принципите на „Safe Harbour" и Вътрешни правила на Кенекса във връзка с обработването и осигурената защита на лични данни.

При анализа на изложеното в искането, както и приложените към него документи, се установи следното:

„Амджен България" ЕООД е еднолично дружество с ограничена отговорност с ЕИК 200734900, със седалище и адрес на управление гр. София общ. Столична, бул."Цар Освободител" 14, ет. 1, с предмет на дейност: търговия на едро с фармацевтични продукти; производство на фармацевтични продукти; производство на фармацевтични препарати; търговия с фармацевтични продукти в специализирани магазини; организационни дейности на изложби, панаири и конгреси; дейности по редактиране на наръчници, резюмета, адресни списъци и други подобни; други дейности от професионално, научно и техническо естество; всякакви други дейности, които не са забранени от закона.

„Амджен България" ЕООД е подал молба за освобождаване от регистрация като администратор на лични данни и тя е уважена от Комисията за защита на личните данни с решение съгласно Протокол № 31 от 21.10.1009г.

В искането за трансфер е посочено, че целта, за която ще бъдат трансферирани данните, е предоставянето от страна на Кенекса на консултантски услуги чрез продукт «Kenexa recruiter Brass-Ring». Този продукт включва получаване, обработка и сортиране на автобиографии на кандидати за работа в дружествата от групата на Амджен, вкл. Амджен България ЕООД. В тази връзка Амджен е създал и поддържа интернет страница, на която всяко физическо лице може да се регистрира като кандидат за работа в някое от дружествата от Групата на Амджен. За тази цел физическите лица ще подават чрез интернет страницата на Групата на Амджен определен тип лични данни, които включват име, адрес, телефонен номер, имейл адрес и биографична информация. Съгласно искането информация относно пол, етнос/раса може да се предоставя от лицата само по тяхно желание и ако това е позволено от приложимия закон. Получените лични данни Амджен ще обработва чрез програмния продукт, поддържан от Кенекса.

Съгласно Директива № 95/46/ЕО на Европейския парламент и на Съвета трансфер на лични данни в трети страни може да бъде осъществен, само ако въпросната трета държава предоставя адекватно ниво на защита на данните.

Предоставянето на лични данни от администратор, установен на територията на Република България към друг администратор на лични данни извън страната, се извършва по реда на Закона за защита на личните данни, като определящ критерий относно режима на трансфер на данни е държавата, в която ще бъдат предоставени данните.

Предоставяне на лични данни в трета държава се допуска само, ако тя осигурява адекватно

ниво на защита на личните данни на своя територия.

В основния (мастер) договор за предоставяне на услуги между Амджен и Кенекса Технолъджи от 30 юни 2009г. подробно са разписани услугите и дейностите, които Кенекса ще осигурява на Амджен. През месец януари 2010г. е сключено изменение номер едно към основния договор за предоставяне на услуги, което е насочено към защитата на лични данни. Включен е раздел с наименование „Поверителна и лична информация". Съгласно разпоредбите на договора получателят на данните Кенекса се задължава да спазва приложимото законодателство в областта на личните данни и да използва получените лични данни само за целта на осъществяването на услугите по договора. В качеството си на обработващ личните данни Кенекса се задължава да използва разумни технологични, физически, административни и процедурни предпазни мерки, за да осигури защита на личните данни срещу непозволено ползване, достъп или разкриване, както и да защитава поверителността, цялостта и наличността на информацията, която се идентифицира като лична. В тази връзка е разписано, че Кенекса ще въведе разумни ограничения по отношение на физическия и електронния достъп до лични данни, като контрол на физическия достъп, защитени протоколи за удостоверяване на потребителя, методи за контрол върху защитения достъп, защитна стена, защита от вреден софтуер и използване на криптиране. Кенекса е длъжна да прилага процедури по оценка, мониторинг и одит, за да осигури вътрешно съответствие с предприетите предпазни мерки. Получателят на данните също така следва да провежда цялостна оценка на предпазните мерки поне веднъж годишно и при писмено искане, да предоставя доклад от тази оценка.

В общите условия за регистрация като кандидат за работа в Амджен изрично е указано на кандидатите, че те оторизират Амджен да събира, ползва и разкрива цялата информация относно тяхното ползване на сайта и цялата информация, предоставена от тях в съответствие с политиката за поверителност на дружеството. В политиката за поверителност се съобщава, че информацията, която кандидатите за работа предоставят, ще бъде достъпна и до дружества, с които Амджен е в договорни отношения. Указано е, че с ползването на сайта или услугите на Амджен, съответните потребители недвусмислено се съгласяват със събирането, съхраняването и обработването на данните в която и да е друга държава, където е възможно да бъде прехвърлена информация в хода на бизнес операциите на Амджен. Предвидено е също така, че лични данни на кандидатите за работа може да бъдат разкривана пред оператори или изпълнители на поддръжка във връзка с предоставяните от тях услуги за сайта на Амджен. Използвайки услугите на Амджен, физическите лица се съгласяват недвусмислено на подобна употреба на данните. Лицата могат да оттеглят своето съгласие за ползване на личните им данни с изпращане на електронно писмо и поискване на заличаване на потребителския акаунт.

