ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 10.1.2017 г.
COM(2017) 10 final

2017/0003 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения)

(текст от значение за ЕИП)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

1.1. Основания и цели на предложението

Стратегията за цифров единен пазар („**стратегията за ЦЕП**“)[1] има за цел да се увеличат доверието в цифровите услуги и тяхната сигурност. Реформата на рамката за защита на данните, и по-специално приемането на Регламент (ЕС) 2016/679 — Общият регламент относно защитата на данните („**ОРЗД**“)[2], беше основно действие за постигане на тази цел. Като част от стратегията за цифровия единен пазар беше обявен и прегледът на Директива 2002/58/ЕО (**Директивата за правото на неприкосновеност на личния живот и електронни комуникации**)[3], за да се осигурят високо ниво на защита на неприкосновеността на личния живот на ползвателите на електронни съобщителни услуги и еднакви условия на конкуренция за всички участници на пазара. Настоящото предложение съставлява преглед на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, който включва целите на стратегията за ЦЕП и гарантира съгласуваност с ОРЗД.

Директивата за правото на неприкосновеност на личния живот и електронни комуникации гарантира защитата на основните права и свободи, по-специално на правото на зачитане на личния живот, поверителността на комуникациите и защитата на личните данни в сектора на електронните съобщения. Тя гарантира също така свободното движение на данни от електронни съобщения, електронно съобщително оборудване и електронни съобщителни услуги в Съюза. Тя въвежда във вторичното законодателство на Съюза основното право на зачитане на личния живот по отношение на съобщенията, както е заложено в член 7 от Хартата на основните права на Европейския съюз („**Хартата**“).

В съответствие с изискванията за по-добро регулиране Комисията извърши последваща оценка по програмата за пригодност и резултатност на регулаторната рамка („**оценка по REFIT**“) на Директивата за правото на неприкосновеност на личния живот и електронни комуникации. От оценката следва, че целите и принципите на настоящата рамка остават солидни. От прегледа на Директивата за правото на неприкосновеност на личния живот и електронни комуникации през 2009 г. обаче са настъпили важни технологични и икономически промени на пазара. Потребителите и предприятията разчитат все повече на нови услуги за междуличностни съобщения в интернет като например интернет телефония, съобщения в реално време и уеб базирана електронна поща вместо традиционните съобщителни услуги. Тези съобщителни услуги „over-the-top“ („**OTT**“) по принцип не попадат в обхвата на действащата правна рамка на Съюза за електронните съобщения, включително Директивата за правото на неприкосновеност

---

[1] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите — Стратегия за цифров единен пазар за Европа, COM(2015) 192 final.

[2] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1—88).

[3] 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) (ОВ L 201, 31.7.2002 г., стр. 37).

на личния живот и електронни комуникации. Съответно, директивата не е в синхрон с развитието на технологиите, в резултат на което липсва защита на съобщенията, предавани чрез нови услуги.

1.2. Съгласуваност със съществуващите разпоредби в тази област на политиката

Настоящото предложение е *lex specialis* по отношение на ОРЗД и ще го конкретизира и допълни по отношение на данните от електронните съобщения, които се определят като лични данни. Всички въпроси, отнасящи се до обработката на лични данни, които не са изрично уредени в предложението, са обхванати от ОРЗД. Привеждането в съответствие с ОРЗД доведе до отмяната на някои разпоредби, например задълженията за сигурност по член 4 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

1.3. Съгласуваност с другите политики на Съюза

Директивата за правото на неприкосновеност на личния живот и електронни комуникации е част от правната рамка за електронните съобщения. През 2016 г. Комисията прие предложение за директива за установяване на Европейски кодекс за електронните съобщения („**Кодекса**“)[4], с която се преразглежда рамката. Макар настоящото предложение да не е неразделна част от Кодекса, то отчасти се основава на дадените в него определения, включително това за „електронни съобщителни услуги“. Също като Кодекса, настоящото предложение включва в обхвата си доставчиците на ОТТ услуги, за да отрази реалността на пазара. Освен това Кодексът допълва настоящото предложение, като гарантира сигурността на електронните съобщителни услуги.

Директивата за радиосъоръженията 2014/53/ЕС[5] осигурява единен пазар за радиосъоръженията. В нея по-специално се изисква, преди дадено радиосъоръжение да бъде пуснато на пазара, в него да се включат защитни механизми, които да гарантират защитата на личните данни и неприкосновеността на личния живот на потребителя. Съгласно Директивата за радиосъоръженията и Регламента за европейската стандартизация (ЕС) 2015/2012[6], Комисията е оправомощена да приема мерки. Настоящото предложение не засяга Директивата за радиосъоръженията.

Предложението не съдържа никакви специални разпоредби в областта на запазването на данни. То поддържа по същество член 15 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации и го привежда в съответствие с конкретната формулировка на член 23 от ОРЗД, който предоставя основание за държавите членки да ограничават обхвата на правата и задълженията по

---

4 Предложение за Директива на Европейския парламент и на Съвета за установяване на Европейски кодекс за електронни съобщения (преработена) (COM/2016/0590 final - 2016/0288 (COD)).

5 Директива 2014/53/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за хармонизирането на законодателствата на държавите членки във връзка с предоставянето на пазара на радиосъоръжения и за отмяна на Директива 1999/5/ЕО (ОВ L 153, 22.5.2014 г., стр. 62—106).

6 Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ L 316, 14.11.2012 г., стр. 12—33).

конкретни членове от Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Следователно държавите членки са свободни да запазят или създадат национални рамки за запазването на данни, които между другото предвиждат целенасочени мерки за запазване, доколкото такива рамки съответстват на правото на Съюза и отчитат съдебната практика на Съда на Европейския съюз относно тълкуването на Директивата за правото на неприкосновеност на личния живот и електронни комуникации и Хартата на основните права[7].

Не на последно място, предложението не се отнася до дейността на институциите, органите и агенциите на Съюза. Неговите принципи обаче, както и съответните задължения относно правото на зачитане на личния живот и комуникациите във връзка с обработването на данни от електронни съобщения, са включени в предложението за регламент за отмяна на Регламент (ЕО) № 45/2001[8].

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

2.1. Правно основание

Член 16 и член 114 от Договора за функционирането на Европейския съюз („**ДФЕС**“) представляват съответното правно основание на предложението.

С член 16 от ДФЕС се въвежда специално правно основание за приемането на правила във връзка със защитата на лицата по отношение на обработката на лични данни от институции на Съюза от страна на държавите членки при осъществяването на дейности, попадащи в обхвата на законодателството на Съюза, и правила във връзка със свободното движение на тези данни. Тъй като електронните съобщения на физическите лица обикновено се считат за лични данни, защитата на физическите лица по отношение на неприкосновеността на съобщенията им и обработката на такива данни следва да се основава на член 16.

Освен това предложението има за цел да защити съобщенията и свързаните с тях законни интереси на юридическите лица. Съгласно член 52, параграф 3 от Хартата, значението и обхватът на правата, посочени в член 7 от нея, са същите като предвидените в член 8, параграф 1 от Европейската конвенция за защита на правата на човека и основните свободи („**ЕКПЧ**“) Що се отнася до обхвата на член 7 от Хартата, съдебната практика на Съда на Европейския съюз[9] и на Европейския съд по правата на човека[10] потвърждава, че професионалните дейности на юридическите лица не могат да бъдат изключени от закрилата на правото, гарантирано в член 7 от Хартата и в член 8 от ЕКПЧ.

Тъй като инициативата има двойна цел, а компонентът на защитата на съобщенията на юридическите лица и целта за изграждането на вътрешния пазар за електронни

---

7 Вж. съединени дела C-293/12 и C-594/12, *Digital Rights Ireland и Seitlinger и други*, EU:C:2014:238; Съединени дела C-203/15 и C-698/15 *Tele2 Sverige AB и държавния секретар от името на министерство на вътрешните работи*, EU:C:2016:970.

8 Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1—22).

9 Вж. дело C-450/06 *Varec SA*, EU:C:2008:91, точка 48.

10 Вж., *inter alia*, решения на ЕСПЧ *Niemietz/Германия* от 16 декември 1992 г., серия A № 251-B, точка 29; *Société Colas Est и други/Франция*, № 37971/97, точка 41; ЕКПЧ 2002-III; *Peck/Обединеното кралство,* № 44647/98, точка 57, ЕКПЧ 2003-I; както и *Vinci Construction и GTM Génie Civil et Services/Франция*, № 63629/10 и № 60567/10, точка 63, 2 април 2015 г.

съобщения и осигуряването на неговото функциониране в това отношение не могат да се разглеждат просто като съпътстващи, инициативата следва да се основава също така на член 114 от ДФЕС.

2.2. Субсидиарност

Зачитането на съобщенията е основно право, признато в Хартата. Съдържанието на електронните съобщения може да разкрие много чувствителна информация за крайните ползватели, които ги изпращат или получават. Също така метаданните, извличани от електронните съобщения, могат да разкрият много чувствителна и лична информация, както изрично отчита Съдът на ЕС[11]. Повечето държави членки също отчитат необходимостта от защита на съобщенията като самостоятелно конституционно право. Макар да е възможно държавите членки да провеждат политики, които гарантират, че това право не се нарушава, това не би могло да се постигне по единен начин без правила на Съюза и би породило ограничения на трансграничния поток на лични и нелични данни, свързан с използването на електронни съобщителни услуги. На последно място, за да се запази съгласуваността с ОРЗД е необходимо да се преразгледа Директивата за правото на неприкосновеност на личния живот и електронни комуникации и да се приемат мерки за съгласуване на двата акта.

Технологичното развитие и амбициите на стратегията за ЦЕП предлагат нови аргументи в полза на действието на ниво ЕС. Успехът на цифровия единен пазар в ЕС зависи от това доколко ефективно ЕС премахва националната изолираност и пречките и се възползва от предимствата и икономиите на европейския цифров единен пазар. Освен това, тъй като интернет и цифровите технологии нямат граници, измерението на този проблем надхвърля територията на всяка отделна държава членка. Държавите членки не могат ефективно да разрешат проблемите в сегашната ситуация. За доброто функциониране на ЦЕП се изискват еднакви условия на конкуренция за икономическите оператори, предоставящи взаимозаменяеми услуги, както и еднаква защита на крайните ползватели на равнището на ЕС.

