РЕГЛАМЕНТИ

РЕГЛАМЕНТ (ЕС) № 611/2013 НА КОМИСИЯТА

от 24 юни 2013 година

относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) ([1]), и по-специално член 4, параграф 5 от нея,

след като се консултира с Европейската агенция за мрежова и информационна сигурност (ENISA),

след като се консултира с Работната група за защита на лицата по отношение на обработката на лични данни, която е сформирана съгласно член 29 от Директива 95/46/ЕО на Европейския парламент и Съвета от 24 октомври 1995 г. за защита на физическите лица по отношение на обработката на лични данни и за свободното движение на такива данни ([2]) (Работната група по член 29),

след като се консултира с Европейския надзорен орган по защита на данните (ЕНОЗД),

като има предвид, че:

(1) В Директива 2002/58/ЕО се предвижда да бъдат хармонизирани националните разпоредби, необходими за осигуряване на еднаква степен на защита на основните права и свободи, и по-специално правото на неприкосновеност на личния живот и правото на поверителност по отношение на обработката на лични данни в сектора на електронните комуникации, както и да бъде осигурено свободно движение на такива данни и оборудване за електронни комуникации и услуги в Съюза.

(2) Съгласно член 4 от Директива 2002/58/ЕО доставчиците на обществодостъпни електронни съобщителни услуги са задължени да уведомяват компетентните национални органи, а в определени случаи и засегнатите абонати и лица, за нарушенията на сигурността на личните данни. Нарушенията на сигурността на лични данни са дефинирани в член 2, буква и) от Директива 2002/58/ЕО като нарушения на сигурността, които водят до случайно или незаконно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, предавани, съхранявани или обработвани по друг начин във връзка с предоставянето на обществодостъпна електронна съобщителна услуга в Общността.

(3) С цел да се осигури последователност при изпълнението на мерките, посочени в член 4, параграфи 2, 3 и 4 от Директива 2002/58/ЕО, член 4, параграф 5 от нея оправомощава Комисията да приема технически мерки за изпълнение във връзка с обстоятелствата, формата и процедурите, приложими за изискванията за информация и уведомяване, посочени в споменатия член.

(4) Различните национални изисквания в това отношение могат да доведат до правна несигурност, по-сложни и тромави процедури и значителни административни разходи за доставчиците на услуги, извършващи трансгранична дейност. Поради това Комисията счита за необходимо да приеме такива технически мерки за изпълнение.

(5) Настоящият регламент се ограничава със съобщаването на нарушения на сигурността на лични данни и следователно не определя технически мерки за изпълнение във връзка с член 4, параграф 2 от Директива 2002/58/ЕО относно информиране на абонатите, в случай че има конкретна опасност от нарушаване на сигурността на мрежата.

(6) От член 4, параграф 3, първа алинея от Директива 2002/58/ЕО следва, че доставчиците трябва да уведомяват компетентния национален орган за всички нарушения на сигурността на лични данни. Следователно на доставчика не следва да се оставя свобода за вземане на решение дали да уведоми компетентния национален орган. Това обаче не следва да възпрепятства въпросния компетентен национален орган да приоритизира разследването на някои нарушения по начин, който той счита за подходящ в съответствие с приложимото законодателство, и да предприема необходимите мерки за предотвратяване на докладване на недостатъчно или прекалено много нарушения във връзка с лични данни.

(7) Целесъобразно е да се предвиди система за уведомяване на компетентния национален орган за нарушенията на сигурността на лични данни, която се състои, в случаите, в които са изпълнени определени условия, от различни етапи, за всеки от които важат определени срокове. Тази система е предназначена да гарантира, че компетентният национален орган бива информиран възможно най-рано и във възможно най-пълна степен, без обаче да бъде възпрепятстван доставчикът в усилията му да разследва нарушението и да взема необходимите мерки за ограничаване и отстраняване на последствията от него.

([1]) ОВ L 201, 31.7.2002 г., стр. 37.
([2]) ОВ L 281, 23.11.1995 г., стр. 31.

(8) За целите на настоящия регламент, за да се счита, че е било открито нарушение на сигурността на лични данни, не са достатъчни нито обикновеното подозрение, че е имало нарушение на сигурността на лични данни, нито простото откриване на инцидент, без да има налице достатъчно информация, въпреки всички възможни усилия на доставчика да осигури такава. В тази връзка особено внимание следва да се обърне на наличието на информацията, посочена в приложение I.

(9) В контекста на прилагането на настоящия регламент в случай на нарушаване на сигурността на лични данни с трансгранично измерение съответните компетентни национални органи следва да си сътрудничат.

