КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

София 1431
бул. "Акад. Иван Гешов" 15
тел.: 02/ 915 35 15
факс: 02/ 915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

**РЕШЕНИЕ**
**№ В-1370/2010г.**
**гр. София, 23.12.2010г.**

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 16.12.2010 год. (Протокол № 42), разгледа искане с рег. № В-1370/22.01.2010г. от "ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД за получаване на разрешение на основание чл. 36а, ал. 4, т.2 от Закона за защита на личните данни (ЗЗЛД) за трансфер на лични данни към мултинационалната корпоративна група "ЕЙ ТИ ЕНД ТИ ИНКОРПОРЕЙТИД"("AT&T Inc."), САЩ. Искането е подадено чрез адв. Красимир Недев Стефанов-пълномощник на управителя на "ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД. Приложено е пълномощно от Г.Н. – управител на дружеството, от което става видно, че лицето, подало искането за трансфер на данни, е упълномощено да представлява дружеството пред Комисията за защита на личните данни, във връзка с конкретното искане за трансфер.

Съгласно представената информация в искането за издаване на разрешение за трансфер на лични данни, "ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД (дружеството) е част от мултинационалната корпоративна група "ЕЙ ТИ ЕНД ТИ ИНКОРПОРЕЙТИД"("AT&T Inc."), регистрирана в САЩ. Корпоративната група реализира продукти, които включват безжични/мобилни решения, IP-базирани виртуални частни мрежови решения, пренос на глас и VOIP, хостинг решения, защитени бизнес връзки и единни комуникационни решения. Предоставянето на данни между дружествата от корпоративна група "ЕЙ ТИ ЕНД ТИ ИНКОРПОРЕЙТИД" се осъществява съгласно "Вътрешно-групов договор за прехвърляне на лични данни" от 02.07.2009г.

"ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД е вписано в Търговския регистър при Агенцията по вписванията с ЕИК130093285, със седалище и адрес на управление: гр. София, общ. Столична, район "Средец", бул. "Патриарх Евтимий" №19 А, ет. 2 и предмет на дейност: 1. представителство; 2. пласмент; 3.внос; 4. износ; 5. закупуване; 6. продажба; 7.маркетинг; 8. сервиз; 9.работа; 10. инсталиране; 11. поддръжка; 12. производство; 13. обучение; 14. изследвания и развиване; 15. връзки с обществеността в областта на оборудването за телекомуникации и услуги с добавена стойност; 16. развитие, промоция или продажба на продукти и услуги, доставяни съвместно от телекомукационни юридически лица от САЩ и България; 17. доставяне на информация, касаеща телеукомуникационни продукти и услуги; 18. осигуряване на упоменатите дейности за филиални дружества, включително лиазон- дейности с промишлени групи, правителствени институции и други телекомуникационни организации; 19. участие в други дружества, независимо дали са търговски или граждански, като партньор, акционер или държател на квота; 20. оказване на всякакви други услуги, които могат да бъдат допълващи към посочените по-горе.

Съгласно искането получателите на данните ще бъдат: Предприятията от корпоративната група и техните служители; Доставчици на аутсорснати IT услуги;