2.3. Пропорционалност

За да се гарантира ефективна правна защита на личния живот и комуникациите, необходимо е да се разшири обхватът, за да включва и доставчиците на ОТТ услуги. Няколко от популярните доставчици на ОТТ вече спазват изцяло или частично принципа на поверителността на съобщенията, но защитата на основните права не може да бъде оставена на саморегулирането на промишлеността. Освен това нараства и значението на ефективната защита на неприкосновеността на крайните устройства, тъй като тя вече е незаменима за съхраняването на чувствителната информация както в личния, така и в професионалния живот. Прилагането на Директивата за правото на неприкосновеност на личния живот и електронни комуникации не можа ефективно да засили ролята на крайните ползватели. Ето защо за постигането на целта е необходимо принципът да се приложи чрез централизиране на съгласието в софтуера, а на ползвателите да се представя информация за неговите настройки за неприкосновеност. Що се отнася до изпълнението на настоящия Регламент, то се опира на надзорните органи и на механизма за съгласуваност на ОРЗД. Освен това предложението позволява държавите членки да приемат национални мерки за дерогация за конкретни законни цели. Така предложението не надхвърля необходимото за постигане на целите и спазва принципа на пропорционалност, изложен в член 5 от Договора за Европейския съюз.

[11] Вж. бележка под линия 7.

Задълженията, наложени на засегнатите услуги, се запазват на възможно най-ниско ниво, без обаче това да накърнява съответните основни права.

2.4. Избор на инструмент

Комисията представя предложение за регламент, за да осигури съгласуваност с ОРЗД и правна сигурност за ползвателите и предприятията, като избегне различните тълкувания в държавите членки. Регламентът може да гарантира еднаква степен на защита в целия ЕС за ползвателите и по-ниски разходи за привеждане в съответствие за предприятията с трансгранична дейност.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИТЕ ОЦЕНКИ, ОТ КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОТ ОЦЕНКИТЕ НА ВЪЗДЕЙСТВИЕТО

3.1. Последващи оценки/проверки за пригодност на действащото законодателство

С оценката по REFIT беше разгледано доколко ефективно Директивата за правото на неприкосновеност на личния живот и електронни комуникации е допринесла за адекватна защита на личния живот и поверителността на съобщенията в ЕС. Тя беше и опит да се установят евентуални случаи на дублиране.

Оценката по REFIT стигна до заключението, че горепосочените цели на директивата продължават да са **от значение**. Докато ОРЗД осигурява защитата на личните данни, Директивата за правото на неприкосновеност на личния живот и електронни комуникации гарантира поверителността на съобщенията, които също могат да съдържат и нелични данни и данни, свързани с юридически лица. Поради това следва ефективната защита на член 7 от Хартата да бъде осигурена чрез отделен инструмент. Други разпоредби, например правилата за изпращането на нежелани рекламни съобщения, също продължават да са от значение.

По отношение на **ефективността и ефикасността**, оценката по REFIT констатира, че Директивата не е постигнала целите си напълно. Неясната формулировка на някои разпоредби и двусмислието на правни понятия застрашават хармонизирането, като по този начин създават предизвикателства за предприятията при упражняването на трансгранична дейност. Освен това оценката показа, че някои разпоредби създават ненужна тежест за предприятията и потребителите. Например правилото за съгласието с цел защита на поверителността на крайните устройства не постигна целите си, тъй като крайните ползватели са изправени пред искания за приемане на проследяващи бисквитки без да разбират значението им, а в някои случаи дори им се поставят бисквитки без тяхно съгласие. Правилото за съгласието включва прекалено много, тъй като обхваща и практики, които не нарушават неприкосновеността на личния живот; от друга страна, то включва прекалено малко, тъй като явно не обхваща някои техники за проследяване (напр. идентификационна информация за устройството, събирана дистанционно), които може да не предполагат достъп до устройството или съхраняване върху него. На последно място, прилагането на това правило може да се окаже скъпо за предприятията.

Оценката заключи, че правилата на Директивата за правото на неприкосновеност на личния живот и електронни комуникации все още имат **добавена стойност за ЕС** за по-пълно постигане на целта за осигуряване на неприкосновеност онлайн в светлината на все по-многонационален пазар на електронните съобщения. Тя също така показа, че

като цяло правилата са **съгласувани** с другите законодателни актове в тази област, макар че бяха установени някои случаи на дублиране с новия ОРЗД (вж. раздел 1.2).

3.2. Консултации със заинтересованите страни

Комисията организира обществена консултация между 12 април и 5 юли 2016 г. и получи 421 отговора[12]. Основните констатации са следните[13]:

– **Нужда от специални правила за сектора на електронните съобщения относно поверителността на електронните съобщения**: 83,4 % от отговорилите граждани, потребителски организации и организации на гражданското общество и 88,9 % от публичните органи са съгласни, докато 63,4 % от представителите на сектора не са съгласни.

– **Разширяване на обхвата с цел включване на нови услуги (OTT):** 76 % от гражданите и организациите на гражданското общество и 93,1 % от публичните органи са съгласни, а едва 36,2 % от представителите на промишлеността подкрепят такова разширяване.

– **Изменение на изключенията от правилото за съгласие за обработването на данни за движението и местоположението:** 49,1 % от гражданите, потребителските организации и организациите на гражданското общество и 35% от публичните органи предпочитат да не се разширяват изключенията, а 36 % от представителите на сектора са в подкрепа на разширените изключения, като 2/3 от тях поддържат просто отмяна на разпоредбите.

– **Подкрепа за предложените решения на проблема със съгласието за приемане на бисквитки**: 81,2 % от гражданите и 63 % от публичните органи подкрепят налагането на задължения на производителите на крайни устройства да пускат на пазара продукти с активирани по подразбиране настройки за неприкосновеност, докато 58 % от представителите на сектора предпочитат подпомагане на саморегулирането/съвместното регулиране.

Освен това Европейската комисия организира два семинара през април 2016 г.: един отворен за всички заинтересовани страни и един за националните компетентни органи, на който бяха разгледани основните въпроси от обществените консултации. Становищата, изразени по време на семинарите, отразяваха резултатите от обществената консултация.

За да се съберат становища от гражданите, в целия ЕС беше проведено проучване на Евробарометър относно правото на неприкосновеност на личния живот и електронните комуникации[14]. Основните констатации са следните[15]:

– 78 % от запитаните заявяват, че е много важно личната информация на техния компютър, смартфон или таблет да може да бъде достъпна само с тяхно разрешение.

---

12 162 предложения и коментари от граждани, 33 — от организации на гражданското общество и организации на потребителите; 186 — от промишлеността и 40 — от публични органи, включително компетентните органи за прилагане на Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

13 Пълният доклад е достъпен на адрес: https://ec.europa.eu/digital-single-market/news-redirect/37204.

14 Проучване на Евробарометър от 2016 г. (ЕВ) 443 относно правото на неприкосновеност на личния живот и електронните комуникации (SMART 2016/079).

15 Пълният доклад е достъпен на адрес: https://ec.europa.eu/digital-single-market/news-redirect/37205.

– 72 % заявяват, че е много важно поверителността на техните електронни писма и онлайн съобщения в реално време да бъде гарантирана.

– 89 % са съгласни с предложената възможност настройките по подразбиране на браузъра им да спират споделянето на свързана с тях информация.

3.3. Събиране и използване на експертни становища

Комисията използва следните съвети от външни експерти:

– Целеви консултации с експертни групи на ЕС: становище на работната група по член 29; становище на Европейския надзорен орган по защита на данните; становище на платформата REFIT; мнения на ОЕРЕС; мнения на ENISA и мнения на членовете на Мрежата за сътрудничество в областта на прилагане на защита на потребителите.

– Външни експертни мнения, особено следните две проучвания:

  – Проучване „Директивата за правото на неприкосновеност на личния живот и електронни комуникации: оценка на транспонирането, ефективността и съвместимостта с предложения Регламент относно защитата на данните“ (SMART 2013/007116).

  – Проучване „Оценка и преразглеждане на Директива 2002/58 относно неприкосновеността на личния живот и сектора на електронните комуникации“ (SMART 2016/0080).

3.4. Оценка на въздействието

Беше направена оценка на въздействието за настоящото предложение, за която Комитетът за регулаторен контрол даде положително становище на 28 септември 2016 г.[16] За да бъдат взети предвид препоръките на Комитета, в оценката на въздействието се обясняват по-добре обхватът на инициативата, нейната съгласуваност с други правни инструменти (ОРЗД, Европейски кодекс на електронните съобщения, Директивата за възобновяемите енергийни източници) и необходимостта от отделен инструмент. Базовият сценарий е доразвит и доизяснен. Анализът на въздействието е по-задълбочен и по-балансиран, за да се изясни и подчертае описанието на очакваните разходи и ползи.

Следните варианти на политика бяха оценени от гледна точка на критериите за ефективност, ефикасност и съгласуваност:

– **Вариант 1:** незаконодателни мерки (актове с незадължителна юридическа сила);

– **Вариант 2:** ограничено укрепване на неприкосновеността/поверителността и опростяване;

– **Вариант 3:** балансирано укрепване на неприкосновеността/поверителността и опростяване;

– **Вариант 4:** значително укрепване на неприкосновеността/поверителността и опростяване;

– **Вариант 5:** отмяна на Директивата за правото на неприкосновеност на личния живот и електронни комуникации.

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

Вариант 3 беше избран в повечето отношения като **предпочитан вариант** за постигане на целите, като се вземат предвид неговата ефективност и съгласуваност. Основните предимства са:

– подобряване на защитата на поверителността на електронните съобщения чрез разширяване на обхвата на правния инструмент, за да включва нови функционално равностойни електронни съобщителни услуги. Освен това регламентът засилва контрола на крайния ползвател, като изяснява, че съгласието може да се изрази чрез подходящи технически настройки.

– подобряване на защитата от нежелани съобщения чрез въвеждане на задължение за представяне на идентификация на телефонния номер, извършващ повикването, или задължителен код за рекламни обаждания и подобрени възможности за блокиране на повиквания от нежелани номера.

– опростяване и изясняване на регулаторната среда чрез свиване на свободата на действие на държавите членки, отмяна на остарели разпоредби и разширяване на изключенията от правилата за съгласие.

Икономическото въздействие на вариант 3 се очаква да бъде като цяло пропорционално на целите на предложението. За традиционните електронни съобщителни услуги се откриват стопански възможности, свързани с обработването на данни от електронни съобщения, а спрямо доставчиците на ОТТ започват да се прилагат същите правила. Това предполага някои допълнителни разходи за привеждане в съответствие за тези оператори. Промяната обаче няма да засегне съществено онези доставчици на ОТТ, които вече упражняват дейност на основата на съгласието. На последно място, въздействието на варианта няма да бъде усетено в държавите членки, които са разширили тези правила и върху доставчиците на ОТТ услуги.

