Годишник Телекомуникации 2022, том 9, с. 97-105
Yearbook Telecommunications 2022, vol. 9, p. 97-105
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.22.9.10

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ ПРЕДОСТАВЯНЕ НА ЕЛЕКТРОННИ СЪОБЩИТЕЛНИ УСЛУГИ

Алена Добрева

PERSONAL DATA PROTECTION IN THE ELECTRONIC COMMUNICATIONS SECTORS

Alena Dobreva

Резюме: Правото на защита на личните данни е част от правата, защитени съгласно Европейската конвенция за правата на човека, което гарантира зачитането на личния и семейния живот, жилището и кореспонденцията и определя условията, при които се допускат ограничения на това право.
Развитието на съобщенията и информационните технологии във всеки обществен сектор улеснява все повече получаването на достъп и обработката на лични данни, което изисква определени гаранции за неприкосновеността на личната информация и личния живот и същевременно предполага наличието на ясни правила за гарантиране на тази защита.
Значителна стъпка в тази посока е приемането на Общия регламент за защита на личните данни, с който се регламентира защитата на физическите лица при обработването на свързаните с тях лични данни и правото на достъп до събираните и обработвани данни.
Спецификата на обработването на данни в електронните съобщения изисква наред с общите правила да бъдат въведени и допълнителни изисквания при изграждането на електронни съобщително мрежи и предоставянето на електронни съобщителни услуги.
Ключови думи: лични данни, сигурност; електронни съобщения; трафик на данни; европейска регулация;

Abstract: The right to protection of personal data is part of the rights protected under the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence and defines the conditions under which limitations of this right are allowed.
The development of communications and information technology in every public sector makes it increasingly easy to access and process personal data. This requires certain guarantees for the inviolability of personal information and privacy and at the same time implies the existence of clear rules to guarantee this protection.
The specificity of data processing in electronic messages requires that, along with the general rules, additional requirements be introduced in the construction of networks and the provision of services.
Keywords: personal data, security; electronic messages; data traffic; European regulation;

1. Въведение

Ежедневно всеки човек може да стане субект на обработка на лични данни или самият той да борави с такива. С личната информация на гражданите боравят публичните органи на власт и управление, данъчните, полицейските, митническите, социалните, общинските и други органи. Лични данни се обработват и от частния сектор, където работодатели, търговци, банки, лекари, телекомуникационни оператори и други по различни поводи получават достъп и обработват на лични данни.
Най-широко използваните лични данни са имената или прякора на дадено лице, дата на раждане, единен граждански номер, данни от официални документи за самоличност.

Личните данни могат да бъдат свързани със семейното положение на човека, родство, брачен статут или професионална дейност- квалификация, доходи и други. Или лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез един или повече специфични признаци.

Някои категории онлайн данни също биха могли да се приемат за лични данни и сред тях наред с други са включени и IP адресите**.** IP адресът се разглежда като лични данни единствено и само в случаите, в които посредством него или с негова помощ може да бъде идентифицирано конкретно, подлежащо на идентификация физическо лице. IP адресът като тип идентификационен номер, предоставящ информация относно мрежата и хоста, би попаднал под дефиницията "лични данни" само доколкото би могъл да бъде свързан с определено физическо лице.

Развитието на информационните и комуникационни технологии наложи и необходимостта от специфична правна уредба за електронния съобщителен пазар, която да защити основните човешки права на неприкосновеност на личния живот, свободата и тайната на кореспонденцията, без да се ограничава свободното движение и достъп до информация.

2. Общ Регламент за защита на личните данни

Общият Регламент за защита на личните данни засили защитата на физическите лица, като по този начин подчерта необходимостта от защита на данните като основно право. Като осигурява единен набор от правила, пряко приложими в правния ред на държавите от Европейския съюз, той гарантира свободното движение на лични данни и засилва доверието и сигурността на потребителите, абсолютно необходими елементи за създаването на единен цифров пазар.