Извършена бе служебна справка, от която се установи, че към настоящия момент получателят на данните Кенекса е включен в списъка на Safe Harbour. В последния се включват дружества, които декларират пред Департамента по търговия на САЩ, че ще се придържат към така наречената Safe Harbour рамка, създадена от Департамента по търговия в сътрудничество с Европейската комисия. Рамката съдържа насоки към дружествата, регистрирани в САЩ, за предоставяне на адекватно ниво на защита на личните данни, прехвърляни от страни – членки на Европейския съюз към тях.

Видно от Вътрешните правила на Кенекса във връзка с обработването и осигурената защита на лични данни, получателят на данните поема ангажимент да гарантира неприкосновеността и сигурността на данните за съответните физически лица, които данни дружеството поддържа и управлява от името на своя клиент-Амджен. В правилата са разгледани характеристиките на продукта на Кенекса във връзка с неприкосновеността, както и препоръчваните практики за гарантиране на безопасността на данните на физическите лица. Такива са правилата за използване на паролите, криптиране на парола, безопасност на сесията, безопасност на eLink, проверка на потребителите на системата и на конфигурацията на системата.

На основание чл. 36а, ал. 4, т. 1 от ЗЗЛД КЗЛД не извършва преценка на адекватността на нивото на защита на личните данни в трета държава в случаите, когато е необходимо изпълнение на решение на Европейската комисия, с което тя се е произнесла, че третата държава, в която се предоставят лични данни, осигурява адекватно ниво на защита.

При отчитане на решение на Европейската комисия 2000/520 относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот" и свързаните с това често задавани въпроси, публикувани от Департамента по търговия на САЩ, и на основание чл.36а, ал.4, т.1 във връзка с ал.2 от ЗЗЛД Комисията за защита на личните данни

РЕШИ:

Разрешава на администратора на лични данни „Амджен България" ЕООД да предостави лични данни на физически лица-кандидати за работа в „Амджен", касаещи тяхната физическа идентичност на дружество на територията на трета страна - „Кенекса Технолъджи Инк.", САЩ, в следния обем: име, адрес, телефонен номер, имейл адрес и биографична информация, за срока на основния договор за предоставяне на услуги между „Амджен Инк." и „Кенекса Технолъджи Инк.".

Решението на Комисията може да се обжалва пред Върховния административен съд в 14 (четиринадесет) дневен срок от получаването му.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

РЕШЕНИЕ
от 07.04.2010г.

Комисията за защита на личните данни (КЗЛД), в състав: председател Венета Шопова и членове : Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков, на редовно заседание, проведено на 07.04.2010 год. (Протокол № 12), разгледа искане с вх. № в-3289/05.02.2010г. от „Юниливър България" ЕООД, представлявано от управителя на дружеството г-н Едуард Гонгоние за получаване на разрешение на основание чл. 36а, ал. 2 и ал. 3 от Закона за защита на личните данни (ЗЗЛД) за трансфер на лични данни към дружество „АйБиЕм" в САЩ.

В писменото си искане представляващият „Юниливър България" ЕООД се обръща с молба към КЗЛД да бъде дадено разрешение на основание чл. 36а, ал. 2 и ал. 3 от ЗЗЛД да бъдат предоставени лични данни на служители, доставчици и клиенти към дружество „АйБиЕм" в САЩ.

Прехвърлянето на данните засяга регистър „Човешки ресурси". Съгласно информацията в искането, промяната на мястото на обработване на тези данни е във връзка с получаването на услуги за финансови бизнес процеси, които ще бъдат предоставяни от „АйБиЕм". В искането е посочено, че центърът на „АйБиЕм" в САЩ разполага с изградена по последни технологии система за сигурност при спазване на всички изисквания на местното и на европейското законодателство за обработка и съхранение на лични данни. Трансферът ще бъде осъществен по електронен път при спазване на всички изисквания за пълна безопасност при прехвърляне на данни в съответствие с договореностите между „АйБиЕм" и представляващите групата „Юниливър" дружества. В писмото е указано, че физическите лица са надлежно уведомени за планирания трансфер и са изразили писмено съгласие в тази връзка.

При анализа на изложеното в искането, както и приложените към него документи, се установи следното:

„Юниливър България" ЕООД е еднолично дружество с ограничена отговорност с ЕИК 121796402, със седалище и адрес на управление: гр. София 1715, ж.к. Младост 4, ул. Бизнес парк София 1, с предмет на дейност: производство, продажба, дистрибуция, маркетинг, реклама, внос и износ на непотребителски и маркови потребителски стоки от всякакъв вид; търговия на едро, посредничество и търговия на дребно на непотребителски и потребителски стоки от всякакъв вид, вкл. създаване на мрежа за дистрибуция; търговско представителство; организация на изложби и търгове и всяка друга дейност, незабранена от закона.