Консултанти и одитори; Доставчици на услуги във връзка с IT приложения за системи или база данни, в които се съхранява информацията; Доставчици и продавачи на услуги за човешки ресурси и администрация, както и други продавачи и доставчици на услуги за стопанските дейности. Видно от предоставената информация в молбата, трансферът на данни засяга служители, представители, крайни клиенти на клиентите, както и служители и представители на доставчиците на стоки и услуги на администратора. Предмет на трансфер ще бъдат следните категории лични данни, засягащи посочените групи физически лица: име, презиме фамилия, титла; място и дата на раждане; пол; служебен и домашен адрес; телефонен номер и сходни данни, необходими за установяване на връзка; най-близък роднина; информация за банкови сметки; националност; национален идентификационен номер; информация за ветерани/инвалидност; данни за службата, включително дата на наемане на работа, отдел, код на длъжността, идентификационен номер за отдел „Човешки ресурси"; вид и ниво на длъжността; държава на наемане; настояща заплата; информация за набирането на служители и оценки; оценка на резултатите; ръководител; група за целите на възнаграждения; показател за ръководни функции; код за местоположение на служителя; пълен/непълен работен ден; клас на служителя; стандартно работно време в часове на седмица; реален брой часове, при пълен работен ден; план за управление на заплатата; код на план за комисионни; размер на възнаграждението и разноски; IP адрес; информация, записана с гласова поща, кореспонденция по електронна поща, VoIP и други работни продукти и съобщения, създадени, съхранявани или изпратени от служителите, за които се отнасят данните, с помощта на компютърните/далекосъобщителните системи на корпоративната група; информация във връзка с пароли, достъп и други мерки за сигурност, които позволяват достъп и използване на търговските приложения, инструменти и системи; информация във връзка с кандидати за служители, като име, телефонен номер, идентификационен номер за отдел „Човешки ресурси" и електронен адрес, име и държава по месторождение на кандидата, автобиография; информация, записана от охранителни системи (видеонаблюдение); информация, необходима за спазване на законите.

Целите, за които личните данни на служители ще бъдат предоставяни, са: Изпълнение на управленски функции, за целите на управленската информация и управление на работните дейности за служителите, за които се отнасят данните; Обработка на въпроси във връзка с човешки ресурси-предоставяне и прехвърляне на персонал; ведомост; възстановяване на разходи; предоставяне на социални придобивки; дисциплинарни процедури; управление на курсове за обучение и управление на кариерата; Набиране на персонал; прекратяване на трудови правоотношения; водене на съдебни спорове; Поддържане на връзка в извънредни ситуации; спазване на законови и регулаторни изисквания; евентуални инвестиции или закупуване на част от или цялото предприятие или други активи; Други цели, във връзка с управлението на стопанската дейност и служителите.

Целите, за които личните данни на клиенти и доставчици ще бъдат предоставяни са: Въвеждане на ходове, добавки или промени по услугите или техните компоненти; Получаване и обработка на информация за уреждане на рекламации или запитвания от клиентите, във връзка със загуба на услуга или понижаване на качеството; Получаване и отговаряне на запитвания, във връзка с таксуването; Извършване на планова поддръжка, прекъсване или смущение на услугите; Въвеждане на управляеми услуги, вкл. хостинг и управление на софтуер; Диагностициране и разрешаване на проблеми във връзка с работата; Установяване, филтриране и блокиране на зловреден трафик, като вируси, извършване анализи на сигурността и разрешаване на проблеми; Подобряване на скоростта, надеждността и работата на мрежата.

При извършената служебна справка в Регистъра на администраторите на лични данни и на водените от тях регистри, поддържан от КЗЛД, се установи, че дружеството е подало заявление за регистрация с вх. № 1029203/27.01.2010г. като администратор на лични данни и е вписано в регистъра с идентификационен номер 25791. "ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД е заявило поддържането на 2 броя регистри: Регистър "Клиенти": включва лични данни относно служители, представители и крайни клиенти на Администратора (клиенти на клиенти) и Регистър "Доставчици": включва лични данни относно служители и представители на доставчиците на стоки и услуги на Администратора.

Трансферът на данни засяга информацията, поддържана в двата регистъра „Клиенти" и "Доставчици", обявени пред Комисията за защита на личните данни с вписването на дружеството като Администратор на лични данни. "ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД в качеството си на администратор събира лични данни непряко, т.е когато тези данни са предоставени от съответния клиент или доставчик със следните средства: Списъци с информация за контакти, предоставени от клиенти или доставчици; Лични данни на служители или представители на клиенти или доставчици, предоставени с подаването на искане за или предоставянето на услуги, ремонт или друго запитване, подадено от Администратора или клиента, в зависимост от конкретния случай; Разкриване на информация от клиент или доставчик, при свързване с администратора, включително документация за предоставяне на услуги; В резултат на или чрез предоставянето на услуги на клиент/доставчик на друг член на корпоративната група "ЕЙ ТИ ЕНД ТИ ИНКОРПОРЕЙТИД".