Основен принцип в регламента относно защитата на данните е принципът за отчетност, съгласно който администраторът следва да носи отговорност за спазването на всички правила за защита на данните и да отговаря за доказването на това съответствие.

Регламентът защитава личните данни независимо от използваната технология за тяхното обработване, той е „технологично неутрален" и се отнася както за автоматично, така и за ръчно обработване, при условие че данните са организирани в съответствие с предварително определени критерии. Също така е без значение как се съхраняват данните, в ИТ система, чрез видеонаблюдение или на хартиен носител, във всички случаи личните данни са предмет на защита.

Въведени са специални процедури в случай на нарушение сигурността на данните. Ако нарушаването на данните представлява риск, дружествата и организациите, които ги съхраняват, трябва да уведомят съответния орган за защита на данните в определен срок или без ненужно допълнително забавяне. Ако изтичането на данни представлява висок риск и за лицата, тогава те също трябва да бъдат лично информирани.

Общият Регламент се прилага по отношение на дружества или организации, които обработват лични данни като част от дейностите на един от своите клонове, установени в Европейския съюз, независимо от това къде се обработват данните, както и по отношение на организации извън Европейския, които предлагат стоки или услуги, или наблюдават поведението на физически лица в рамките на Европейския съюз.

Съвременните отношения предполагат и голям брой трансгранични прехвърляния на лични данни, които понякога се съхраняват на сървъри в различни държави. Предоставената защита от Общия регламент относно сигурността на данните пътува задно с тях, което означава, че правилата за защита на личните данни продължават да се прилагат, независимо от това къде се намират данните. Това важи и когато данните се прехвърлят на държава, извън Европейския съюз, обикновено наричана "трета страна".

Годишник Телекомуникации 2022, том 9, с. 97-105
Yearbook Telecommunications 2022, vol. 9, p. 97-105
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.22.9.10

В тези случаи регламентът предоставя различни инструменти за прехвърляне на данни от ЕС към тази трета страна.

3. „Щит за личните данни в отношенията между ЕС и САЩ"

Между Европейския съюз и Съединените американски щати съществуват изградени търговски връзки и предаването на лични данни е важен и необходим елемент от трансатлантическите отношения, особено в днешната глобална цифрова икономика. При много трансакции се събират и използват лични данни, което налага през 2016 г. Европейската комисия да приеме т.нар. Решение за адекватност на защитата на личните данни наречено още споразумение или „Щит за личните данни в отношенията между ЕС и САЩ".

Тази правна рамка защитава правата на гражданите на ЕС, чиито лични данни се предават на Съединените щати и установява яснота за предприятията, боравещи с трансатлантическо предаване на данни.

Щитът за личните данни позволява данните да бъдат предадени от Европейския съюз на дружество в Съединените американски щати, при условие че дружеството там обработва личните данни в съответствие с набор от правила и гаранции за защита на данните. Задълженията, които се прилагат по отношение на дружествата съгласно „Щита за личните данни", се съдържат в „Принципите на неприкосновеност на личния живот".

За прилагането на Щита за личните данни е необходимо американските дружества да са регистрирали присъединяването си към тази рамка в Министерството на търговия на САЩ, което отговаря за управлението и администрирането на „Щита" и гарантира, че дружествата спазват своите ангажименти. За да могат да се самосертифицират, дружествата трябва да имат политика в областта на неприкосновеността на личния живот, която е в съответствие с Принципите на неприкосновеност на личния живот. Те трябва да подновяват ежегодно принадлежността си към Щита за личните данни, ако искат да получават и използват лични данни от ЕС съгласно това споразумение.

4. Защита на личните данни в електронните съобщения

Европейската нормативната уредба, свързана със защитата на личните данни в сектора на електронните съобщения, включва наред с общите правила и специални такива, залегнали в редица европейски и национални документи.

Първата обща Директива за защита на личните данни е приета през 1995 година, по-късно отменена през 2018 г. от Общия Регламент за защита на личните данни.