(10) Настоящият регламент не предвижда допълнителна спецификация за регистъра на нарушенията на сигурността на лични данни, който трябва да се поддържа от доставчиците, като се има предвид, че в член 4 от Директива 2002/58/ЕО неговото съдържание се определя изчерпателно. Доставчиците обаче могат да се позовават на настоящия регламент, за да се определи форматът на регистъра.

(11) Всички компетентни национални органи следва да осигурят сигурни електронни средства, така че доставчиците да съобщават за нарушения на сигурността на личните данни в общ формат (основан на стандарт като XML), съдържащ информацията, посочена в приложение I, на съответните езици, така че да се даде възможност на всички доставчици в рамките на Съюза да следват сходна процедура за съобщаване, независимо от това къде се намират или къде е било извършено нарушаването на сигурността на личните данни. В тази връзка Комисията следва да улеснява въвеждането на сигурни електронни средства, като свиква заседания с компетентните национални органи, когато това е необходимо.

(12) При оценяване дали дадено нарушаване на сигурността на личните данни има вероятност да повлияе неблагоприятно на личните данни или неприкосновеността на личния живот на абонат или лице следва да се вземе предвид по-специално естеството и съдържанието на съответните лични данни, по-специално когато данните касаят финансова информация, като например данни за кредитни карти и подробности за банкови сметки; специалните категории от данни, посочени в член 8, параграф 1 от Директива 95/46/ЕО; както и някои данни, конкретно свързани с предоставянето на телефонни или интернет услуги, т.е. данни за електронната поща, данни за местоположението, файлове със статистика за интернет връзките, история на посетените уебстраници и списъци с повиквания, указани по позиции.

(13) При изключителни обстоятелства, когато уведомяването на абоната или лицето може да изложи на риск правилното разследване на нарушаването на сигурността на личните данни, на доставчика следва да бъде разрешено да забавя уведомяването на абоната или лицето. В този контекст извънредни обстоятелства могат да включват криминални разследвания, както и други нарушения на сигурността на лични данни, които не са равностойни на сериозно престъпление, но за които може да е целесъобразно уведомяването да бъде отложено. Във всеки случай националният компетентен орган следва да е този, който преценява за всеки отделен случай и в светлината на обстоятелствата дали да даде съгласие за отлагане или да изиска уведомяване.

(14) Макар че доставчиците следва да имат данни за контакт със своите абонати предвид преките им договорни отношения, за други лица, засегнати от нарушаването на сигурността на личните данни може да няма такава информация. В такъв случай следва да бъде разрешено доставчикът да уведоми въпросните лица първоначално посредством съобщения в основните национални или регионални средства за масова информация, като например вестници, които веднага щом бъде възможно трябва да бъдат последвани от индивидуално уведомяване, както е предвидено в настоящия регламент. Доставчикът следователно не е длъжен като такъв да уведомява чрез средствата за масова информация, а по-скоро е упълномощен да действа по този начин, ако пожелае, когато все още е в процес на определяне на всички лица, които са засегнати.

(15) Информацията за нарушението следва да бъде съсредоточена върху нарушението, а не да бъде свързана с информация по друга тема. Така например включването на информация за нарушаване на сигурността на лични данни в редовна фактура не следва да се счита за адекватен начин за уведомяване за нарушаване на сигурността на лични данни.

(16) В настоящия регламент не се определят конкретни технически мерки за защита, които да оправдават дерогация от задължението за уведомяване на абонатите и лицата за нарушаване на сигурността на личните данни, тъй като тези мерки могат да търпят промени с течение на времето и развитието на технологиите. Комисията обаче следва да бъде в състояние да публикува примерен списък на конкретни такива технологични мерки за защита в съответствие с текущите практики.

(17) Прилагането на криптиране или хеширане не следва да се смята за достатъчно само по себе си, за да позволи доставчиците да претендират в по-широк план, че са изпълнили общото задължение за сигурност, посочено в член 17 от Директива 95/46/ЕО. В тази връзка доставчиците следва също така да прилагат подходящи организационни и технически мерки за предотвратяване, откриване и блокиране на нарушения на сигурността на личните данни. Доставчиците следва да вземат предвид всеки остатъчен риск, който може да съществува, след като са били извършени проверки, с цел да разберат къде потенциално може да има нарушения на сигурността на личните данни.