Необходимостта от трансфер на лични данни произтича от основния предмет на дейност на дружеството в рамките на корпоративната група, обхващаща голям брой отделни юридически лица (съгласно "Вътрешно-групов договор за прехвърляне на лични данни" те са 148 в повече от 60 юрисдикции.

При извършената служебна проверка е установено, че посочените в регистрите „Клиенти" и "Доставчици" лични данни съвпадат със заявените за трансфер. Предвидена е също така и възможността данните да бъдат предоставяни в държави, които са членки на Европейския съюз, както и в държави, които не са членки на Европейския съюз и на Европейското икономическо пространство.

Предоставянето на данни между дружествата от корпоративна група "ЕЙ ТИ ЕНД ТИ ИНКОРПОРЕЙТИД" се осъществява съгласно "Вътрешно-групов договор за прехвърляне на лични данни", сключен на 02.07.2009г., като са използвани общите договорни клаузи съгласно Решение на Европейската комисия № 2004/915/ЕО от 27.12.2004г. за изменение на Решение №2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни и Решение на Европейската комисия №2002/16/ЕО от 27.12.2001г. относно общите договорни клаузи за трансфера на лични данни към лицата, които ги обработват в трети страни съгласно Директива 95/46/ЕО. Страните по договора са 148-те дружества от корпоративната група, подробно описани в Приложение №3, неразделна част от цитирания договор, сред които е и "ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД.

Договорът е структуриран, както следва:

Клаузи 1-13: определят обхвата на приложение на стандартните договорни клаузи при предоставяне на данни между дружествата в корпоративната група: Определения на основните термини; Общи положения; Валидност на приложенията; Обработка от обработващи личните данни в държави с адекватна защита; Нови страни; Предимство, при

възникване на конфликт; Арбитраж; Изменения в договора; Прекратяване на договора; Уведомления по договора; Права на трети страни; Приложимо право-английските закони; Отказ от права; Прехвърляне на права; Допълнителни гаранции; Невалидност на някоя от разпоредбите на договора; Договора като цялостно споразумение между страните; Брой екземпляри.

Приложение №1: Съдържа стандартните договорни клаузи за прехвърляне на лични данни между администратори на лични данни съгласно Решение на Европейската комисия № 2004/915/ЕО от 27.12.2004г. за изменение на Решение №2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни;

Приложение №2: Регламентира стандартните договорни клаузи за прехвърляне на лични данни от администратори на лични данни към лица, обработващи данните съгласно Решение на Европейската комисия №2002/16/ЕО от 27.12.2001г. относно общите договорни клаузи за трансфера на лични данни към лицата, които ги обработват в трети страни съгласно Директива 95/46/ЕО ;

Приложение №3: Съдържа списък на страните по договора;

Приложение №4: Предоставя се възможност за прибавяне на приложение за дадена държава, където могат да се отбележат съответните изменения, специфични за тази държава;

Приложение №5: Представлява образец на договор за приобщаване, който следва да бъде сключен с нови страни по договора;

Приложение №6: В това приложение могат да бъдат записани специфични условия за дадена държава, уреждащи предоставянето на данни от държави, които не са членки на Европейското икономическо пространство.