През 1997 година е приета и специална Директивата за защита на данните в сектора на телекомуникациите, заменена през 2002 г. от Директива 58/ЕО за правото на неприкосновеност на личния живот и електронните съобщения. През 2009 година е приета Директива2009/136/ЕО /за изменение е допълнение на Директивата от 2002 г./, често наричана „**закон за бисквитките**", тъй като наред с всички останали въпроси и дейности по отношение защитата на данните регламентира и т.нар. "Бисквитки".

Директива 2002/58/ЕО има специфичен обхват. Насочена е към обработването на лични данни във връзка с предоставянето на електронни съобщителни услуги в обществените мрежи, включително мрежи, поддържащи устройства за събиране на данни и идентификация, и е приложима спрямо предприятията, предоставяши електронни съобщителни услуги.

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ ПРЕДОСТАВЯНЕ НА ЕЛЕКТРОННИ СЪОБЩИТЕЛНИ УСЛУГИ

Алена Добрева

В рамките на този обхват, Директивата има за цел да осигури едновременно високо ниво на защита на личните данни в електронния съобщителен сектор и да позволи свободното движения на лични данни в рамките на съюза. Това оказа голямо въздействие върху бързоразвиващия се сектор на електронните съобщения, осигурявайки по-високо ниво на защита на данните в тази област.

Същото се отнася и до субектите, които са специално уредени от Директивата. Тя се прилага само спрямо предприятия, които предоставят електронни съобщителни услуги, а обработването на данни, включително за трафик, от субекти, които не са предприятия, предоставящи електронни съобщителни услуги, се уреждат от общите правила на регламента.

Директивата за правото на неприкосновеност на личния живот в електронните съобщения добави и някои специфични термини като „потребител", „данни за трафик", „данни за местонахождение", „услуга с добавена стойност" и „нарушение на сигурността на личните данни", като най-важното изменение в определенията на основни институти касае „съгласието" като законно основание за обработване на лични данни.

Директивата определя три основни категории данни, създавани в процеса на комуникацията:

- ❖ Данни, представляващи съдържанието на съобщенията, изпратени по време на комуникацията, които са строго поверителни;
- ❖ Данни, необходими за установяване и поддържане на комуникация или т. нар. данни за трафика, където се включват информация за участниците, време и продължителност на комуникацията;
- ❖ В рамките на данните за трафика има данни, които се отнасят конкретно до местоположението на комуникационното устройство, т.нар. данни за местонахождението; тези данни същевременно са данни за местонахождението *на потребителите* на комуникационните устройства и са особено важни по отношение на потребителите на мобилни комуникационни устройства.

Данните за трафика могат да се използват от доставчика на услуги само с цел изготвяне на сметка и техническо предоставяне на услугата. Със съгласието на заинтересованото лице, обаче, тези данни могат да бъдат разкривани на други администратори на данни, които предлагат услуги с добавена стойност, като предоставяне на свързана с местонахождението на потребителя информация за най-близката станция на метрото или аптека или например прогнозата за времето за това място.

За друг достъп до данните за комуникациите в електронните мрежи, например достъп за целите на разследването на престъпления, трябва да са спазени изискванията за обоснована намеса в правото на защита на личните данни.

Ограниченията за изпращането на електронна поща за целите на директния маркетинг се разпростират и върху кратките съобщения (SMS), мултимедийните услуги (MMS) и други видове подобни приложения; изпращането на електронна поща за целите на маркетинга е забранено освен ако не е получено предварително съгласие. Без такова съгласие електронна поща за маркетингови цели може да се адресира само до предишни клиенти, ако те са предоставили адреса на своята електронна поща и не възразяват на това.

Инсталирането на „бисквитки" на компютъра, софтуер, който наблюдава и записва действията на използващия го, вече не е позволено без неговото съгласие. Националното законодателство следва да регламентира по-подробно начините, по които да се изрази и получи съгласието, за да предложи достатъчна степен на защита.