„Юниливър България" ЕООД е администратор на лични данни и в това си качество е подал Заявление за регистрация № 2275/28.11.2003г. В заявлението е посочено, че дружеството поддържа три регистъра: човешки ресурси; договорни отношения; промоции и рекламна дейност. Заявена е възможността за предоставяне на данни в други държави, и по-конкретно в САЩ, по отношение на данните в регистър човешки ресурси.

Има издадено Удостоверение за регистрация № 1632 за вписване в „Регистъра на администраторите на лични данни и на водените от тях регистри", воден от КЗЛД.

В искането за трансфер е посочено, че целта, за която ще бъдат трансферирани данните, е

получаването на услуги за финансови бизнес процеси, които ще бъдат предоставяни от „АйБиЕм". Твърди се също, че физическите лица, чиито данни ще бъдат предмет на трансфера, са дали своето изрично писмено съгласие личните им данни да бъдат предоставени в центъра на „АйБиЕм" в САЩ, за което е приложена като доказателство декларация - съгласие. С подписването на декларацията се предоставя възможност на всяко едно лице самостоятелно, писмено и изрично да заяви, че е запознато с предстоящия трансфер и е съгласно личните му данни да бъдат предоставени на държава извън Европейското икономическо пространство, като същите бъдат обработвани в тази държава при спазване на условията, поставени от Юниливър.

Съгласно Директива № 95/46/ЕО на Европейския парламент и на Съвета трансфер на лични данни в трети страни може да бъде осъществен, само ако въпросната трета държава предоставя адекватно ниво на защита на данните.

Предоставянето на лични данни от администратор, установен на територията на Република България към друг администратор на лични данни извън страната, се извършва по реда на Закона за защита на личните данни, като определящ критерий относно режима на трансфер на данни е държавата, в която ще бъдат предоставени данните.

Предоставяне на лични данни в трета държава се допуска само, ако тя осигурява адекватно ниво на защита на личните данни на своя територия. Извършена бе служебна справка, от която се установи, че към настоящия момент получателят на данните „АйБиЕм" не е включен в списъка на Сейф Харбар (Safe Harbour). В последния се включват дружества, които декларират пред Департамента по търговия на САЩ, че ще се придържат към така наречената Сейф Харбар рамка, създадена от Департамента по търговия в сътрудничество с Европейската комисия. Рамката Сейф Харбар съдържа насоки към дружествата, регистрирани в САЩ, за предоставяне на адекватно ниво на защита на личните данни, прехвърляни от страни – членки на Европейския съюз към тях.

Към преписката е приложен Рамков договор, сключен между „ЮНИЛИВЪР ПЛС" дружество, учредено във Великобритания, „ЮНИЛИВЪР НВ" дружество, учредено в Нидерландия, и „АйБиЕм Глобъл Сървисиз", звено на „АйБиЕм КОРПОРЕЙШЪН". „ЮНИЛИВЪР" сключва договора като представител за и от името на всяко едно от дружествата на „ЮНИЛИВЪР ГРУП", като всяко едно от тях е обвързано с условията на договора. Всеки договор за обработка на данни обаче се счита за отделен договор между съответното дружество на „ЮНИЛИВЪР ГРУП" и вносителя на данни, като задълженията на дружествата са обвързващи за всяко едно от тях поотделно.

Цел на трансфера, съгласно договора, е осъществяването на дейности, свързани с финансови транзакции. За тази цел „ЮНИЛИВЪР" ще предоставя на „АйБиЕм", в качеството му на администратор на лични данни, данни от категорията физическа и икономическа идентичност, както следва:

- на свои служители - лични имена, информация относно служебни финансови разходи, извършени от служителя, като билети за транспорт, фактури от ресторант, електронни адреси;
- на доставчици – имена, адрес, информация относно обслужваща банка, номер на сметки, телефонни номера;
- на клиенти- имена, адрес, информация относно обслужваща банка, номер на сметка, история на плащането, клиентски номер, телефонни номера.

Като приложение към договора са включени стандартни договорни клаузи съобразно Решение на Комисията 2001/497/ЕО от 15 юни 2001г. относно общите договорни клаузи за трансфера на лични данни към трети страни съгласно Директива 95/46/ЕО. В допълнение към стандартните договорни клаузи са включени разпоредби относно техническите и организационните мерки за сигурност, които вносителят на данните ще прилага. Подробно са разписани правилата за физическа сигурност, средствата за обезпечаване на сигурността, както и организационната схема за сигурността на IT-системите. В тази връзка с договора са указани използваните програми за обезпечаване на съответната сигурност, както и периодичността на провеждане на проверките за сигурност.

Страните са се договорили, че след прекратяване на предоставянето на услуги по обработването на лични данни, вносителят на данните, в зависимост от избора на износителя на данните, връща всички предадени лични данни, както и копията от тях, или унищожава тези данни, като предоставя на износителя надлежни доказателства за това.