В "Анекс Б" към Приложение № 2 от "Вътрешно-групов договор за прехвърляне на лични данни" са включени клаузи относно техническите и организационните мерки за сигурност, които се ръководят от "Главния отдел за сигурност" към корпоративната група. Неговите функционални задължения са: 1. да защитава управляваните активи и ресурси на корпоративната група от нарушения на правилата за сигурност, чрез наблюдение на евентуалните заплахи за сигурността, съпоставяне на мрежови мероприятия и осигуряване спазването на законовите и подзаконовите разпоредби за сигурност; 2. да притежава и управлява процесите за сигурност на компанията и носи крайната отговорност за всички аспекти на мрежовата и информационната сигурност; 3. осигурява спазването на политиките за сигурност и програмата за мрежова и информационна сигурност на компанията в рамките на последователна политика за целия свят за всички мрежи. Въведена е тристепенна рамка за класификация на информацията, за категоризиране на информация въз основа на чувствителността на съдържанието и конкретните законови изисквания. За всяка класификация данни е посочена маркировка за документи, с оглед установяване на начините и нивата за защита на информацията по всяка класификация. Процедурите за унищожаване и изключване на информация, която не подлежи на оповестяване, за служители на компанията за гарантиране, че електронните и хартиени носители, съдържащи поверителна информация са физически унищожени и надлежно изтрити съгласно общоприетите практики, когато данните бъдат прехвърлени на лица, извън компанията. Въведени са физически мерки за контрол на достъпа: 1. ограничаване и контрол на физическия достъп до и движение през съоръженията на компанията, чрез системи за физическо наблюдение и датчици за физическо проникване; 2. ограничаване на достъпа чрез обучена охрана и/или технически средства като автоматични системи за картов достъп и достъп с биометрични данни; 3.

периодични задълбочени проучвания на физическата сигурност и проверка на съоръженията и помещенията. Разписани са логически мерки за контрол на достъпа: всеки потребител, който изисква достъп до системите на компанията, трябва да има текуща нужда от достъп, трябва да получи уникален идентификатор и трябва да докаже, че е лицето, за което се представя. Всички потребители, които са физически лица, трябва да бъдат положително идентифицирани като уникални потребители, преди да получат достъп. Използват се няколко метода: пароли, лични идентификационни номера и идентификационни устройства. Принципът "минимални правомощия" гарантира, че всеки достъп до компютърни ресурси е ограничен само до командите, данните и системите, необходими за изпълнение на позволените дейности. Съставянето на дневници осигурява записи за всеки успешен и неуспешен опит за достъп. Всички пароли за установяване самоличността на потребителите трябва да съответстват на установени правила. Въведен е контрол на достъпа до мрежови елементи: достъпът се контролира от сървър, който валидира и проверява достъпа на потребителите, като гарантира, че се предоставя достъп само на персонала, отговорен за клиентските мрежи. Всеки достъп до устройства в помещенията за клиенти се записва, както и неуспешните опити, след което съответните акаунти се блокират. Паролите непрекъснато се променят съобразно политиката на компанията. Само персоналът има право на физически и логически достъп до съоръженията и системите. Като мярка за контрол физическият и логическият достъп се превалидира редовно през определени интервали от време. Собственикът или операторът на мрежовите елементи или на съоръженията се задължава да извърши ревалидирането на достъпа на персонала с ръководителя, за да гарантира достъпа на своите служители. Външните мрежови връзки на компанията са защитени от защитни стени, които проверяват входящия и изходящия трафик въз основа на адреса, протокола и порта на източника и местозначението, в съответствие с процедурите за сигурност. Външните връзки на клиенти и партньори до мрежите на компанията са защитени с мерки за контрол на достъпа, които проверяват входящите и изходящите пакети. Въведени са комбинация от вътрешно разработени и общодостъпни инструменти за установяване на опитите на неупълномощени лица да проникнат в световната мрежа на компанията. Тя защитава, както своите активи, така и активите на своите клиенти чрез система от процеси и технологии. Извършват се редовни тестове и оценки, за да се гарантира, че средствата за контрол се поддържат и функционират в съответствие с провежданата политика. Въведена е Програма за управление на риска, чрез която, когато бъде установена уязвимост, същата се оценява по отношение на нейната сериозност и възможен ефект за компанията и нейните клиенти. Компанията също така използва вътрешен процес за придобиване и разпространяване на Бюлетин по въпросите на сигурността в целия свят. Бюлетините са с произход организации за промишлена сигурност, доставчици на оборудване и системи. Оперативните центрове на компанията извършват денонощен контрол на сигурността в реално време, с цел разследване, реакции при събития и предприемане на действия. Извършва се одит за спазване изискванията за сигурността. Извършват се външни прегледи и сертифициране на конкретни услуги. Компанията използва процеси за управление на промените, чрез въвеждане, одобряване и докладване на промените. Корпоративната служба за планиране на непрекъснатите бизнес процеси осигурява техническите консултации и опит за програмно управление. Световната организация за сигурност поддържа вътрешен сайт за осведоменост по въпросите за сигурността, тримесечен информационен бюлетин, бюлетин за всички служители, технологични конференции, семинари и курсове по въпросите на сигурността.