Запазването на телекомуникационни данни представлява намеса в правото на защита на данните. Способите за наблюдение или прихващане на съобщения, като например устройствата за подслушване или записване, са позволени само ако това е предвидено в

Годишник Телекомуникации 2022, том 9, с. 97-105
Yearbook Telecommunications 2022, vol. 9, p. 97-105
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.22.9.10

закон и ако представлява необходима мярка в интерес на защита на държавната сигурност, обществената безопасност, паричните интереси на държавата или борбата с престъпността.

5. Специфична уредба на защита на данните в електронните съобщения

Съгласно действащата регламентация, предприятията, предоставящи електронни съобщителни услуги, са длъжни да предприемат „подходящи технически и организационни мерки, за да защитят сигурността на своите услуги", като същевременно и ако е необходимо, това трябва да бъде направено заедно с предприятието, изграждащо обществената електронна съобщителна мрежа.

Директивата за правото на неприкосновеност на личния живот и електронни съобщения и регламентът предвиждат задължение за гарантиране на сигурността,както и задължение за уведомяване на националния надзорен орган в случай на нарушение сигурността на личните данни.

Нивото на сигурност трябва да бъде „съответстващо на риска", като се вземат предвид както техническите възможности, така и разходите за въвеждане на необходимите мерки. Въведените мерки трябва да гарантират, че

- достъп до личните данни да имат само упълномощени служители на компанията за законно разрешени цели;
- защитават съхраняваните или предавани лични данни от случайно или незаконно унищожаване, случайна загуба или промяна, като и неразрешено или незаконно съхраняване, обработка, достъп или разкриване;
- гарантират осъществяването на политиката на сигурност по отношение на обработката на лични данни.

Ако нарушението на сигурността на личните данни има вероятност да повлияе неблагоприятно на личните данни или неприкосновеността на личния живот на абоната, тогава предприятието „уведомява засегнатото лице" за това нарушение „без ненужно забавяне". Не се изисква абонатите и другите засегнати лица, да бъдат информирани за нарушение на сигурността, засягащо техни данни, ако предприятието може да докаже пред компетентния орган, че данните, които са били компрометирани (по-специално, всички данни, които може да са били неправилно разкрити или предоставени на трети лица), са били направени напълно „неразбираеми" чрез подходящи технологични мерки за защита.

Предприятията са длъжни да поддържат регистър на нарушенията по отношение на личните данни, който съдържа факти, свързани с нарушенията, последиците от тях и предприетите действия, които трябва да бъдат достатъчни, за да се създаде възможност за компетентните национални органида проверят спазването на разпоредбите. Регистърът следва да съдържа единствено информацията, необходима за тази цел.

Директивата за правото на неприкосновеност на личния живот и електронни съобщения подчертава основното значение на поверителността на съобщенията като предвижда, че националното законодателство трябва да гарантира конфиденциалност на съобщенията и свързания трафик на данни през обществените съобщителни мрежи и услуги. Забранено е слушане, записване, съхранение и други видове подслушване или наблюдение на съобщения и свързаните данни за трафика от страна на лица, различни от потребители без тяхното съгласие.

6.„Бисквитки”

Така наречените софтуер за наблюдение, уеб грешки, скрити идентификатори и други подобни устройства могат да влязат в терминала на потребителите без тяхното знание, за да получат достъп до информация, да съхраняват скрита информация или да проследяват действията на потребителя и могат сериозно да засегнат правото на неприкосновеност на личния живот на тези потребители.

Съхраняването на информация или получаването на достъп до информация, вече съхранявана в крайното оборудване на абоната, е позволено само при условие, че той е дал своето съгласие след получаване на ясна и изчерпателна информация относно целите на обработването. Това не е пречка за техническо съхранение или достъп когато целта е осъществяване предаването на съобщение по електронна съобщителна мрежа или доколкото е строго необходимо, за да може предприятието да предостави съответната услуга, поискана от потребителя. Основните средства, използвани за това, са т.нар. „Бисквитки” поради което Директивата от 2009 г. първоначално е наричана „Закон за бисквитките” на ЕС.

Потребителите трябва да имат възможност да откажат „Бисквитки” или подобни приспособления, което е особено важно, когато потребители, различни от абоната на услугата, имат достъп до терминалното оборудване и по такъв начин до данни, съдържащи информация, свързана с правото на неприкосновеност на личния живот, която е съхранена в такова оборудване.