Чрез централизирането на съгласието в софтуер, като например интернет браузъри, приканването на ползвателите да изберат настройките си за неприкосновеност и разширяването на изключенията от правилото за съгласие за бисквитки значителна част от предприятията биха могли да премахнат банерите или известията за бисквитки, което потенциално ще доведе до значителни спестявания и опростяване. Това може обаче да означава, че за рекламодателите с онлайн насоченост ще стане по-трудно да получат съгласие, ако голяма част от ползвателите изберат настройката „Отхвърли бисквитки на трети страни“. Същевременно централизираното съгласие не лишава операторите на уебсайтове от възможността да получат съгласие чрез индивидуално запитване към крайните ползватели и така да запазят настоящия си бизнес модел. За някои доставчици на браузъри или подобен софтуер ще възникнат допълнителни разходи, тъй като те ще трябва да осигурят подпомагащи поверителността настройки.

Външното проучване установи три различни сценария за реализирането на вариант 3 според това кой предоставя диалогов прозорец между ползвателя, избрал настройките „Отхвърли бисквитки на трети страни“ или „Не проследявай“, и уебсайтовете, които той е посетил и които биха желали той да преразгледа избора си. Потенциални изпълнители на тази техническа задача са: 1) софтуер, като например интернет браузъри; 2) проследяващ софтуер на трета страна; 3) отделните уебсайтове (т.е. услуга на информационното общество, поискана от потребителя). Вариант 3 би довел до общи икономии на разходи за постигане на съответствие в сравнение с базовия сценарий в размер на 70 % (948,8 млн. евро) в първия сценарий (решение чрез браузъра), заложен в настоящото предложение. Икономиите на разходи в другите сценарии ще бъдат по-малки. Тъй като цялостните икономии до голяма степен произтичат от значително понижаване на броя на засегнатите предприятия, индивидуалният размер на разходите

за привеждане в съответствие, които дадено предприятие се очаква да понесе, биха били средно по-високи, отколкото понастоящем.

3.5. Пригодност и опростяване на законодателството

Мерките на политиката, предложени в рамките на предпочетения вариант, разглеждат целта за опростяване и намаляване на административната тежест съгласно констатациите на оценката по REFIT и становището на платформата REFIT[17].

Платформата REFIT издаде три набора от препоръки до Комисията:

– Защитата на личния живот на гражданите следва да бъде засилена чрез привеждане в съответствие на Директивата за правото на неприкосновеност на личния живот и електронни комуникации с Общия регламент за защитата на данните;

– Ефективността на защитата на гражданите от нежелана реклама следва да бъде подобрена чрез добавянето на изключения от правилото за съгласие за бисквитките;

– Комисията обръща внимание на проблемите с прилагането на национално равнище и улеснява обмена на най-добри практики между държавите членки.

Предложението включва по-конкретно:

– да се използват технологично неутрални определения, за да се осигури пригодността на регламента към бъдещи нови услуги и технологии;

– да се отменят правилата за сигурност, за да се елиминират случаите на нормативно дублиране;

– да се изясни обхватът, за да се спомогне за отстраняването/намаляването на риска от различно прилагане в държавите членки (точка 3 от становището);

– да се изясни и опрости правилото за съгласие за използването на бисквитки и други идентификатори, както е обяснено в раздели 3.1 и 3.4 (точка 2 от становището);

– надзорните органи да съответстват на органите, компетентни за прилагането на ОРЗД, и осланяне на механизма за съгласуваност на ОРЗД.

3.6. Въздействие върху основните права

Предложението има за цел да повиши ефективността и нивото на защита на неприкосновеността на личния живот и личните данни, обработвани във връзка с електронните съобщения съгласно членове 7 и 8 от Хартата, и да осигури повече правна сигурност. Предложението допълва и конкретизира ОРЗД. Ефективната защита на поверителността на съобщенията е от съществено значение за упражняване на свободата на изразяване и правото на информация и други свързани права, като например правото на защита на личните данни и свободата на мисълта, съвестта и религията.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Предложението няма отражение върху бюджета на Съюза.

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

5. ДРУГИ ЕЛЕМЕНТИ

5.1. Планове за изпълнение и механизъм за наблюдение, оценка и докладване

Комисията ще наблюдава прилагането на регламента и ще представя доклад с оценката си на Европейския парламент, на Съвета и на Европейския икономически и социален комитет на всеки три години. Тези доклади ще бъдат публично достъпни и ще разглеждат подробно ефективното прилагане и изпълнение на настоящия регламент.

5.2. Подробно разяснение на специалните разпоредби на предложението

Глава I съдържа общите разпоредби: предмета (член 1), обхвата (членове 2 и 3) и неговите определения, включително препратки към съответните определения от други инструменти на ЕС, например ОРЗД.

Глава II съдържа ключовите разпоредби, с които се осигурява поверителността на електронните съобщения (член 5) и ограничените разрешени цели и условия за обработването на такива данни от съобщения (членове 6 и 7). Тя също така разглежда защитата на крайното устройство, като i) гарантира целостта на съхраняваната в него информация и ii) защитава информацията, изпратена от крайно устройство, тъй като тя може да позволи идентифицирането на крайния ползвател (член 8). На последно място, в член 9 се разяснява подробно съгласието на крайните ползватели, основен правен аспект на настоящия регламент, с изрично позоваване на определението му и условията, предвидени в ОРЗД, а с член 10 се налага задължение на доставчиците на софтуер, позволяващ електронни съобщения, да помогнат на крайните ползватели да направят ефективен избор на настройки за неприкосновеност. В член 11 подробно се описват целите и условията, при които държавите членки могат да ограничават горепосочените разпоредби.

Глава III е посветена на правата на крайните ползватели да контролират изпращането и получаването на електронни съобщения с цел да защитят неприкосновеността на личния си живот: i) правото на крайните ползватели да попречат на показването на идентификация на повикващия номер, за да гарантират анонимността си (член 12), със съответните изключения (член 13), и ii) задължението за доставчиците на обществено достъпни междуличностни съобщения посредством номер да предоставят възможността да се ограничи получаването на нежелани повиквания (член 14). Тази глава урежда също условията, при които крайните ползватели могат да бъдат включени в обществено достъпни указатели (член 15) и условията, при които могат да се изпращат нежелани съобщения за целите на директния маркетинг (член 17). Тя се отнася също така до рисковете за сигурността и предвижда задължение за доставчиците на електронни съобщителни услуги да сигнализират на крайните ползватели за определени рискове, които биха могли да компрометират сигурността на мрежите и услугите. Задълженията за сигурност по Общия регламент относно защитата на данните и Европейския кодекс за електронни съобщения ще се отнасят за доставчиците на електронни съобщителни услуги.

Глава IV разглежда надзора и прилагането на настоящия регламент и го поверява на надзорните органи, отговарящи за ОРЗД, предвид значителните синергични взаимодействия между общите въпроси за защита на данните и поверителността на съобщенията (член 18). Правомощията на Европейския надзорен орган по защита на данните се разширяват (член 19), а механизмът за сътрудничество и съгласуваност, предвиден в ОРЗД, ще се прилага по трансгранични въпроси, свързани с настоящия регламент (член 20).

В глава V се изброяват разнообразните средства за правна защита, към които могат да прибегнат крайните ползватели (членове 21 и 22), и санкциите, които могат да бъдат налагани (член 24), включително общите условия за налагане на административни глоби (член 23).

Глава VI се отнася до приемането на делегирани актове и актове за изпълнение в съответствие с членове 290 и 291 от Договора.

И накрая, в глава VII се съдържат заключителните разпоредби на настоящия регламент: отмяна на Директивата за правото на неприкосновеност на личния живот и електронни комуникации, наблюдение и преглед, влизане в сила и прилагане. Що се отнася до прегледа, Комисията възнамерява да оцени, между другото, дали все така е необходим отделен нормативен акт предвид правните, техническите или икономическите промени, като вземе предвид първата оценка на Регламент (ЕС) 2016/679, която трябва да бъде представена до 25 май 2020 г.

2017/0003 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения)

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално членове 16 и 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет[1],

като взеха предвид становището на Комитета на регионите[2],

като взеха предвид становището на Европейския надзорен орган по защита на данните[3],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) С член 7 от Хартата на основните права на Европейския съюз („Хартата“) се защитава основното право на всеки на зачитане на личния и семейния живот, дома и комуникациите. Зачитането на неприкосновеността на съобщенията е съществено измерение на това право. Поверителността на електронните съобщения гарантира, че информацията, обменяна между страните, и външните елементи на съобщението (включително кога е била изпратена информацията, откъде, до кого) не се разкрива на никого, освен на страните, участващи в съобщението. Принципът на поверителност следва да се прилага по отношение на съществуващи и бъдещи средства за комуникация, включително гласови повиквания, достъп до интернет, приложения за съобщения в реално време, електронна поща, интернет телефония и лични съобщения, осигурявани от социалните медии.

(2) Съдържанието на електронните съобщения може да разкрие много чувствителна информация за физическите лица, участващи в съобщенията, от лични преживявания и емоции до заболявания, сексуални предпочитания и политически възгледи, чието разкриване може да доведе до лични и социални вреди, икономическа загуба или смущение. Също така метаданните, извличани

[1] ОВ С [...], [...] г., стр. [...].
[2] ОВ С [...], [...] г., стр. [...].
[3] ОВ С [...], [...] г., стр. [...].

от електронните съобщения, могат да разкрият много чувствителна и лична информация. Метаданните включват избрани номера, посетени уебсайтове, географско местоположение, час, дата и продължителност на проведен разговор и т.н., което позволява точни заключения относно личния живот на лицата, участващи в електронните съобщения, като например социалните им взаимоотношения, навиците и ежедневните дейности, техните интереси, вкусове и др.

(3) Данните от електронни съобщения могат да разкрият и информация за юридически лица, например търговски тайни или друга поверителна информация с икономическа стойност. Следователно разпоредбите на настоящия регламент следва да се прилагат както към физически, така и към юридически лица. Освен това настоящият регламент следва да гарантира, че разпоредбите на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[4] се прилагат и спрямо крайни ползватели, които са юридически лица. Това включва определението на понятието „съгласие“ в съответствие с Регламент (ЕС) 2016/679. Когато се прави позоваване на „съгласие от краен ползвател“, включително юридически лица, се прилага това определение. Също така юридическите лица следва да се ползват със същите права като крайните ползватели, които са физически лица по отношение на надзорните органи. Освен това надзорните органи по силата на настоящия регламент следва да отговарят и за наблюдението на прилагането на настоящия регламент спрямо юридическите лица.