(18) Когато доставчикът използва друг доставчик за извършването на част от услугата, например във връзка с фактуриране или управленски функции, в случай на нарушение на сигурността на лични данни този друг доставчик,

който няма преки договорни отношения с крайния потребител, не следва да бъде задължен да издава уведомления. Вместо това той следва да предупреди и информира за това доставчика, с който има преки договорни взаимоотношения. Това следва да се прилага и в контекста на предоставянето на едро на електронни съобщителни услуги, когато обикновено доставчикът на едро няма преки договорни отношения с крайния потребител.

(19) В Директива 95/46/ЕО се определя обща рамка за защита на личните данни в Европейския съюз. Комисията представи предложение за регламент на Европейския парламент и на Съвета, който да замени Директива 95/46/ЕО (Директивата за защитата на данните). Предложеният регламент за защитата на данните ще въведе задължение за всички администратори на лични данни да уведомяват за нарушаване на сигурността на личните данни, основавайки се на член 4, параграф 3 от Директива 2002/58/ЕО. Настоящият регламент на Комисията е напълно съвместим с тази предложена мярка.

(20) Предложеният регламент за защитата на данните също така прави ограничен брой технически изменения в Директива 2002/58/ЕО, за да се вземе предвид преобразуването на Директива 95/46/ЕО в регламент. Съществените правни последици от новия регламент за Директива 2002/58/ЕО ще бъдат обект на преразглеждане от страна на Комисията.

(21) Прилагането на настоящия регламент следва да бъде преразгледано три години след влизането му в сила, а неговото съдържание — преразгледано в светлината на действащата нормативна уредба към горепосочения момент, включително в светлината на предложения регламент за защитата на данните. Преразглеждането на настоящия регламент следва да бъдат свързано, когато това е възможно, с евентуално бъдещо преразглеждане на Директива 2002/58/ЕО.

(22) Прилагането на настоящия регламент може да бъде оценено въз основа, *inter alia*, на всяка статистика, водена от националните компетентни органи, за съобщените нарушения на сигурността на лични данни. Тези статистически данни могат да включват например информация относно броя на нарушенията на сигурността на лични данни, съобщени на националния компетентен орган, броя на нарушенията на сигурността на лични данни, съобщени на абоната или лицето, времето, необходимо за разрешаването на проблема с нарушението на сигурността на лични данни, както и дали са били взети технически мерки за защита. Тези статистически данни следва да осигурят на Комисията и на държавите членки последователни и сравними статистически данни и не трябва да разкриват нито самоличността на уведомяващия доставчик, нито тази на засегнатите абонати или лица. За тази цел Комисията може също така да провежда редовни срещи с националните компетентни органи и други заинтересовани страни.

(23) Мерките, предвидени в настоящия регламент, са в съответствие със становището на Комитета за регулиране на съобщенията,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Обхват

Настоящият регламент се прилага за съобщаването на нарушения на сигурността на лични данни от страна на доставчици на публичнодостъпни електронни съобщителни услуги („доставчикът“).

Член 2

Уведомяване на компетентните национални органи

1. Доставчикът уведомява националния компетентен орган за всички нарушения на сигурността на личните данни.

2. Доставчикът уведомява националния компетентен орган за нарушението на сигурността на лични данни не по-късно от 24 часа след откриване на нарушението на сигурността на лични данни, когато това е възможно.

Доставчикът трябва да включи в своето уведомление до националния компетентен орган информацията, посочена в приложение I.

Счита се, че е открито нарушение на сигурността на лични данни, когато доставчикът е получил достатъчно информация, че е имало произшествие, свързано със сигурността, довело до компрометиране на лични данни, за да направи той съдържателно уведомление, както се изисква съгласно настоящия регламент.

3. Когато не е налице цялата информация, посочена в приложение I, и се изисква допълнително разследване на нарушението на сигурността на лични данни, на доставчика следва да бъде разрешено да изпрати първоначалното уведомление на националния компетентен орган не по-късно от 24 часа след откриване на нарушението на сигурността на лични данни. Това първоначално уведомяване на националния компетентен орган включва информацията, посочена в раздел 1 от приложение I. Доставчикът изпраща второ уведомление на националния компетентен орган възможно най-скоро и най-късно в рамките на три дни след първоначалното уведомяване. Това второ уведомление включва информацията, посочена в раздел 2 от приложение I, и когато е необходимо, актуализира вече предоставената информация.

Когато доставчикът, въпреки разследванията си, не е в състояние да предостави цялата информация в тридневен срок от първоначалното уведомяване, той съобщава толкова информация, с колкото разполага за този срок, и предоставя на националния компетентен орган мотивирана обосновка за закъснялото съобщаване на останалата информация. Доставчикът съобщава останалата информация на националния компетентен орган и когато е необходимо, актуализира вече предоставената информация във възможно най-кратък срок.