Директивата промени режима, приложим спрямо употребата на тези технологии от такъв, при който абонатът или потребителят трябваше да бъде информиран и да има право да откаже залагането на бисквитки на режим, при който бисквитки се позволяват, само при условие че абонатът или потребителят не само е бил информиран, но е и дал положително, свободно, конкретно, информирано и недвусмислено съгласие. Това означава, че използването на “предварително отбелязани” полета за употребата на бисквитки и други, вече не отговаря на изискванията за съгласие в електронните съобщения.

7. Данни за трафик

Данните за трафик могат да се обработват и съхраняват от предприятията, предоставящи електронни съобщителни услуги само за целите на пренасяне на електронни съобщения, изготвяне на сметка за абоната за съобщенията или във връзка с плащания, свързани с взаимно свързване на мрежите. Това обработване не изисква съгласие на абоната или потребителя на услугата, защото е необходимо за самото й предоставяне. Когато данните вече не са необходими за тези услуги, те трябва да бъдат “изтрити или да се направят анонимни”

Данните за трафик могат да се използват и за маркетинг на електронни съобщителни услуги или за предоставянето на услуги с добавена стойност, но в тези случаи се изисква изрично съгласие на потребителя. Съгласието трябва да бъде свободно дадено, конкретно, информирано и недвусмислено, чрез което потребителят чрез изявление или ясно потвърждаващо действие, изразява съгласието си за използване на неговите данни за трафик за маркетинг или предоставянето на услуга с добавена стойност. Предприятието трябва да информира потребителя относно видовете данни за трафик, които се обработват и продължителността на това обработване.

Обработването на “данни за местонахождение, различни от данни за трафик”, т.е. данни, обработвани в електронна съобщителна мрежа, които посочват географската позиция на крайното устройство на потребителя, но които не се обработват за целите на пренасянето на електронно съобщение или изготвяне на сметка за такова съобщение, могат да се обработват само, когато се направят анонимни или доколкото могат да бъдат използвани

Годишник Телекомуникации 2022, том 9, с. 97-105
Yearbook Telecommunications 2022, vol. 9, p. 97-105
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.22.9.10

за предоставяне на услуга с добавена стойност, със съгласието на потребителите или абонатите.

8. Идентификация на входящи и изходящи повиквания и автоматично препращане на повикване

Предприятията, предоставящи електронни съобщителни услуги, трябва да предложат на викащите и виканите потребители възможността да предотвратят идентифицирането на викащата линия от страна на виканото лице, но тези, които получават повиквания от неидентифициран номер трябва да могат да блокират обаждането и да могат да изключват идентифицирането на своята викаща линия за всяко отделно повикване, като и да информират своите абонати за тези възможности.

При спазване на националните правила, предприятията, предоставящи електронни съобщителни услуги могат да отменят блокирането на идентификацията на викащата линия или при искане на абоната да се проследят зложелателни или нарушаващи спокойствието повиквания (за да могат доставчиците и разследващите органи да отговарят на жалби и да се осигурят доказателства при съдебни дела), или за да се съдейства на службите за спешна помощ при отзоваване на спешни повиквания.

9. Указатели на абонати

Абонатите трябва да бъдат информирани за всяко намерение за включване на техни данни, стационарен или мобилен телефонен номер, в указател на абонати, който е или публично достъпен или достъпен чрез услуги за справка. Те трябва да имат възможност да не бъдат включвани в такива указатели без да е необходимо да дават причини за това.

Тези права се прилагат основно за физически лица, но необходимите мерки трябва да осигурят „законните интереси и на абонатите - юридически лица, които също да бъдат „достатъчно защитени".