(4) Съгласно член 8, параграф 1 от Хартата и член 16, параграф 1 от Договора за функционирането на Европейския съюз всеки има право на защита на личните му данни. С Регламент (ЕС) 2016/679 се определят правила за защитата на физическите лица във връзка с обработването на лични данни, както и правила във връзка със свободното движение на лични данни. Данните от електронни съобщения може да включват лични данни, както е определено в Регламент (ЕС) 2016/679.

(5) Разпоредбите на настоящия регламент конкретизират и допълват общите правила за защита на личните данни, установени с Регламент (ЕС) 2016/679 по отношение на данните от електронни съобщения, които се определят като лични данни. Следователно настоящият регламент не понижава равнището на защита, от което се ползват физическите лица съгласно Регламент (ЕС) 2016/679. Обработването на данните от електронни съобщения от доставчиците на електронни съобщителни услуги следва да се допуска само в съответствие с настоящия регламент.

(6) Макар принципите и основните разпоредби на Директива 2002/58/ЕО на Европейския парламент и на Съвета[5] да продължават да са като цяло стабилни, тя не съответства напълно на темпа на развитие на технологиите и пазарната

---

[4] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1—88).

[5] 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) (ОВ L 201, 31.7.2002 г., стр. 37).

реалност, което води до несъгласувана или недостатъчно ефективната защита на правото на неприкосновеност и поверителност по отношение на електронните съобщения. Това развитие включва навлизането на пазара на електронни съобщителни услуги, които от гледна точка на потребителя могат да заменят традиционните услуги, но не е нужно да спазват същия набор от правила. Друга промяна засяга новите техники, които позволяват проследяване на онлайн поведението на крайните ползватели, които не са обхванати от Директива 2002/58/ЕО. Следователно Директива 2002/58/ЕИО следва да бъде отменена и заменена от настоящия регламент.

(7) Държавите членки следва да могат, в рамките, установени с настоящия регламент, да запазят или да въведат национални разпоредби за допълнително уточняване и изясняване на прилагането на правилата на настоящия регламент, за да гарантират ефективно прилагане и тълкуване на тези правила. Следователно свободата на преценка, която държавите членки си запазват в това отношение, следва да поддържа равновесието между защитата на неприкосновеността на личния живот и личните данни и свободното движение на данните от електронни съобщения.

(8) Настоящият регламент следва да се прилага за доставчиците на електронни съобщителни услуги, доставчиците на обществено достъпни указатели, както и доставчиците на софтуер, позволяващ електронни съобщения, включително извличане и представяне на информация в интернет. Настоящият регламент следва също така да се прилага по отношение на физическите и юридическите лица, които използват електронни съобщителни услуги за изпращане на съобщения на директния маркетинг или събират информация, свързана с или съхранявана в терминалните устройства на крайните ползватели.

(9) Настоящият регламент следва да се прилага към данни от електронни съобщения, обработвани във връзка с предоставянето и използването на електронни съобщителни услуги в Съюза, независимо дали обработването им се извършва в Съюза. Освен това, за да не се лишават крайните ползватели в Съюза от ефективна защита, настоящият регламент следва да се прилага и за данни от електронни съобщения, обработвани във връзка с доставката на електронни съобщителни услуги от държави извън Съюза на крайни ползватели в Съюза.

(10) Радиосъоръженията и техният софтуер, които се пускат на вътрешния пазар в Съюза, трябва да отговарят на изискванията на Директива 2014/53/ЕС на Европейския парламент и на Съвета[6]. Настоящият регламент следва да не засяга приложимостта на никое от изискванията на Директива 2014/53/ЕС, нито правомощието на Комисията да приема делегирани актове съгласно Директива 2014/53/ЕС, с които да изисква конкретни категории или класове радиосъоръжения да включват предпазни механизми, за да се гарантира защитата на личните данни и на неприкосновеността на личния живот на крайните ползватели.

(11) Услугите, използвани за съобщителни цели, и техническите средства за тяхното доставяне, претърпяха значително развитие. Крайните ползватели все по-често

[6] Директива 2014/53/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за хармонизирането на законодателствата на държавите членки във връзка с предоставянето на пазара на радиосъоръжения и за отмяна на Директива 1999/5/ЕО (ОВ L 153, 22.5.2014 г., стр. 62).

заместват традиционната гласова телефония, текстовите съобщения (SMS) и услугите за пренос на електронна поща с функционално равностойни онлайн услуги, като например интернет телефонията, съобщенията в реално време и уеб базираните имейл услуги. За да се гарантира ефективна и еднаква защита на крайните ползватели при използването на функционално равностойни услуги, настоящият регламент използва определението на електронни съобщителни услуги, дадено в [Директива на Европейския парламент и на Съвета за установяване на Европейски кодекс за електронните съобщения[7]]. Това определение обхваща не само услуги за достъп до интернет и услуги, състоящи се изцяло или частично в пренасянето на сигнали, но също така и междуличностни съобщителни услуги, независимо дали посредством номер или не, като например интернет телефонията, съобщенията в реално време или уеб базираните имейл услуги. Защитата на поверителността на съобщенията е от съществено значение също и по отношение на междуличностните съобщителни услуги, които са спомагателни за друга услуга. Следователно такъв тип услуги с комуникационни функционалности следва да бъдат обхванати от настоящия регламент.

(12) Свързаните устройства и машини все повече общуват помежду си чрез използване на електронни съобщителни мрежи (Интернет на предметите). Предаването на съобщения между машини включва пренос на сигнали през мрежа и следователно обикновено представлява електронна съобщителна услуга. За да се гарантира пълната защита на правата на неприкосновеност на личния живот и поверителност на съобщенията и за да се насърчи надежден и сигурен Интернет на предметите на цифровия единен пазар, е необходимо да се уточни, че настоящият регламент следва да се прилага по отношение на предаването на съобщения между машини. Следователно принципът на поверителност, залегнал в настоящия регламент, следва също да се прилага към предаването на съобщения между машини. В секторното законодателство също могат да бъдат приети конкретни предпазни механизми, като например Директива 2014/53/ЕС.

(13) Разработването на бързи и ефективни безжични технологии стимулира нарастващото наличие на достъп до интернет за обществеността чрез безжични мрежи, достъпни за всеки на публични места, например „горещи точки“ на различни места в чертите на града, универсални магазини, търговски центрове и болници. Доколкото тези съобщителни мрежи са предоставени на неопределена група от крайни ползватели, поверителността на съобщенията, предавани чрез тези мрежи, следва да бъде защитена. Фактът, че безжичните електронни съобщителни услуги може да се явяват допълнение към други услуги не следва да възпрепятства обезпечаването на защита на поверителността на данните от съобщения и прилагането на настоящия регламент. Следователно настоящият регламент следва да се прилага за данните от електронни съобщения, за които се използват електронни съобщителни услуги и обществени съобщителни мрежи. Той обаче не следва да се прилага за затворени групи крайни ползватели, като например корпоративни мрежи, достъпът до които е ограничен до членовете на предприятието.

[7] Предложение за Директива на Европейския парламент и на Съвета за установяване на Европейски кодекс за електронни съобщения (преработена) (COM/2016/0590 final - 2016/0288 (COD).

(14) Данните от електронни съобщения следва да се определят достатъчно широко и технологично неутрално, за да могат да обхванат всяка информация, засягаща предаденото или обменено съдържание (съдържание на електронните съобщения) и информацията, засягаща крайния ползвател на електронни съобщителни услуги, обработвана за целите на предаване, разпространяване или обмен на съдържание на електронни съобщения, включително данни за проследяване и идентифициране на източника и местоназначението на дадено съобщение, географското местоположение и датата, часът, времетраенето и вида на съобщението. Независимо дали такива сигнали и свързаните с това данни се предават посредством проводници, радиовълни, оптични или електромагнитни способи, включително спътникови мрежи, кабелни мрежи, фиксирани (с комутиране на канали и пакети, включително интернет) и мобилни наземни мрежи или електропроводни системи, данните, свързани с тези сигнали, следва да бъдат считани за метаданни на електронни съобщения и следователно да са обект на разпоредбите на настоящия регламент. Метаданните на електронните съобщения може да включват информация, която е част от абонамента за услугата, когато такава информация се обработва за целите на предаването, разпространението или обмена на съдържание на електронни съобщения.

(15) Данните от електронни съобщения следва да се считат за поверителни. Това означава, че всяка намеса в предаването на данните от електронни съобщения, независимо дали пряко чрез човешка намеса или чрез посредничеството на автоматизирана обработка от машини, без съгласието на участниците в съобщението, следва да бъде забранена. Забраната за прихващане на данни от съобщения следва да се прилага по време на предаването им, т.е. до получаването на съдържанието на електронното съобщение от лицето, за което е предназначено. Прихващане на данни от електронни съобщения може да настъпи например когато някой различен от участниците в съобщението слуша повиквания, чете, сканира или съхранява съдържанието на електронните съобщения или на свързаните с тях метаданни за цели, различни от обмена на съобщения. Прихващането настъпва също така, когато трети страни наблюдават посещаваните уебсайтове, времето на посещенията, взаимодействието с други лица и т.н. без съгласието на съответния краен ползвател. Тъй като технологиите се развиват, нараства и броят на техническите възможности за осъществяване на прихващането. Някои начини могат да варират от инсталиране на оборудване, което събира данни от крайни устройства в целеви области, като т.нар. уловители на международния идентификатор на мобилен абонат (IMSI), до програми и техники, които например прикрито наблюдават навици за сърфиране за целите на създаване на профили на крайните ползватели. Други примери за прихващане включват улавянето на полезните данни или данните от съдържанието през некриптирани безжични мрежи и рутери, включително навиците за сърфиране, без съгласието на крайните ползватели.

(16) Забраната за съхранение на съобщения не е предназначена да забрани всяко автоматично, междинно и краткотрайно съхранение на тази информация, стига това да се извършва единствено с цел осъществяване на предаването в електронната съобщителна мрежа. Не следва да се забранява нито обработването на данни от електронни съобщения с цел гарантиране на сигурността и непрекъснатостта на електронните съобщителни услуги, включително проверка на заплахи за сигурността като присъствие на зловреден софтуер, нито обработването на метаданни с цел гарантиране на изискванията за качество на услугата като например закъснение, колебание и т.н.