трансфер на данни на свое заседание от 10.03.2010г. и реши, че преди произнасянето по

същество по искането е необходимо следното:

- „Юниливър България" ЕООД да представи сключения договор за предоставяне на услуги за финансови бизнес процеси между „Юниливър" и получателя на данните в САЩ в частта, касаеща целта на прехвърлянето на данните и обема от данни-предмет на трансфер;

- декларацията за изразяване на съгласие на физическите лица, чиито данни ще бъдат трансферирани, да бъде конкретизирана, като в образеца на декларация бъде отразен получателят на данните и държавата, в която се намира той.

В изпълнение на указанията на Комисията, с писмо рег. № 3289/26.03.2010г., представляващият „Юниливър България" ЕООД представя новия образец на декларация за изразяване на съгласие за извършването на съответния трансфер. В декларацията са указани изрично получателят на данните и държавата, в която ще бъде осъществен трансферът на данни.

Договорът за финансови бизнес процеси в частта, имаща отношение към разрешаването на трансфера на данни, не е представен. В писмото си управителят на дружеството изтъква като причини за непредоставянето му обстоятелството, че по съображения за сигурност и конфиденциалност, достъпът до този рамков договор е ограничен и той се съхранява в централата на „Юниливър" в Холандия. В тази връзка дружеството изтъква като аргументи в полза на разрешаването на трансфера на данни използването на стандартни договорни клаузи в договора.

На основание чл. 36а, ал. 4, т. 2 от ЗЗЛД КЗЛД не извършва преценка по ал. 3 в случаите, когато е необходимо изпълнение на решение на Европейската комисия, с което тя се е произнесла, че определени стандартни договорни клаузи осигуряват адекватно ниво на защита. В допълнение към това, видно от преписката, лицата, чиито данни ще са предмет на трансфер, дават изрично своето писмено съгласие за осъществяването на трансфера.

След запознаване със съдържанието на новия образец на декларацията за изразяване на съгласие за извършване на трансфер на данни, при зачитане на съображенията за конфиденциалност на сключения договор за предоставяне на услуги за финансови бизнес процеси и предвид факта, че за извършване на трансфера се използват стандартни договорни клаузи съгласно решение на Комисията 2001/497/ЕО от 15 юни 2001г. относно общите договорни клаузи за трансфера на лични данни към трети страни съгласно Директива 95/46/ЕО и на основание чл.36а, ал.4, т.2 във връзка с ал.2 от ЗЗЛД Комисията за защита на личните данни

РЕШИ:

Разрешава на администратора на лични данни „Юниливър България" ЕООД да предостави лични данни на физически лица (служители на дружеството, доставчици и клиенти), касаещи тяхната физическа и икономическа идентичност, за срока на договора за предоставяне на услуги за финансови бизнес процеси, сключен между дружествата на „Юниливър" и „АйБиЕм Глобъл Сървисиз" в САЩ, както следва:

- на служители на „Юниливър" - лични имена, информация относно служебни финансови разходи, извършени от служителя, като билети за транспорт, фактури от ресторант, електронни адреси;

- на доставчици – имена, адрес, информация относно обслужваща банка, номер на сметки, телефонни номера;

- на клиенти- имена, адрес, информация относно обслужваща банка, номер на сметка, история на плащането, клиентски номер, телефонни номера.

Решението на Комисията може да се обжалва пред Върховния административен съд в 14 (четиринадесет) дневен срок от получаването му.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/
Мария Матева /п/
Веселин Целков /п/

СТАНОВИЩА НА КЗЛД

СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ОТНОСНО: *Събиране и обработване на PNR/API данни от Британската митническа агенция във връзка с въвеждането на системата "Електронни граници" (e-borders).*

Комисията за защита на личните данни (КЗЛД), в състав: Венета Шопова, Красимир Димитров и Валентин Енев, на редовно заседание, проведено на 10.03.2010 год. (Протокол № 8), разгледа писмо с рег .№ 4880/16.02.2010г. от заместник-министъра на вътрешните работи Веселин Вучков, с което се обръща към Комисията за защита на личните данни (КЗЛД) за становище относно събирането и обработването на PNR/API данни от британската митническа агенция във връзка с въвеждането на системата "Електронни граници" (e-borders).

I. Фактическа обстановка

В Комисията за защита на личните данни е получено писмо с рег. № 4880/16.02.2010г. от заместник-министъра на вътрешните работи Веселин Вучков, към което е приложен нон-пейпър от Посолството на Великобритания в Република България. Отправена е молба за становище от националния надзорен орган за защита на данните във връзка със събирането и обработването на лични данни (PNR/API данни) от британската митническа агенция във връзка с въвеждането на системата "Електронни граници" (e-borders)). Касае се за национална британска програма, по линия на която митническата агенция изисква събирането на предварителни данни за пътниците (API данни) от вътрешни за общността полети, в т.ч. по въздух, суша и море, с цел борба с организираната престъпност, тероризма и нарушенията на имиграционния режим. В тази връзка и предвид острите реакции на някои европейски държави е обменена кореспондения между Великобритания и Европейската комисия за изясняване на законосъобразността на изискванията на британското законодателство за събиране на данни от държавата на тръгването.