4. Националният компетентен орган предоставя на всички доставчици, установени в съответната държава членка, сигурни електронни средства за съобщаване на нарушения на сигурността на лични данни и на информация относно процедурите за достъп до тях и използването им. Когато е необходимо, Комисията свиква заседания с компетентните национални органи, за да улесни прилагането на тази разпоредба.

5. Когато нарушаването на сигурността на личните данни засяга абонати или лица от държави членки, различни от тази на националния компетентен орган, на който е било съобщено нарушаване на сигурността на личните данни, националният компетентен орган информира другите съответни национални органи.

За да улесни прилагането на тази разпоредба, Комисията създава и поддържа списък на националните компетентни органи и съответните звена за контакт.

Член 3

Уведомяване на абоната или лицето

1. Когато има вероятност нарушението на сигурността на личните данни да повлияе неблагоприятно на личните данни или неприкосновеността на личния живот на абонат или отделно лице, освен уведомяването, посочено в член 2, доставчикът също така уведомява засегнатия абонат или лице.

2. Дали дадено нарушаване на сигурността на личните данни има вероятност да повлияе неблагоприятно на личните данни или неприкосновеността на личния живот на абонат или отделно лице се преценява, като се вземат предвид по-специално следните обстоятелства:

а) естеството и съдържанието на съответните лични данни, по-специално когато данните се отнасят за финансова информация, специалните категории от данни, посочени в член 8, параграф 1 от Директива 95/46/ЕО, както и данни за местоположението, файлове със статистика за интернет връзките, история на посетените уебстраници, данни за електронната поща и списъци с повиквания, указани по позиции;

б) вероятните последици от нарушаването на сигурността на личните данни за засегнатия абонат или лице, по специално когато нарушението може да доведе до кражба на самоличност или измама с фалшива самоличност, физическа вреда, психично разстройство, накърняване на достойнството или на репутацията; както и

в) обстоятелствата на нарушаването на сигурността на личните данни, по-специално когато данните са били откраднати или когато доставчикът знае, че данните са в притежание на неупълномощена трета страна.

3. Уведомяването на абоната или лицето се извършва без ненужно забавяне след откриването на нарушението на сигурността на лични данни, както е определено в член 2, параграф 2, трета алинея. То не зависи от уведомяването на националния компетентен орган за нарушаване на сигурността на лични данни, посочено в член 2.

4. Доставчикът трябва да включи в своето съобщение до абоната или лицето информацията, посочена в приложение II. Уведомяването на абоната или лицето се извършва на ясен и лесноразбираем език. Доставчикът не трябва да използва уведомяването като възможност за популяризиране или реклама на нови или допълнителни услуги.

5. При изключителни обстоятелства, когато уведомяването на абоната или лицето може да изложи на риск правилното разследване на нарушението на сигурността на лични данни, на доставчика се разрешава, след като е получил съгласие от страна на националния компетентен орган, да забави уведомяването на абоната или лицето, докато компетентният национален орган счете, че е възможно да уведоми за нарушаването на сигурността на лични данни в съответствие с настоящия член.

6. Доставчикът уведомява засегнатия абонат или лице за нарушаването на сигурността на личните данни чрез средства за комуникация, гарантиращи незабавното получаване на информация и чиято сигурност е защитена по подходящ начин в съответствие със съвременното техническо ниво. Информацията за нарушението трябва да бъде съсредоточена върху нарушението, а не да бъде свързана с информация по друга тема.

7. Когато доставчикът, който има преки договорни отношения с крайния потребител, независимо от положените целесъобразни усилия не е в състояние в рамките на срока, посочен в параграф 3, да определи всички лица, които има вероятност да са засегнати по неблагоприятен начин от нарушението на сигурността на лични данни, той може да уведоми въпросните лица посредством обявления в основните национални или регионални медии в съответните държави членки в рамките на посочения срок. Тези обявления следва да съдържат информацията, посочена в приложение II, и когато е необходимо — в сбита форма. В такъв случай доставчикът трябва да продължи да полага всички целесъобразни усилия да определи посочените лица и да им съобщи информацията, посочена в приложение II, във възможно най-кратък срок.

Член 4

Технически мерки за защита

1. Чрез дерогация от член 3, параграф 1 не се изисква уведомяване на засегнат абонат или отделно засегнато лице за нарушение на сигурността на лични данни, ако доставчикът е доказал в удовлетворителна степен пред националния компетентен орган, че е взел подходящи технически мерки за защита и че тези мерки са приложени за данните, засегнати от нарушаването на сигурността. Такива технически мерки за защита трябва да правят данните неразбираеми за всяко лице, което не е упълномощено за достъп до тях.