(17) Обработването на данни от електронни съобщения може да бъде от полза за предприятията, потребителите и обществото като цяло. По отношение на Директива 2002/58/ЕО настоящият регламент разширява възможностите за доставчиците на електронни съобщителни услуги да обработват метаданните на електронни съобщения на основата на съгласие на крайния ползвател. Крайните ползватели обаче отдават голямо значение на поверителността на своите съобщения, включително на своите онлайн дейности, и желаят да контролират използването на данни от своите електронни съобщения за цели, различни от предаване на съобщението. Ето защо настоящият регламент следва да изисква от доставчиците на електронни съобщителни услуги да получат съгласието на крайните ползватели, за да обработват метаданни на електронни съобщения, които следва да включват данни за местоположението на устройството, генерирани с цел предоставяне и поддържане на достъп и връзка с услугата. Данните за местоположението, генерирани извън контекста на предоставянето на електронни съобщителни услуги, не следва да се разглеждат като метаданни. Примерите за търговско използване на метаданни на електронни съобщения от доставчиците на електронни съобщителни услуги може да включват предоставянето на т.нар. „топлинни карти“ — графично представяне на данни с използване на цветове за указване на присъствието на лица. За да се изобразят движенията в определени посоки за определен период от време, е необходим идентификатор на позициите на лицата през определени интервали. Този идентификатор нямаше да съществува, ако трябваше да се използват анонимни данни, и нямаше да е възможно да се представи подобно движение. Подобно използване на метаданни на електронни съобщения може да бъде от полза на публичните органи и на операторите в сектора на обществения транспорт, за да определят къде да разработят нова инфраструктура въз основа на използването и натиска върху наличната инфраструктура. Когато обработването на метаданни на електронни съобщения, по-специално с нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, има вероятност да доведе до висок риск за правата и свободите на физическите лица, преди обработването следва да се извърши оценка на въздействието върху защитата на данните и, по целесъобразност, консултация с надзорния орган съгласно членове 35 и 36 от Регламент (ЕС) 2016/679.

(18) Крайните ползватели може да дадат съгласието си за обработването на техните метаданни, за да получат конкретни услуги, например услуги за защитата срещу измамни дейности (чрез анализ на данните за използване, местоположението или потребителския профил в реално време). В цифровата икономика услугите често се предоставят срещу насрещна престация, различна от пари, например чрез излагане на крайните ползватели на реклами. За целите на настоящия регламент, съгласие на крайния ползвател, независимо дали последният е физическо или юридическо лице, следва да има същото значение и да подлежи на същите условия като съгласието на субекта на данните съгласно Регламент (ЕС) 2016/679. Услугите за базов широколентов достъп до интернет и гласови съобщения следва да се разглеждат като основни услуги, позволяващи на физическите лица да общуват и да се ползват от цифровата икономика. Съгласието за обработването на данни от използването на интернет или гласови съобщения няма да бъде валидно, ако субектът на данните не разполага с действителен и свободен избор или не е в състояние да оттегли съгласието си без отрицателни последици.

(19) Съдържанието на електронните съобщения се отнася до същността на основното право на зачитане на личния и семейния живот, жилището и тайната на съобщенията, което е защитено по силата на член 7 от Хартата. Всяка намеса в съдържанието на електронните съобщения следва да се позволява само при много ясно определени условия, за конкретни цели и да бъде обект на адекватни предпазни мерки срещу злоупотреба. Настоящият регламент предвижда възможността доставчиците на електронни съобщителни услуги да обработват данни от електронни съобщения при преминаването им с информираното съгласие на засегнатите крайни ползватели. Например доставчиците могат да предлагат услуги, които предполагат сканирането на електронни съобщения с цел премахване на даден предварително определен материал. Предвид чувствителността на съдържанието на съобщенията, настоящият регламент установява презумпцията, че обработването на данни от такова съдържание ще доведе до висок риск за правата и свободите на физическите лица. Когато обработва такива данни, доставчикът на електронни съобщителни услуги следва винаги да се консултира с надзорния орган преди обработването. Такава консултация следва да се осъществява в съответствие с член 36, параграфи 2 и 3 от Регламент (ЕС) 2016/679. Презумпцията не включва обработването на данни от съдържание с цел предоставяне на услуга, поискана от крайния ползвател, когато крайният ползвател е дал съгласието си за такова обработване и то се извършва за целите и времетраенето, които са строго необходими и съразмерни за тази услуга. След като съдържанието на електронните съобщения е било изпратено от крайния ползвател и получено от адресата или адресатите, то може да бъде записано или съхранявано от тях или от трета страна, на която те са възложили да записва и съхранява такива данни. Всяко обработване на такива данни трябва да се извършва в съответствие с Регламент (ЕС) 2016/679.

(20) Крайните устройства на крайните ползватели на електронни съобщителни мрежи и всяка информация, свързана с използването на такива устройства, независимо дали е съхранявана на тях или е изпращана, изисквана или обработвана с цел да им позволи свързване към друго устройство или мрежово оборудване, са част от сферата на личния живот на крайните ползватели, която изисква защита съгласно Хартата на основните права на Европейския съюз и Европейската конвенция за защита на правата на човека и основните свободи. Като се има предвид, че тези устройства съдържат или обработват информация, която може да разкрие подробности за емоционалните, политическите или социалните аспекти от живота на дадено лице, включително съдържанието на съобщения и изображения или местоположението на лицата чрез достъп до GPS функционалността на устройството, списъците с контакти и друга информация, която вече се съхранява в устройството, информацията, свързана с подобни устройства, се нуждае от засилена защита на неприкосновеността. Освен това така наречените шпионски софтуер, пикселни маркери, скрити идентификатори, проследяващи бисквитки и други подобни нежелани инструменти за проследяване могат да проникнат в крайното устройство на крайния ползвател без негово знание, за да получат достъп до информация, да съхраняват скрита информация или да следят действията му. Информацията, свързана с устройството на крайния ползвател, може да бъде събирана и от разстояние за целите на идентифициране и проследяване, като се използват техники като т.нар. „отпечатъци на устройства“, често без знанието на крайния ползвател, и може сериозно да наруши неприкосновеността на личния му живот. Техниките, които тайно следят действията на крайните ползватели, например онлайн заниманията

им или местонахождението на крайните устройства, или саботират функционирането на крайните устройства на крайните ползватели, пораждат значителна заплаха за неприкосновеността на личния живот на крайните ползватели. Следователно всяко подобно вмешателство в крайното устройство на крайния ползвател следва да се позволява само с негово съгласие и само за конкретни прозрачни цели.

(21) Изключения от задължението за получаване на съгласие за използване капацитета за обработване и съхранение на крайните устройства или за достъп до информация, съхранявана в тях, следва да се ограничава до ситуации, които не представляват или представляват много ограничено нарушение на неприкосновеността на личния живот. Например не следва да се иска съгласие за съхранение или достъп по технически съображения, което е строго необходимо и пропорционално на законната цел да се даде възможност за използване на конкретна услуга, изрично поискана от крайния ползвател. Това може да включва съхраняването на бисквитки за времетраенето на една установена сесия на даден уебсайт, за да се проследи нанесената от крайния ползвател информация при попълване на онлайн формуляри от няколко страници. Бисквитките могат да бъдат легитимен и полезен инструмент, например за измерване на трафик на даден уебсайт. Доставчиците на услуги на информационното общество, които предприемат проверка на конфигурацията, за да доставят услуга в съответствие с настройките на крайния ползвател и самото регистриране на факта, че устройството на крайния ползвател не е в състояние да получи поискано от него съдържание, не следва да съставляват достъп до такова устройство или използване на неговия капацитет за обработка.

(22) Методите, използвани за доставяне на информация и получаване на съгласието на крайния ползвател, следва да бъдат възможно най-лесни за използване. Предвид повсеместното използване на проследяващи бисквитки и други техники за проследяване, от крайните ползватели все по-често се иска да дадат съгласието си за съхраняването на такива проследяващи бисквитки на крайното си устройство. В резултат на това крайните ползватели са претоварени с искания за даване на съгласие. Използването на технически средства за даване на съгласие, например чрез прозрачни и лесни за използване настройки, може да реши този проблем. Поради това в настоящия регламент следва да се предвиди възможност за изразяване на съгласие чрез използване на съответните настройки на браузър или друго приложение. Изборът, направен от крайните ползватели при определянето на общите настройки за неприкосновеност на браузър или друго приложение, следва да бъде обвързващ за трети страни и да позволява принудително изпълнение срещу тях. Уеб браузърите са вид софтуерно приложение, което позволява извличането и представянето на информация в интернет. Други видове приложения, например такива, които позволяват повиквания и съобщения или представят указания за маршрути, имат същите възможности. Уеб браузърите посредничат при голяма част от взаимодействията между крайния ползвател и уебсайта. От тази гледна точка те са в привилегировано положение да играят активна роля за подпомагане на крайния ползвател да контролира потока от информация към и от съответното крайно устройство. По-специално уеб браузърите могат да се използват като „портиери“, като по този начин помагат на крайните ползватели да попречат на достъпа до и съхранението на информация от тяхното крайно устройство (например смартфон, таблет или компютър).

(23) Принципите на защита на данните при проектирането и по подразбиране бяха кодифицирани в член 25 от Регламент (ЕС) 2016/679. Понастоящем настройките по подразбиране за бисквитки в най-актуалните браузъри са „Приеми всички бисквитки“. Следователно доставчиците на софтуер, който позволява извличане и представяне на информацията в интернет, следва да имат задължението да конфигурират софтуера така, че да предлага възможност да се възпрепятстват трети страни от съхраняването на информация на крайното устройство; това често се представя като „Отхвърли бисквитки на трети страни“. На крайните ползватели следва да се предложи набор от варианти на настройките за неприкосновеност, които варират от по-високи (например „Никога не приемай бисквитки“) към по-ниски (например „Винаги приемай бисквитки“) и средни (например „Отхвърли бисквитки на трети страни“ или „Приемай само собствени бисквитки“). Подобни настройки за неприкосновеност следва да бъдат представени лесно забележимо и разбираемо.

(24) За да могат уеб браузърите да получат съгласието на крайните ползватели, както е определено в Регламент (ЕС) 2016/679, например за съхраняването на проследяващи бисквитки на трети страни, те следва между другото да изискат ясно потвърждение от крайния ползвател на крайното устройство, че дава свободното си, конкретно информирано и недвусмислено съгласие за съхраняване и достъп на такива бисквитки в и от крайното устройство. Подобно действие може да се смята за потвърждение, например, ако се изисква крайните ползватели активно да изберат настройката „Приемай бисквитки на трети страни“, за да потвърдят съгласието си и им се предлага необходимата информация, за да направят избора си. За тази цел е необходимо от доставчиците на софтуер, който позволява достъп до интернет, да се изисква в момента на инсталацията крайните ползватели да бъдат информирани за възможността за избор на настройките за неприкосновеност измежду различните варианти и да бъдат помолени да направят избор. Предоставената информация не следва да разубеждава крайните ползватели да изберат настройките за по-висока защита на неприкосновеността и следва да включва меродавна информация за рисковете, свързани с допускането на съхраняване на бисквитки на трети страни на компютъра, включително съставянето на дългосрочни записи на историята на сърфирането и използването на такива записи за изпращане на целенасочена реклама. Насърчава се практиката уеб браузърите да предлагат на крайните ползватели лесни начини за промяна на настройките за неприкосновеност по време на ползване и да им позволяват да въвеждат изключения, да добавят някои уебсайтове в списък на доверени източници, или да определят бисквитки от кои уебсайтове винаги да се приемат/отхвърлят.