Европейската комисия е изразила становище, че програмата „Електронни граници" не е в нарушение на Директива 95/46 на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни и на Директива 2004/38/ЕО от 29 април 2004 година относно правото на граждани на Съюза и на членове на техните семейства да се движат и да пребивават свободно на територията на държавите–членки. За целта обаче, Комисията е указала необходимостта британската страна да предприеме и въведе конкретни мерки и гаранции за защита на правата на лицата, както следва:

- на пътниците, които са граждани на съюза или членовете на техните семейства, да не се отказва влизане/излизане на територията на Великобритания или да не им се налагат санкции на основание на това, че данни за тях не са били предоставени на властите, независимо от причините;
- да не се налагат санкции на превозвачите за непредоставяне на информация по причини, които не се дължат на тях;
- британските власти да инструктират съответните превозвачи, че те не следва да отказват качването на пътници, независимо от тяхната националност, които не са предоставили API данни, както и че предоставянето на API данни не е задължително, нито е условие за закупуването или продажбата на билети;
-британските власти да осигуряват на пътниците от и до Обединеното Кралство информацията, изисквана от чл.10 от директива 95/46 (информация, която физическото лице следва да получи), както и да съдействат на превозвачите да предоставят тази информация на пътниците;
- да бъде създадена една точка за контакт с цел даване на възможност на лицата да упражняват своите права;
- при трансфери на данни в трети страни да се прилагат подходящи мерки за защита в съответствие с изискванията на органа по защита на данните на Обединеното Кралство;

- срокът за задържане на данните да бъде намален от 10 години, за да не се различава съществено от сроковете, предвидени в директива 2004/82/ЕО.

В заключение, Комисията отбелязва, че правното основание за събирането на предварителни данни за пътниците трябва да се търси в законодателството на съответната държава, в която се извършва обработването на данните. Надзорният орган на държавата, в която се обработват данните, следва да изрази становище относно това дали признава наличието на обществен интерес, преследван от третото лице, което иска да му бъдат разкрити данните. Такъв обществен интерес може да бъде признат, например, на основата на сътрудничество в борбата с нелегалната имиграция или с митническите нарушения. Такава преценка не може да бъде направена от превозвачите. Това на практика означава националният орган по защитата на данните в държавата, където е седалището на превозвача, формално да одобри трансфера на данни от тази държава-членка към Великобритания.

В тази връзка британската страна е отправила молба Комисията за защита на личните данни да се произнесе, че е налице правно основание за предаването на Великобритания на предварителни данни за пътниците (API). В своя нон-пейпър Посолството на Великобритания изказва следните разбирания:

- Великобритания силно поддържа френската инициатива за бързо постигане на споразумение и приемане на европейски акт за резервационните данни на пътниците (PNR), за да се осигури ясна правна база за събирането и обработването на данни за пътниците, като споразумението да съдържа възможност за обработване на данни от вътрешните за ЕС полети;

- Британската страна вярва, че възможността да се събират и обработват PNR-данни от вътрешните полети е особено важна за подобряване на сигурността в рамките на ЕС, още повече, че вътрешните за ЕС маршрути са идентифицирани като едни от най-рисковите за нелегална имиграция, контрабанда и друга престъпна дейност.

II. Правен анализ

Правното основание за искането на британската страна на данни за пътниците е закон №5 от 2008 г. и заповед на имиграционните власти и полицията относно предоставянето на информация за пътниците, екипажа и услугите, като се уточнява какви данни, свързани с пътуването, могат да бъдат изисквани от имиграционните власти или полицейските служители от корабите, въздухоплавателните средства и влаковете, които влизат или напускат Великобритания. Тези данни са разделени в две групи –задължителни данни, които трябва да бъдат събрани и предоставени при поискване и допълнителни данни, които трябва да бъдат предоставени само в обем, известен на превозвача.

Задължителните данни включват следната информация:

- за пътниците и екипажа - информация, свързана с документите за пътуването, съдържаща се в частта на документите за самоличност, която се сканира при проверка. Това е т.нар. API информация или предварителна информация за пътниците;

- информация за въздухоплавателната услуга, като номер на полет, името на превозвача, местата на излитане и кацане.

Допълнителните данни включват друга информация за пътника, каквато са PNR данните. Тези данни са имената на пътника, адрес, телефонен номер, информация за билета и маршрута на пътуването.