10. Нежелани съобщения

Възможно е клиент да предостави електронни данни за контакт (телефонен номер или адрес на електронна поща) на дружество в контекста на продажба на продукт или услуга. В тези случаи продавачът може да използва тези детайли за маркетинг на собствените си подобни продукти или услуги за този клиент (т.нар. "Мобилен маркетинг чрез близко разположени системи"), при условие, че на клиента се предлагат лесни начини да възрази на такива подходи във всяко съобщение (т.е. освен ако всяко съобщение не съдържа опция за "отписване" от следващи маркетингови съобщения).

По отношение на другите форми на директен маркетинг (директен маркетинг, различен от мобилния маркетниг чрез близко разположени системи и маркетинг, който използва средства, различни от автоматично набиране, факс машини или електронна поща), в националното законодателство може да се предвиди предварително съгласие (т.е. "вписване", което се предлага към момента на събиране на личните данни) и модел на „отписване" ("информиран, но не възразил").

Изпращането на директни маркетингови съобщения по електронна поща обаче „прикриваща или скриваща идентичността на подателя, от чието име се прави комуникацията, или без валиден адрес, на който получателят да може да изпрати искане да се спрат такива съобщения, във всички случаи е забранено.

Някои права и задължения могат да бъдат ограничени поради причини от важен обществен интерес, т.е. „Когато такова ограничаване представлява необходима, подходяща и пропорционална мярка, за да гарантира националната сигурност, отбрана, обществена безопасност и превенция, разследване, разкриване и преследване на криминални действия.

11. Национална регулация

Общият регламент за защита на личните данни има пряко приложение във вътрешното законодателство на страната. Защитата на личните данни в България е регламентирана в Закона за защита на личните данни на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни.

Специфичното законодателство в Република България в областта на защитата на личните данни в електронните съобщения се основава на основните понятия и принципи, залегнали в Европейското законодателство и Закона за защита на личните данни. Законът за електронните съобщения предвижда специални разпоредби, отнасящи се защитата на личните данни и данните на крайните ползватели на електронни съобщителни услуги.

Предприятията, предоставящи обществени електронни съобщителни мрежи или услуги, включително мрежи, поддържащи устройства за събиране на данни и идентификация, могат да обработват данни на крайните ползватели, само когато те са непосредствено предназначени за предоставяне на електронни съобщителни услуги. Тези данни включват:

- ✓ трафични данни, които са необходими за предоставяне на електронни съобщителни услуги, за таксуване и за формиране на сметките на крайните ползватели;
- ✓ данни за крайния ползвател във връзка със сключване на договори, като за физически лица тези данни са трите имена, единен граждански номер и адрес, съответно личен номер за чуждестранни лица, а за юридическите лица - наименование, седалище, адрес на управление и единен идентификационен код;

Предоставянето на обществени електронни съобщителни услуги не може да е поставено под условие за предоставяне на услугите в зависимост от съгласието на крайния ползвател данните му да бъдат използвани и за други цели. След приключване на повикването събраните трафични данни трябва да бъдат изтрити или съответно деперсонифицирани, освен ако са непосредствено необходими за осъществяване на ново повикване или връзка.

Данните се съхраняват за нуждите на националната сигурност и за предотвратяване, разкриване и разследване на тежки престъпления. Други данни, включително разкриващи съдържанието на съобщенията, не могат да бъдат съхранявани.

Обработването на трафичните данни се извършва от определени от предприятията длъжностни лица, които имат достъп само до данните, необходими за съответната дейност.

Крайните ползватели имат възможност безвъзмездно и по всяко време да оттеглят даденото съгласие за обработването на данни за тяхното местоположение.

Осигуряването сигурността на данните и упражняването на надзор върху дейността на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, за спазване на правилата при съхранение на данните за гарантиране тяхната защита и сигурност в Република България е възложено на Комисията за защита на личните данни. Като регулаторен и контролен орган комисията има всички правомощия, съгласно българското и европейското законодателство.