(25) Достъпът до електронните съобщителни мрежи изисква редовното изпращане на определени пакети данни, за да се открие или поддържа връзка с мрежата или други устройства в нея. Освен това устройствата трябва да разполагат с уникален адрес, определен с цел да могат да бъдат идентифицирани в тази мрежа. Безжичните и мобилните телефонни стандарти също така включват изпращането на активни сигнали, съдържащи уникални идентификатори като MAC адрес, IMEI (международен идентификатор на мобилно устройство), IMSI и т.н. Всяка безжична базова станция (т.е. предавател и приемник), като например точка за безжичен достъп, има специален обхват, в който тази информация може да бъде улавяна. Появиха се доставчици на услуги, които предлагат услуги за проследяване на основата на сканиране на информация за устройствата с различни функционални възможности, включително за

преброяване на хора, предоставяне на данни за броя на чакащите на опашка, установяване на броя на хората в даден район, и т.н. Тази информация може да се използва за по-агресивни цели, като изпращане на търговски съобщения до крайни ползватели, например при влизане в магазин, и персонализирани предложения. Макар някои от тези функции да не водят до високи рискове за неприкосновеността, други ги пораждат, например тези, които включват следенето на лица за определени периоди от време, включително повтарящи се посещения на конкретни места. Доставчиците, упражняващи такива практики, следва да поставят лесно забележими надписи по периметъра на района на покритие, за да информират крайните ползватели преди да влязат в него, че технологията е в действие в определен периметър, за целта на проследяването, за отговорното лице и за наличието на мерки, които крайният ползвател може да вземе, за да ограничи или спре събирането на данни. Когато се събират лични данни, съгласно член 13 от Регламент (ЕС) 2016/679 следва да бъде предоставяна допълнителна информация.

(26) Когато обработването на данни от електронни съобщения от доставчици на електронни съобщителни услуги попада в приложното поле на настоящия регламент, регламентът следва да предвижда възможност при определени условия Съюзът или държавите членки да наложат със закон ограничения върху определени задължения и права, ако такова ограничение представлява необходима и пропорционална мярка в едно демократично общество за защита на конкретни обществени интереси, например националната сигурност, отбраната, обществената сигурност и предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност и други важни цели от широк обществен интерес за Съюза или за дадена държава членка, по-специално важен икономически или финансов интерес на Съюза или на дадена държава членка, или функция по наблюдение, инспекция или регулиране, свързана с упражняването на публична власт за защитата на такива интереси. Следователно настоящият регламент не следва да засяга способността на държавите членки да провеждат законно прихващане на електронни съобщения или да предприемат други мерки, ако са необходими и пропорционални за защита на горепосочените обществени интереси, в съответствие с Хартата на основните права на Европейския съюз и Европейската конвенция за защита на правата на човека и основните свободи, според тълкуването на Съда на Европейския съюз и на Европейския съд по правата на човека. Доставчиците на електронни съобщителни услуги следва да предвидят подходящи процедури с цел да се улеснят законните искания от страна на компетентните органи, и когато е целесъобразно, също да вземат предвид ролята на представителя, определен съгласно член 3, параграф 3.

(27) По отношение на идентификацията на повикващата линия е необходимо да се защити правото на повикващата страна да откаже показване на идентификация на повикващата линия, от която се прави повикването, и правото на повиканата страна да отхвърли повиквания от неидентифицирани линии. Някои абонати, по-специално линии за помощ и подобни организации, имат интерес да се гарантира анонимността на техните посетители. По отношение на идентификацията на свързаната линия е необходимо да се защитят правото и законният интерес на повиканата страна да откаже показване на идентификация на линията, към която повикващата страна е свързана.

(28) В специфични случаи има оправдание за незачитане елиминирането на показване на идентификацията на повикващата линия. Правата на крайните ползватели за неприкосновеност на личния им живот по отношение на идентификацията на повикващата линия следва да бъдат ограничени, когато това е необходимо, за да се проследят досадни повиквания; по отношение на идентификацията на повикващата линия и данните за местонахождението те следва да бъдат ограничени, когато това е необходимо, за да се позволи на аварийните служби, например спешното повикване от автомобил (eCall), да изпълняват задачите си колкото е възможно по-ефективно.

(29) Съществува технология, която дава възможност на доставчиците на електронни съобщителни услуги да ограничат получаването на нежелани обаждания от крайните ползватели по различни начини, включително блокирането на автоматични повиквания и други измамни или досадни обаждания. Доставчиците на обществено достъпни електронни съобщителни услуги посредством номер следва да въведат тази технология и да защитават крайните ползватели безплатно срещу досадни обаждания. Доставчиците следва да гарантират, че на крайните ползватели е известно съществуването на такива функции, например като оповестят факта на своята интернет страница.

(30) Обществено достъпните указатели на крайни ползватели на електронни съобщителни услуги са широко разпространени. Обществено достъпни указатели означава всеки указател или услуга, съдържащи информация за крайните ползватели, като телефонни номера (включително мобилни телефони), електронен адрес, данните за контакт, и включва услугите за справки. Правото на неприкосновеност на личния живот и на защита на личните данни на физическите лица изисква от крайните ползватели, които са физически лица, да се поиска съгласието им преди техните лични данни да бъдат включени в указател. Законният интерес на юридическите лица изисква на крайните ползватели, които са юридически лица, да се даде правото да възразят срещу включването в указателя на данни, които се отнасят до тях.

(31) Ако крайните ползватели, които са физически лица, дадат съгласието си данните им да бъдат включени в такива указатели, те следва да могат да определят чрез съгласие кои категории лични данни да бъдат включени в указателя (например име, електронен адрес, домашен адрес, потребителско име, телефонен номер). Освен това доставчиците на обществено достъпни указатели следва да информират крайните ползватели за целите на указателя и за неговите функции за търсене преди да ги включат в този указател. Крайните ползватели следва да могат да определят посредством съгласие въз основа на кои категории лични данни могат да бъдат търсени техните данни за контакт. Категориите лични данни, включени в указателя, и категориите лични данни, на основата на които могат да се търсят данните за контакт на крайния ползвател, не са непременно едни и същи.

(32) В настоящия регламент директен маркетинг се отнася до всяка форма на реклама, чрез която физическо или юридическо лице изпраща преки маркетингови съобщения непосредствено до един или повече идентифицирани или идентифицируеми крайни ползватели, които използват електронни съобщителни услуги. Освен предлагането на продукти и услуги с търговска цел, това следва да включва и съобщения, изпращани от политически партии, които се свързват с физически лица посредством електронни съобщителни услуги, за да провеждат кампании за популяризиране. Същото следва да се прилага и за

съобщения, изпратени от други организации с нестопанска цел в подкрепа на целите на организацията.

(33) Следва да се осигурят защитни механизми за предпазване на крайните ползватели срещу нежелани съобщения за целите на директния маркетинг, които се натрапват в техния личен живот. Степента на навлизане в личния живот и причиненото неудобство се смятат за приблизително сходни, независимо от голямото разнообразие от технологии и канали за осъществяването на тези електронни съобщения — чрез автоматизирани повикващи системи и системи за комуникация, приложения за съобщения в реално време, електронна поща, SMS, MMS, Bluetooth и т.н. Следователно е обосновано да се изисква получаването на съгласие от крайния ползвател преди да му се изпратят търговски електронни съобщения за целите на директния маркетинг, за да може личният живот на физическите лица и законните интереси на юридическите лица да бъдат ефективно защитени. Правната сигурност и нуждата да се гарантира бъдещата пригодност на правилата за защита срещу нежелани електронни съобщения обосновават необходимостта от определяне на единен набор от правила, които не се променят в зависимост от използваната за предаване на нежелани съобщения технология, като същевременно се гарантира еднакво ниво на защита за всички граждани в целия Съюз. Разумно е обаче да се позволи използването на данни за контакт по електронна поща в контекста на съществуващи връзки с клиенти с цел предлагане на подобни продукти или услуги. Подобна възможност следва да се отнася единствено за същата компания, която е получила данните за контакт по електронна поща в съответствие с Регламент (ЕС) 2016/679.

(34) Когато крайните ползватели са дали съгласието си да получават нежелани съобщения за целите на директен маркетинг, те следва да имат възможност да оттеглят лесно това съгласие във всеки момент. За да се улесни ефективното прилагане на правилата на Съюза относно нежелани съобщения за директен маркетинг, е необходимо да се забрани прикриването на самоличността и използването на фалшива самоличност и фалшиви адреси или номера за отговор при изпращането на нежелани търговски съобщения за целите на директния маркетинг. Нежеланите рекламни съобщения следва да бъдат ясно разпознаваеми като такива и да посочват самоличността на юридическото или физическото лице, което ги изпраща, или от чието име се изпраща съобщението, и да предоставят на получателите необходимата информация, за да могат да упражнят правото си да се противопоставят на получаването на още писмени и/или устни рекламни съобщения.

(35) За да е възможно лесното оттегляне на съгласието, юридическите или физическите лица, които изпращат съобщения на директния маркетинг по електронна поща, следва да предоставят хипервръзка или валиден адрес на електронна поща, който крайните ползватели могат да използват удобно за целта. Юридическите или физическите лица, които осъществяват директен маркетинг чрез гласови повиквания или автоматизирани повикващи системи и системи за комуникация, следва да показват идентификация на линията си, на която дружеството може да бъде потърсено, или да предоставят специфичен код, който да удостоверява обстоятелството, че става дума за рекламно обаждане.

(36) Гласовите повиквания за целите на директния маркетинг, които не включват използването на автоматизирани повикващи системи и системи за комуникация, са по-скъпи за повикващия и не налагат финансови разходи на крайните ползватели. Следователно държавите членки следва да могат да установят и

поддържат национални системи, които позволяват осъществяването на такива повиквания само до крайните ползватели, които не са възразили срещу тях.