По отношение правната уредба на събирането на данни за пътниците на европейско равнище, то това е Директива 2004/82/ЕО на Съвета относно задължението на превозвачите да съобщават данни на пътниците. Директивата изисква от държавите-членки да предприемат необходимото, за да задължат превозвачите (само превозвачи на пътници по въздушен път) да предават при поискване на органите, извършващи контрола на лицата по външните граници, преди края на регистрацията, данните за пътниците, които предстои да превозят към граничния пункт, през който тези лица ще влязат на територията на дадена държава-членка. В директивата изчерпателно и лимитативно е посочен видът на сведенията, които превозвачите са длъжни да предоставят на съответните гранични власти. Тези задължения по никакъв начин не се отразяват на задълженията на превозвачите, произтичащи

от чл.26 от Конвенцията за прилагане на споразумението от Шенген. Целта на предаването на тези данни за пътниците е уредено в директивата, а именно : улесняване извършването на проверките и водене на по-ефикасна борба с незаконната имиграция. Органите, извършващи проверките на лицата по външните граници, съхраняват тези данни във временен архив. Разписано е задължение за заличаване на данните в срок до 24 часа след предаването им, като е допусната възможност те да се съхраняват и за по-дълъг срок, ако това е необходимо за упражняване на правомощията на граничните контролни органи съгласно националното законодателство. Задължение за заличаване на данните на пътниците в срок от 24 часа след пристигане на транспортното средство имат и самите превозвачи. Директивата допуска използването на данните и за нуждите на органите на реда.

В България Директива на Съвета 2004/82/ЕО от 29 април 2004 относно задължението на превозвачите да предават данни за пътниците е въведена в Закона за чужденците в Република България, като тази информация се използва за нуждите на подобряването на граничния контрол и борбата с нелегалната миграция (чл. 20а от ЗЧРБ). Данните, които се събират в тази връзка са следните:

1. вид и номер на документа за пътуване на пътника;
2. имена, дата на раждане и гражданство на пътника;
3. граничен контролно-пропускателен пункт на влизане в страната;
4. код на транспорта;
5. дата и час на тръгване и пристигане на транспортното средство;
6. общ брой на превозваните пътници за конкретното пътуване;
7. начален пункт на тръгване.

Обработването на посочените категории лични данни следва да става при спазване на Закона за защита на личните данни и на международните договори, по които Република България е страна. Посоченото задължение за предоставяне на данни за пътниците превозвачите имат само в случаите на превозване по въздух на пътници до Република България. Друг нормативен акт, в който се регламентира задължението за събиране на данни, е Наредба № 38 от 31.10.2003г. за общите правила за въвеждане и използване на компютъризирани системи за резервация (CCP). Съгласно чл 18, ал.2 от наредбата данните за резервационните операции включват полетните номера, кодовете на резервационните заявки, датата на пътуване, времената за заминаване и пристигане, статуса на сегментите, имената и инициалите на пътниците с техните адреси за контакт и/или телефонни номера, както и статуса на билета.

Към настоящия момент липсва унифицирана правна уредба относно съдържанието на понятията PNR и API данни. Изброяване на категориите информация, които попадат в приложното поле на тези определения, се съдържат в двустранните споразумения на ЕС с Канада, САЩ и Австралия, но липсва единен термин на европейско ниво в тази връзка. Директива 2004/82 говори за "данните за пътниците", като изчерпателно разписва категориите данни, по отношение на които превозвачите имат задължения за предоставяне на съответните власти. В този смисъл директивата е единственият акт на ниво ЕС, който въвежда определени задължения във връзка с предоставянето на данните за пътниците.

С оглед на гореизложеното и на основание чл. 10, ал.1, т.4 от ЗЗЛД Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. Комисията за защита на личните данни одобрява събирането и обработката на данни на пътниците за нуждите на подобряването на граничния контрол и борбата с нелегалната миграция. Видът на събираните данни за пътниците трябва да бъде в съответствие с категориите данни, предвидени в чл. 3, ал. 2 на Директива на Съвета 2004/82/ЕО от 29 април 2004 г. относно задължението на превозвачите да предават данни за пътниците. Няма правно основание въздушните превозвачи, регистрирани по българското законодателство, да събират и предоставят данни в обем, по-голям от предвидения в Директива на Съвета 2004/82/ЕО.

2. В българското законодателство липсва изрична правна норма, която да признава обществения интерес при предоставянето на API данни на компетентни органи в други страни, както и липсва правна норма относно признаването като правно основание за събиране и трансфер на данни към друга страна-членка, упражняването на правомощия на орган от държава-членка.

3. По отношение на инициативата за създаване на отделен правен инструмент за резервационните данни на пътниците на ниво Европейски съюз, Комисията за защита на личните данни счита, че такъв не е необходим. На европейско ниво, информация, необходима за нуждите на правораздавателната и правоприлагащата система, както и за борбата с тежките престъпления и тероризма, може да бъде събирана от множество информационни системи като тази на Европол, Шенген, митническата, Евродак и др. Всички тези системи дават възможност в зависимост от конкретния случай да бъде събиран голям обем от лични данни, поради което не е необходимо създаване на специална информационна PNR система.