ИЗТОЧНИЦИ:

1. ПАСАРЕЛСКИ, Росен. *Универсални мобилни телекомуникационни системи: радиоинтерфейс-изследване на каналите, слоевете и протоколите*. София: НБУ, 2013. ISBN 978-954-535-770-1. [PASARELSKI, Rosen. *Universalni mobilni telekomunikatsionni sistemi: radiointerfeys-izsledvane na kanalite, sloevete i protokolite.* Sofia: NBU, 2013. ISBN 978-954-535-770-1.]
2. ПАСАРЕЛСКИ, Росен, Васил КЪДРЕВ и Теодора ПАСАРЕЛСКА. Петото поколение (5G) - мобилни системи и технологии за комуникации на бъдещето. *XXV научна конференция с международно участие*

Годишник Телекомуникации 2022, том 9, с. 97-105
Yearbook Telecommunications 2022, vol. 9, p. 97-105
eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii
DOI: https://doi.org/10.33919/YTelecomm.22.9.10

„Телеком 2017“, София, 26-27.10.2017: Сборник доклади [CD]. 2017, с. 1-10. ISSN 1314-2690. [PASARELSKI, Rosen, Vasil KADREV i Teodora PASARELSKA. Petoto pokolenie (5G) - mobilni sistemi i tehnologii za komunikatsii na badeshteto. *XXV nauchna konferentsia s mezhdunarodno uchastie „Telekom 2017“, Sofia, 26-27.10.2017: Sbornik dokladi:* [CD]. 2017, s. 1-10. ISSN 1314-2690.]

3. ПАСАРЕЛСКИ, Росен и Теодора ПАСАРЕЛСКА. Изследване на фазите за мрежово планиране на мобилни клетъчни мрежи. *Индустриални технологии*. Бургас: Университет „Проф. д-р Асен Златаров“, 2022, (8), с. 122-129. ISSN 1314-9911. [PASARELSKI, Rosen i Teodora PASARELSKA. Izsledvane na fazite za mrezhovo planirane na mobilni kletachni mrezhi. *Industrialni tehnologii*. Burgas: Universitet „Prof. d-r Asen Zlatarov“, 2022, (8), s. 122-129. ISSN 1314-9911.]
4. Закон за електронните съобщения
5. Становище на КЗЛД относно законосъобразното обработване на трафични данни от предприятията, предоставящи обществени електронни съобщителни услуги - КЗЛД (cpdp.bg)
6. КОРФ, Дау и Мари ЖОРЖ, състав. Наръчник за длъжностните лица по защита на данните: Насоки за длъжностните лица по защита на данните в публичния сектор относно това как да осигурят спазване на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните). *Комисия за защита на личните данни* [онлайн]. [прегледан на 23 януари 2023]. Достъпен на: https://www.cpdp.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG.pdf [KORF, Dau i Mari ZHORZH, sastav. Narachnik za dlazhnostnite litsa po zashtita na dannite: Nasoki za dlazhnostnite litsa po zashtita na dannite v publichnia sektor otnosno tova kak da osiguryat spazvane na Reglament (ES) 2016/679 (Obsht reglament otnosno zashtitata na dannite). *Komisia za zashtita na lichnite danni* [onlayn]. [pregledan na 23 yanuari 2023]. Dostapen na: https://www.cpdp.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG.pdf
7. Data protection in the electronic communications sector. *European Union regulations. European Encyclopedia of law* [online]. [viewed 23 January 2023]. Available from: https://europeanlaw.lawlegal.eu/data-protection-in-the-electronic-communications-sector/
8. KZLD_Bulletin_May_2018.pdf (bcnl.org)
9. https://eur-lex.europa.eu/
10. https://expert95.com/
11. 13.pdf (nbu.bg)

Информация за автора:
д-р Алена Добрева, Департамент”Телекомуникации”, НБУ, ул. Монтевидео № 21, 2-609, Тел.: 02 8110609, e-mail: alenadobreva@abv.bg

Contacts:
Alena Dobreva, PhD, Department Telecommunications, New Bulgarian University, 21 Montevideo St. Tel.: (359) 2 8110609, e-mail: **alenadobreva@abv.bg**

Дата на постъпване на ръкописа(Date of receipt of the manuscript): 19.08.2022
Дата на приемане за публикуване(Date of adoption for publication): 30.09.2022