(37) Доставчиците на услуги, които предлагат електронни съобщителни услуги, следва да информират крайните ползватели за мерките, които могат да вземат с цел защита на сигурността на своите съобщения, например чрез използване на специални софтуерни или криптиращи технологии. Изискването да се информират абонатите за специални рискове относно сигурността не освобождава доставчика на услуга от задължението да предприеме на свои разноски подходящи и незабавни мерки, за да отстрани всякакви нови, непредвидими рискове за сигурността и да възстанови нивото на нормална сигурност на услугата. Предоставянето на информация относно рисковете за сигурността на абонатите следва да бъде безплатно. Сигурността се оценява, като се взема предвид член 32 от Регламент (ЕС) 2016/679.

(38) За да се осигури пълна съгласуваност с Регламент (ЕС) 2016/679, прилагането на разпоредбите на настоящия регламент следва да се повери на същите органи, които отговарят за прилагането на разпоредбите на Регламент (ЕС) 2016/679, а настоящият регламент разчита на механизма за съгласуваност на Регламент (ЕС) 2016/679. Държавите членки следва да могат да създават повече от един надзорен орган, за да отговаря на тяхната конституционна, организационна и административна структура. Надзорните органи следва да отговарят и за наблюдението на прилагането на настоящия регламент по отношение на данните от електронни съобщения на юридически лица. Такива допълнителни задачи не следва да застрашават способността на надзорния орган да изпълнява своите задачи по отношение защитата на личните данни в съответствие с Регламент (ЕС) 2016/679 и настоящия регламент. На всеки надзорен орган следва да бъдат осигурени финансови и човешки ресурси, помещения и инфраструктура, които са необходими за ефективното изпълнение на задачите му съгласно настоящия регламент.

(39) Всеки надзорен орган следва да бъде компетентен на територията на собствената си държава членка да упражнява правомощията и изпълнява задачите, предвидени в настоящия регламент. За да се осигури съгласуваното наблюдение и прилагане на настоящия регламент навсякъде в Съюза, надзорните органи във всяка държава членка следва да имат еднакви задачи и ефективни правомощия да сезират съдебните власти за нарушения на настоящия регламент и да участват в съдебни производства, без да се засягат правомощията на прокуратурата съгласно националното законодателство. Държавите членки и техните надзорни органи се приканват да вземат предвид специфичните нужди на микропредприятията, малките и средните предприятия при прилагането на настоящия регламент.

(40) За да се подкрепи прилагането на правилата на настоящия регламент, всеки надзорен орган следва да има правомощието да налага санкции, включително административни глоби, за всяко нарушение на настоящия регламент, в допълнение към или вместо всякакви други подходящи мерки по силата на настоящия регламент. В настоящия регламент следва да се посочат нарушенията и максималният размер и критериите за определяне на съответните административни наказания „глоба“ или „имуществена санкция“, които следва да се определят от компетентния надзорен орган във всеки отделен случай, като се вземат предвид всички обстоятелства, свързани с конкретната ситуация, по-специално при надлежно отчитане на естеството, тежестта и продължителността

на нарушението и на последиците от него, както и на мерките, предприети, за да се гарантира спазване на задълженията по настоящия регламент и за да се предотвратят или смекчат последиците от нарушението. За целите на определянето на размера на глобата съгласно настоящия регламент, „предприятие“ следва да се разбира по смисъла на членове 101 и 102 от Договора.

(41) За да бъдат постигнати целите на настоящия регламент, а именно защита на основните права и свободи на физическите лица, и по-специално на тяхното право на защита на личните данни, както и за да се гарантира свободното движение на лични данни в рамките на Съюза, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от ДФЕС, за да допълва настоящия регламент. Делегирани актове следва да бъдат приети по-специално по отношение на информацията, която трябва да се представи, включително посредством стандартизирани икони, за да се даде лесно видим и разбираем обзор на събирането на информация, излъчвана от крайното устройство, целта на това събиране, отговорното за него лице и мерките, които крайният ползвател на крайното устройство може да вземе, за да го ограничи. Необходими са също така делегирани актове за определяне на код, с който да се идентифицират повиквания за целите на директния маркетинг, включително тези, извършвани чрез автоматизирани повикващи системи и системи за комуникация. От особена важност е Комисията да проведе подходящи консултации и тези консултации да бъдат проведени в съответствие с принципите, залегнали в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 г.[8] По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове. За да се гарантират еднакви условия за прилагане на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия, когато това е предвидено в него. Тези правомощия следва да се упражняват в съответствие с Регламент (ЕС) № 182/2011.

(42) Доколкото целта на настоящия регламент, а именно осигуряване на еквивалентно ниво на защита на физическите лица и свободното движение на данни от електронни съобщения навсякъде в Съюза, не може да бъде постигната в достатъчна степен от държавите членки, а поради обхвата или последиците от предвиденото действие, може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигане на тази цел.

(43) Директива 2002/58/ЕО следва да бъде отменена.

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

---

[8] Междуинституционално споразумение между Европейския парламент, Съвета на Европейския съюз и Европейската комисия за по-добро законотворчество от 13 април 2016 г. (ОВ L 123, 12.5.2016 г., стр. 1—14).

ГЛАВА I
ОБЩИ РАЗПОРЕДБИ

Член 1
Предмет

1. С настоящия регламент се определят правилата по отношение защитата на основните права и свободи на физическите и юридическите лица при предоставянето и използването на електронни съобщителни услуги, и по-специално правата на зачитане на личния живот и тайната на съобщенията и защитата на физическите и юридическите лица при обработката на лични данни.

2. С настоящия регламент се гарантира свободното движение на данни от електронни съобщения и електронни съобщителни услуги в рамките на Съюза, което не се ограничава, нито забранява по причини, свързани със зачитането на неприкосновеността на личния живот и тайната на съобщенията на физическите и юридическите лица и защитата на физическите лица при обработката на лични данни.

3. Разпоредбите на настоящия регламент конкретизират и допълват Регламент (ЕС) 2016/679 чрез определяне на конкретни правила за целите, посочени в параграфи 1 и 2.

Член 2
Материален обхват

1. Настоящият регламент се прилага за обработването на данни от електронни съобщения във връзка с предлагането и използването на електронни съобщителни услуги и за информация, свързана с крайните устройства на крайните ползватели.

2. Настоящият регламент не се прилага по отношение на:

а) дейности, които попадат извън обхвата на законодателството на Съюза;

б) дейности на държавите членки, които попадат в обхвата на дял V, глава 2 от Договора за Европейския съюз;

в) електронни съобщителни услуги, които не са обществено достъпни;

г) дейности на компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност.

3. Обработката на данните от електронни съобщения от институциите, органите, службите и агенциите на Съюза се урежда от Регламент (ЕС) 00/0000 [нов Регламент, който заменя Регламент (ЕО) № 45/2001].

4. Настоящият регламент не накърнява прилагането на Директива 2000/31/ЕО[9], по-специално разпоредбите относно отговорността на доставчиците на междинни услуги, посочени в членове 12—15 от същата директива.

5. Настоящият регламент не засяга разпоредбите на Директива 2014/53/ЕС.

Член 3
Териториален обхват и представител

1. Настоящият регламент се прилага за:

а) предоставянето на електронни съобщителни услуги на крайните ползватели в Съюза, независимо дали от тях се изисква да ги заплащат;

б) използването на такива услуги;

в) защитата на информацията, свързана с крайните устройства на крайните ползватели, намиращи се в Съюза.

2. Когато доставчикът на електронни съобщителни услуги не е установен в Съюза, той определя писмено свой представител в Съюза.

3. Представителят е установен в една от държавите членки, където се намират крайните ползватели на такива електронни съобщителни услуги.

4. Представителят притежава правомощието да отговаря на въпроси и да предоставя информация в допълнение към или вместо доставчика, когото представлява, по-специално на надзорните органи и крайните ползватели, по всички въпроси, свързани с обработката на данни от електронни съобщения с цел осигуряване на съответствие с настоящия регламент.

5. Определянето на представител съгласно параграф 2 не засяга съдебните производства, които биха могли да бъдат открити срещу физическо или юридическо лице, обработващо данни от електронни съобщения във връзка с предоставянето на електронни съобщителни услуги от държави извън ЕС за крайни ползватели в Съюза.

Член 4
Определения

1. За целите на настоящия регламент се прилагат следните определения:

а) определенията в Регламент (ЕС) 2016/679;

б) определенията на понятията „електронна съобщителна мрежа“, „електронна съобщителна услуга“, „междуличностна съобщителна услуга“, „междуличностна съобщителна услуга посредством номер“, „междуличностна съобщителна услуга, която не е посредством номер“, „краен ползвател“ и „повикване“ в член 2, съответно точки 1, 4, 5, 6, 7, 14 и 21 от [Директива за установяване на Европейски кодекс за електронните съобщения];

в) определението за „крайно устройство“ в член 1, точка 1 от Директива 2008/63/ЕО на Комисията[10].

[9] Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия) (ОВ L 178, 17.7.2000 г., стр. 1—16).

2. За целите на параграф 1, буква б) определението на „междуличностна съобщителна услуга“ включва услуги, които позволяват междуличностна и интерактивна комуникация само като незначителна допълнителна възможност, неразделно свързана с друга услуга.

3. Освен това за целите на настоящия регламент се прилагат и следните определения:

а) „данни от електронни съобщения“ означава съдържание и метаданни на електронните съобщения;

б) „съдържание на електронни съобщения“ означава съдържанието, обменено посредством електронни съобщителни услуги, като например текст, глас, видео, изображения и звук;

в) „метаданни на електронни съобщения“ означава данни, обработени в електронна съобщителна мрежа за целите на предаването, разпространението или обмена на съдържание на електронни съобщения, включително данните, използвани за проследяване и идентифициране на източника и местоназначението на съобщението, данните за местоположението на устройството, генерирани в контекста на предоставянето на електронни съобщителни услуги, както и датата, часа, продължителността и вида на съобщението;

г) „обществено достъпен указател“ означава указател на крайните ползватели на електронни съобщителни услуги, независимо дали е на хартиен носител или в електронна форма, който се публикува или предоставя на обществеността или част от нея, включително посредством справочна услуга;

д) „електронна поща“ означава всяко електронно съобщение, съдържащо информация като текст, глас, видео, звук или изображение, изпратено по електронна съобщителна мрежа, което може да бъде съхранявано в мрежата или свързани с нея изчислителни устройства, или на крайното устройство на получателя си;

е) „съобщение за целите на директния маркетинг“ означава всяка форма на реклама, независимо дали е писмена или устна, изпратена от един или повече идентифицирани или идентифицируеми крайни ползватели на електронни съобщителни услуги, включително използването на автоматизирани повикващи системи и системи за комуникация със или без човешка намеса, електронна поща, SMS и т.н.;

ж) „гласови повиквания за целите на директния маркетинг“ означава гласови повиквания, които не предполагат използването на автоматизирани повикващи системи и системи за комуникация;

з) „автоматизирани повикващи системи и системи за комуникация“ означава системи, които са в състояние да започнат повиквания към един или повече получатели в съответствие със зададени на системата инструкции, и да предават звуци, които не са говор в реално време, включително повиквания чрез използването на автоматизирани повикващи системи и системи за комуникация, които свързват повиканото лице с физическо лице.