ПРЕДСЕДАТЕЛ:
Венета Шопова /п/

ЧЛЕНОВЕ:
Красимир Димитров /п/
Валентин Енев /п/

СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ОТНОСНО: *Искане за становище с вх.№ 6636/13.04.2010г. от инж. Иван Димитров-Директор и Председател на Комисията за защита на личните данни в Министерството на вътрешните работи (МВР) във връзка с разработването и внедряването на технология за проверка през интернет за вече издаден български личен документ и съответствието й със Закона за защита на личните данни (ЗЗЛД).*

Комисията за защита на личните данни (КЗЛД), в състав: председател: Венета Шопова, и членове: Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков, разгледа искане за становище е вх. рег. № 6636/13.04.2010 г. от инж. Иван Димитров - Директор и Председател на Комисията за защита на личните данни в Министерството на вътрешните работи (МВР) във връзка е разработването и внедряването на технология за проверка през интернет за вече издаден български личен документ и съответствието й със ЗЗЛД .

Фактическа обстановка:

Получено е искане за становище с вх. рег. № 6636/13.04.2010 г. от инж. Иван Димитров - Директор и Председател на Комисията за защита на личните данни в Министерството на вътрешните работи (МВР) във връзка с разработването и внедряването на технология за проверка през интернет за вече издаден български личен документ. Посочено е, че технологията е разработена във връзка с въвеждането на новата автоматизирана система за български лични документи. Предвижда се гражданин, който е подал заявление за издаване на нов личен документ, да има възможност да провери дали същият е вече издаден от съответната структура на МВР. Това ще се осъществи, като се даде възможност на съответното заинтересовано лице да въведе в специално приложение данни за: ЕГН и вида на личния документ. Информацията, която ще бъде предоставена от страна на МВР, ще съдържа датата на издаване на документа и указания за срока и място на получаването му. С писмото се иска становище, относно това, дали внедряването на новата технология е в съответствие със ЗЗЛД.

Правен анализ:

Информационната дейност в МВР се ръководи от Министъра на вътрешните работи. Съгласно чл. 163, ал. 1 от Закона за министерството на вътрешните работи (ЗМВР) администратор на лични данни по смисъла на Закона за защита на личните данни е министърът на вътрешните работи, който възлага обработката на лични данни на определени от него длъжностни лица. В изпълнение на чл. 17 от ЗЗЛД администраторът на лични данни може да започне обработване на данни след подаване на заявление за регистрация. Същият е подал заявление и е регистриран в Регистъра на администраторите на лични данни и водените от тях регистри при КЗЛД, като е заявил поддържането на 22 броя регистри, един от които е регистър на българските документи за самоличност.

Разработването и внедряването на технологията за проверка през интернет на издаден български личен документ се прави с цел да бъдат улеснени гражданите в процеса на подновяване на документите за самоличност. Следва да се има предвид, че за осъществяване на възложените му със закон правомощия по издаване на документи за самоличност, МВР обработва лични данни, предоставени от съответното физическо лице, от момента на подаване на заявлението за нов личен документ. Към момента на извършване на справка чрез интернет с цел проверка дали заявеният документ е издаден, предоставеното ЕГН вече се обработва в информационните масиви на МВР. Получаването на информация за финализиране на процеса по издаване на съответен документ за самоличност, е част от процедурата по неговото издаване. Услугата, чрез тази технология, представлява за гражданите една възможност за извършване на справка. Изборът дали ще се възползват от този начин за проверка е предоставен изцяло в преценка на съответното физическо лице. От изложеното в писмото става ясно, че физическите лица ще въвеждат самостоятелно и доброволно съответните данни (ЕГН и вид на документа) с цел да получат насрещна услуга (информация относно датата на издаване на документа за самоличност и указания за срока и мястото на получаването му).

С факта на подаване на заявление за издаване на документ за самоличност физическото лице е изразило своето съгласие за обработване на личните му данни. Чрез вписване на информацията за ЕГН и вид на документ за самоличност, съответното лице демонстрира по безпорен и недвусмислен начин волята си да получи информация от системата на МВР относно неговото издаване.

“Обработване на личните данни”, съгласно легалната дефиниция, посочена в § 1, т.1 от Допълнителните разпоредби на ЗЗЛД, е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване. Получаването на данни от физическите лица, както и тяхното ползване от страна на МВР, с цел предоставяне на определена информация (услуга), съставляват действия по обработване на лични данни.

По отношение законосъобразните условия, при които се допуска обработването на лични данни, се прилагат разпоредбите на чл. 4 от ЗЗЛД, според който обработването на лични данни се допуска, когато е налице поне едно от изчерпателно изброените и дадени алтернативно в закона условия за допустимост, а именно:

1. обработването е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни;
2. физическото лице, за което се отнасят данните, е дало изрично своето съгласие;
3. обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по негово искане;
4. обработването е необходимо, за да се защитят животът и здравето на физическото

лице, за което се отнасят данните;

5. бработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес;

6. обработването е необходимо за упражняване на правомощия, предоставени със закон на администратора или на трето лице, на което се разкриват данните;

7. обработването е необходимо за реализиране на законните интереси на администратора на лични данни или на трето лице, на което се разкриват данните, освен когато пред тези интереси преимущество имат интересите на физическото лице, за което се отнасят данните.