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, както и към обработващ данните, 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.

На основание чл. 36а, ал. 4, т. 2 от ЗЗЛД КЗЛД не извършва преценка на адекватността на нивото на защита на личните данни в третата държава 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 конкретния случай, съгласно "Вътрешно-групов договор за прехвърляне на лични данни", в случаите, когато осъществява трансфер на данни в трета държава, се използват стандартни договорни клаузи, както следва:

1. Към администратор на лични данни - стандартните договорни клаузи за прехвърляне на лични данни съгласно Решение на Европейската комисия № 2004/915/ЕО от 27.12.2004г. за изменение на Решение №2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни;

2. Към обработващ данните –стандартните договорни клаузи съгласно Решение 2002/16 от 27 декември 2001 година относно общите договорни клаузи за трансфера на лични данни към лицата, които ги обработват, установени в трети страни съгласно Директива 95/46/ЕО. Въпреки, че това Решение е отменено, считано от 15.05.2010г. с Решение на Европейската комисия №2010/593/ЕО от 05.02.2010г. относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО, на основание чл.7 от него, договор сключен между износител на данни и вносител на данни, съгласно Решение №2002/16/ЕО преди 15.05.2010г. остава в сила и продължава да поражда последици, докато предаването и операциите по обработване на данни, остават непроменени и личните данни, обхванати от настоящото решение, продължават да бъдат предавани между страните.

Предвид факта, че за извършване на трансфера се използват стандартни договорни клаузи съгласно горепосочените решения на Европейската комисия 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 "ЕЙ ТИ ЕНД ТИ ГЛОУБЪЛ НЕТУЪРК СЪРВИСИЗ БЪЛГАРИЯ" ЕООД да предостави лични данни, относно служители, представители и крайни клиенти, както и на служители и представители на доставчиците на стоки и услуги за нуждите на корпоративна група "ЕЙ ТИ ЕНД ТИ ИНКОРПОРЕЙТИД" ("AT&T Inc."), САЩ за срока на действие на Вътрешно–групов договор за прехвърляне на лични данни , в следния обем:

- Име, презиме фамилия, титла; място и дата на раждане; пол; служебен и домашен адрес; телефонен номер и сходни данни, необходими за установяване на връзка; най-близък роднина; информация за банкови сметки; националност; национален идентификационен номер; информация за ветерани/инвалидност;

- Данни за службата, включително дата на наемане на работа, отдел, код на длъжността, идентификационен номер за отдел "Човешки ресурси"; вид и ниво на длъжността; държава на наемане; настояща заплата; информация за набирането на

служители и оценки; оценка на резултатите; ръководител; група за целите на възнагражденията; показател за ръководни функции; код за местоположение на служителя; пълен/непълен работен ден; клас на служителя; стандартно работно време в часове на седмица; реален брой часове, при пълен работен ден; план за управление на заплатата; код на план за комисионни; размер на възнаграждението и разноски;

-IP адрес;

-Информация, записана с гласова поща, кореспонденция по електронна поща, VoIP и други работни продукти и съобщения, създадени, съхранявани или изпратени от служителите, за които се отнасят данните, с помощта на компютърните/ далекосъобщителните системи на корпоративната група;

-Информация във връзка с пароли, достъп и други мерки за сигурност, които позволяват достъп и използване на търговските приложения, инструменти и системи;

-Информация във връзка с кандидати за служители, като име, телефонен номер, идентификационен номер за отдел ЧР и електронен адрес, име и държава по месторождение на кандидата, автобиография;

-Информация, записана от охранителни системи (видеонаблюдение);

-Информация, необходима за спазване на законите.

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/**