2. Данните се разглеждат като неразбираеми, ако:

а) са сигурно шифровани със стандартизиран алгоритъм, като ключът, използван за дешифриране на данните, не е бил разкрит при нарушение на сигурността, и ключът, използван за дешифриране на данните, е генериран така, че да не може да бъде открит с наличните технически средства от което и да било лице, което не е упълномощено за достъп до ключа; или

б) са заменени с тяхната хеширана стойност, изчислена със стандартизирана шифроваща хеш-функция с ключ, като ключът, използван за хеширане на данните, не е бил разкрит при нарушение на сигурността, и ключът, използван за хеширане на данните, е генериран така, че да не може да бъде открит с наличните технически средства от което и да било лице, което не е упълномощено за достъп до ключа.

3. В съответствие с текущите практики, след консултация с компетентните национални органи посредством Работната група по член 29, с Европейската агенция за мрежова и информационна сигурност и с Европейския надзорен орган по защита на данните, Комисията може да публикува ориентировъчен списък с подходящи технически мерки за защита, споменати в параграф 1.

Член 5

Използване на друг доставчик

Когато се използва друг доставчик за доставянето на част от електронната съобщителна услуга без преки договорни отношения с абонатите, в случай на нарушение, свързано с личните данни, този друг доставчик незабавно уведомява доставчика, който го е ангажирал.

Член 6

Докладване и преразглеждане

В рамките на три години от влизането в сила на настоящия регламент Комисията следва да представи доклад за прилагането на настоящия регламент, неговата ефективност и въздействието му върху доставчиците, абонатите и физическите лица. Въз основа на този доклад Комисията преразглежда настоящия регламент.

Член 7

Влизане в сила

Настоящият регламент влиза в сила на 25 август 2013 г.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 24 юни 2013 година.

За Комисията
Председател
José Manuel BARROSO

ПРИЛОЖЕНИЕ I

Съдържание на уведомлението до националния компетентен орган

Раздел 1

Идентификационни данни за доставчика

1. Наименование на доставчика

2. Самоличност и координати за връзка на длъжностното лице по защита на данните или на друго звено за контакт, от което може да се получи повече информация

3. Уточнение дали става въпрос за първо или второ уведомление

Първоначална информация относно нарушението на сигурността на личните данни (попълва се в последващи съобщения, когато е приложимо)

4. Дата и време на произшествието (ако са известни; при необходимост може да бъде направена приблизителна оценка), както и на откриването на произшествието

5. Обстоятелства около нарушението на сигурността на личните данни (напр. загуба, кражба, копиране)

6. Естество и съдържание на въпросните лични данни

7. Технически и организационни мерки, които се вземат (или ще бъдат взети) от доставчика по отношение на засегнатите лични данни

8. Съответно използване на други доставчици (когато е приложимо)

Раздел 2

Допълнителна информация относно нарушението на сигурността на личните данни

9. Обобщение на произшествието, което е причинило нарушаването на сигурността на личните данни (включително физическото място на нарушението и съответните носители на данни)

10. Брой на засегнатите абонати или лица

11. Потенциални последствия и потенциални неблагоприятни последици за абонатите или лицата

12. Технически и организационни мерки, взети от доставчика за смекчаване на възможните неблагоприятни последици

Възможно допълнително уведомяване на абонатите или лицата

13. Съдържание на уведомлението

14. Използвани средства за комуникация

15. Брой на уведомените абонати или лица

Възможни трансгранични въпроси

16. Нарушение на сигурността на лични данни, свързано с абонати или лица в други държави членки

17. Уведомяване на други национални компетентни органи

ПРИЛОЖЕНИЕ II

Съдържание на уведомлението до абоната или лицето

1. Наименование на доставчика

2. Самоличност и координати за връзка на длъжностното лице по защита на данните или на друго звено за контакт, откъдето може да се получи повече информация

3. Обобщение на произшествието, което е причинило нарушаването на сигурността на личните данни

4. Приблизителна дата на произшествието

5. Естество и съдържание на съответните лични данни, както е посочено в член 3, параграф 2

6. Вероятни последствия от нарушението на сигурността на личните данни за засегнатия абонат или лице, както е посочено в член 3, параграф 2

7. Обстоятелства около нарушението на сигурността на личните данни, както е посочено в член 3, параграф 2

8. Мерки, взети от доставчика, за разрешаване на проблема с нарушението на сигурността на личните данни

9. Мерки, препоръчани от доставчика, за смекчаване на възможните неблагоприятни последици