Технологията за извършване на справки за издаден документ за самоличност през интернет следва да отговаря на всички нормативни изисквания по отношение на предприетите технически и организационни мерки за защита на данните. Администраторът следва да осигури технически системата по начин, който да гарантира, че при извършването на справки, чрез отдалечен достъп, се предоставя информация единствено по отношение на издаването на личен документ, съответстващ на въведеното в системата ЕГН.

С оглед гореизложеното, в конкретния случай са налице две кумулативно дадени условия за допустимост на обработване на лични данни, а именно: физическото лице, за което се отнасят данните, е дало изрично своето съгласие (чл. 4, ал. 1, т. 2 от ЗЗЛД) и/или обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна (чл. 4, ал. 1, т. 3 от ЗЗЛД).

Предвид наличието на предпоставки за допустимост на обработването на лични данни и предприетите от страна на администратора технически и организационни мерки за защита на данните, така създадената технология и нейното въвеждане в експлоатация са в съответствие със Закона за защита на личните данни.

С оглед на гореизложеното и на основание чл. 10, ал. 1 т. 4 от ЗЗЛД Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

Законосъобразното обработване на лични данни от страна на администратора на лични данни се осъществява при наличие на условие за допустимост, съобразно разпоредбата на чл. 4, ал. 1 от ЗЗЛД и при спазване на принципите, съгласно чл. 2, ал. 2 от ЗЗЛД. В конкретния случай, за извършване на справка чрез интернет относно издаването на документ за самоличност, както и относно мястото и срока за неговото получаване, са налице две кумулативно дадени условия за допустимост на обработване на лични данни, а именно: физическото лице, за което се отнасят данните, е дало изрично своето съгласие (чл. 4, ал. 1, т. 3 от ЗЗЛД) и/или обработването е необходимо за изпълнения на задължение по договор, по който физическото лице, за което се отнасят данните е страна (чл. 4, ал. 1, т. 3 от ЗЗЛД).

Администраторът следва да осигури технически системата по начин, който да гарантира, че при извършването на справки, чрез отдалечен достъп, се предоставя информация единствено по отношение на издаването на личен документ, съответстващ на въведеното в системата ЕГН.

Поради наличието на предпоставки за допустимост на обработването на лични данни и предприетите от страна на администратора технически и организационни мерки за защита на информацията, създадената технология и нейното въвеждане в експлоатация са в съответствие със Закона за защита на личните данни.

ПРЕДСЕДАТЕЛ: /п/
/ВЕНЕТА ШОПОВА/

ВИЕ ПИТАТЕ, НИЕ ОТГОВАРЯМЕ

Въпрос: *Има ли право управителят на етажната собственост да иска личните данни от живеещите в блока с обяснението, че по закон може да ги събира?*

Отговор: На свое редовно заседание, проведено на 24.02.2010г., Комисията за защита на личните данни прие решение, с което освобождава управителите на етажната собственост (председателите на управителните съвети) от задължение за регистрация като администратори на лични данни на основание чл. 17а, ал. 2 от Закона за защита на личните данни. С решението си Комисията указва на същите да събират в книгата на собствениците само посочените в чл. 7, ал. 2 от Закона за управление на етажната собственост (ЗУЕС) данни - трите имена на собственика, на членовете на неговото домакинство и на обитателите, както и самостоятелния обект и началната дата на обитаване.

Въпрос: *Имат ли право касиерите в търговските обекти да изискват от клиентите лична карта, когато плащането се извършва с кредитна или дебитна карта?*

Отговор: Правото на даден търговец да иска документ за самоличност на картодържатели при изпълнение на операции с платежна карта е регламентирано в чл.32 от Наредба № 3 от 16 юли 2009г. за условията и реда за изпълнение на платежни операции и за използване на платежни инструменти. Съгласно тази разпоредба търговец, при който се намира терминално устройство ПОС, чрез което се извършва плащане, може да откаже използването на платежна карта в случай на отказ от страна на държателя на картата да представи документ, потвърждаващ неговата самоличност или когато търговецът установи, че неоправомощено лице използва платежната карта. Обработването на личните данни в този случай е допустимо и законосъобразно, тъй като то е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни.

Въпрос: *Подадох молба за освобождаване от регистрация. Кога ще бъда вписан в регистъра на администраторите на лични данни, освободени от регистрация с решение на КЗЛД?*

Отговор: Преди да бъдете вписан в регистъра трябва да се обработи подадената от Вас информация. Обработването е свързано с проверка на обстоятелствата, поради които желаете да бъдете освободен, изготвяне на предложение и гласуването му от комисията. Поради големият брой молби за освобождаване, постъпили в периода януари-февруари 2010 г. ще е необходимо по-голямо технологично време за тяхното обработване. Списъкът се обновява ежеседмично на сайта на Комисията за защита на личните данни.

Комисия за защита на личните данни
Председател: Венета Шопова
Членове: Красимир Димитров
Валентин Енев
Мария Матева
Веселин Целков

Информационен бюлетин № 3 (24) / 2010 г.
Издава се съгласно чл. 10, ал. 3 от ЗЗЛД
Отговорник на броя: Надежда Борисова

Набор и печат: КЗЛД
Разпространява се в електронен вид