---

[10] Директива 2008/63/ЕО на Комисията от 20 юни 2008 г. относно конкуренцията на пазарите на крайни далекосъобщителни устройства (ОВ L 162, 21.6.2008 г., стр. 20—26).

ГЛАВА II
ЗАЩИТА НА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ НА ФИЗИЧЕСКИ И ЮРИДИЧЕСКИ ЛИЦА И НА ИНФОРМАЦИЯТА, ПАЗЕНА В ТЕХНИТЕ КРАЙНИ УСТРОЙСТВА

Член 5

Поверителност на данните от електронни съобщения

Данните от електронни съобщения са поверителни. Всяка намеса в тях, например подслушване, проследяване, съхраняване, наблюдение, сканиране или друг вид прихващане, наблюдение или обработка на данните от електронни съобщения от лица, различни от крайните ползватели, се забранява, освен когато е разрешена от настоящия регламент.

Член 6

Разрешена обработка на данни от електронни съобщения

1. Доставчиците на електронни съобщителни мрежи и услуги могат да обработват данни от електронни съобщения, ако:

а) това е необходимо, за да се осъществи предаване на съобщението, за времето, необходимо за тази цел; или

б) това е необходимо за запазване или възстановяване на сигурността на електронните съобщителни мрежи или услуги, или за установяване на технически проблеми и/или грешки в предаването на електронни съобщения, за времето, необходимо за тази цел.

2. Доставчиците на електронни съобщителни услуги могат да обработват метаданни на електронни съобщения, ако:

а) това е необходимо за постигане на съответствие със задължителни изисквания за качество на услугата съгласно [Директива за установяване на Европейски кодекс за електронните съобщения] или Регламент (ЕС) 2015/2120[11] за времето, необходимо за тази цел. или

б) това е необходимо за фактуриране, изчисляване на плащания при взаимна връзка, установяване или прекратяване на измамна или неправомерна употреба на или абонамент за електронни съобщителни услуги; или

в) засегнатият краен ползвател е дал съгласието си за обработване на метаданните на неговите съобщения за една или повече конкретни цели, включително предоставянето на конкретни услуги на крайни ползватели, стига тези цели да не могат да бъдат постигнати чрез обработване на анонимизирана информация.

[11] Регламент (ЕС) 2015/2120 на Европейския парламент и на Съвета от 25 ноември 2015 г. за определяне на мерки относно достъпа до отворен интернет и за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги и на Регламент (ЕС) № 531/2012 относно роуминга в обществени мобилни съобщителни мрежи в рамките на Съюза (ОВ L 310, 26.11.2015 г., стр. 1—18).

3. Доставчиците на електронни съобщителни услуги могат да обработват съдържание на електронни съобщения само:

а) за целите на предоставянето на конкретна услуга на краен ползвател, ако съответният краен ползвател/ползватели е дал изрично съгласие за обработването на съдържанието на неговите или нейните електронни съобщения и услугата не може да бъде осигурена без обработването на такова съдържание; или

б) ако всички засегнати крайни ползватели са дали съгласието си за обработването на съдържанието на електронните им съобщения за една или повече конкретни цели, които не могат да бъдат постигнати чрез обработването на анонимизирана информация, а доставчикът се е консултирал с надзорния орган. Член 36, точки 2 и 3 от Регламент (ЕС) 2016/679 се прилагат за консултацията с надзорния орган.

Член 7

Съхраняване и заличаване на данни от електронни съобщения

1. Без да се засягат разпоредбите на член 6, параграф 1, буква б) и член 6, параграф 3, букви а) и б), доставчикът на електронна съобщителна услуга заличава съдържанието на електронните съобщения или анонимизира тези данни след получаването на съдържанието на електронните съобщения от техния получател или получатели. Такива данни могат да бъдат записвани или съхранявани от крайните ползватели или от трети страни, на които те са поверили записването, съхранението или друга обработка на такива данни съгласно Регламент (ЕС) 2016/679.

2. Без да се засягат разпоредбите на член 6, параграф 1, буква б) и член 6, параграф 2, букви а) и в), доставчикът на електронна съобщителна услуга заличава метаданните на електронните съобщения или анонимизира тези данни, когато те вече не са необходими за целите на предаването на дадено съобщение.

3. Когато обработването на метаданни на електронни съобщения се извършва за целите на фактурирането в съответствие с член 6, параграф 2, буква б), съответните метаданни могат да се пазят до края на периода, през който фактурата може да бъде законно оспорена или може да се осигури получаване на плащане съгласно националното законодателство.

Член 8

Защита на информацията, съхранявана в и свързана с крайните устройства на крайните ползватели

1. Използването на капацитета за обработка и съхранение на крайните устройства и събирането на информация от крайните устройства на крайните ползватели, включително информация за софтуера и хардуера, различна от тази, за която крайният ползвател е дал съгласието си, е забранено, освен ако са налице следните основания:

а) това е необходимо единствено с цел да бъде осъществено предаването на съобщение по електронна съобщителна мрежа; или

б) крайният потребител е дал своето съгласие; или

в) това е необходимо за предоставяне на услуга на информационното общество, поискана от крайния ползвател; или

г) ако е необходимо за измерване на интернет аудиторията, стига това измерване да се извършва от доставчика на услугата на информационното общество, поискана от крайния ползвател.

2. Събирането на информация, излъчена от крайното устройство, за да позволи свързването му към друго устройство или към мрежово оборудване, е забранено, освен когато:

а) това се извършва единствено с цел установяването на връзка и за времето, необходимо за него; или

б) ако се показва ясно и видно съобщение, което информира най-малко за условията на събиране, целта, лицето, отговарящо за него и друга информация, изисквана съгласно член 13 от Регламент (ЕС) 2016/679, когато се събират лични данни, както и всяка мярка, която крайният ползвател на крайното устройство може да предприеме, за да спре или сведе до минимум събирането.

Събирането на такава информация се допуска само при прилагането на подходящи технически и организационни мерки, които гарантират ниво на сигурност, съответстващо на риска, както е посочено в член 32 от Регламент (ЕС) 2016/679.

3. Информацията, която се предоставя съгласно параграф 2, буква б), може да се предоставя в комбинация със стандартизирани икони, за да предложи разбираемо резюме на събирането по лесно видим, разбираем и ясен начин.

4. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 27 за определяне на информацията, която да бъде представена чрез стандартизираната икона, и на процедурите за предоставяне на стандартизирани икони.

Член 9
Съгласие

1. Прилагат се определението и условията за съгласие, предвидени в член 4, параграф 11 и член 7 от Регламент (ЕС) 2016/679.

2. Без да се засягат разпоредбите на параграф 1, когато е технически възможно и осъществимо, за целите на член 8, параграф 1, буква б) съгласие може да бъде изразено чрез използването на съответните технически настройки на софтуерно приложение, което дава достъп до интернет.

3. Крайни ползватели, които са дали съгласието си за обработването на данните от електронни съобщения, както е предвидено в член 6, параграф 2, буква в) и член 6, параграф 3, букви а) и б), получават възможността да оттеглят съгласието си по всяко време, както е предвидено в член 7, параграф 3 от Регламент (ЕС) 2016/679, и да им бъде напомняно за тази възможност през интервали от 6 месеца, докато продължава обработката.

Член 10

Предоставяна информация и варианти за настройки за неприкосновеност

1. Пуснатият на пазара софтуер за осъществяване на електронни съобщения, включително за извличане и представяне на информация по интернет, предлага възможност да се забрани на трети страни да съхраняват информация на крайното устройство на краен ползвател или да обработват информация, която вече се съхранява на това устройство.

2. При инсталиране софтуерът информира крайния ползвател за вариантите на настройките за неприкосновеност, и за да продължи процесът на инсталиране, изисква от крайния ползвател да се съгласи с една от тях.

3. В случай на вече инсталиран софтуер към 25 май 2018 г., изискванията по параграфи 1 и 2 се спазват при първата актуализация на софтуера, но не по-късно от 25 август 2018 г.

Член 11

Ограничения

1. Законодателството на Съюза или на държавите членки може да ограничи чрез законодателна мярка обхвата на задълженията и правата, предвидени в членове 5—8, когато такова ограничение спазва по същество основните права и свободи и представлява необходима, целесъобразна и пропорционална мярка в едно демократично общество, с която се защитават един или повече от широките обществени интереси, посочени в член 23, параграф 1, букви а) — д) от Регламент (ЕС) 2016/679, или функция по наблюдение, инспекция или регулиране, свързана с упражняването на публична власт за защитата на такива интереси.

2. Доставчиците на електронни съобщителни услуги установяват вътрешни процедури за удовлетворяване на искания за достъп до данни от електронни съобщения на крайните ползватели на основата на законодателна мярка, приета съгласно параграф 1. При поискване от страна на компетентния национален орган те му предоставят информация относно посочените процедури, броя на получените искания, посочената правна обосновка и своя отговор.

ГЛАВА III
ПРАВА НА ФИЗИЧЕСКИТЕ И ЮРИДИЧЕСКИТЕ ЛИЦА ЗА КОНТРОЛ ВЪРХУ ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ

Член 12

Показване и ограничаване на идентификацията на повикваща и свързана линия

1. Когато показването на идентификацията на повикващата и свързаната линия се предлага съгласно член [107] от [Директива за установяване на Европейски кодекс за електронните съобщения], доставчиците на обществено достъпни междуличностни съобщителни услуги посредством номер предоставят следното:

а) на повикващия краен ползвател — възможността да спре показването на идентификацията на повикващата линия на база отделен разговор, връзка, или постоянно;

б) на повикания краен ползвател — възможността да спре показването на идентификацията на повикващата линия за входящи повиквания;

в) на повикания краен ползвател — възможността да отхвърли входящи повиквания, когато показването на идентификацията на повикващата линия е било спряно от повикващия краен ползвател;

г) на повикания краен ползвател — възможността да спре показването на идентификацията на свързаната линия на повикващия краен ползвател.

2. Възможностите, посочени в параграф 1, букви а), б), в) и г), се предлагат на крайните ползватели безплатно и с прости средства.

3. Параграф 1, буква а) се прилага също по отношение на повиквания от Съюза към трети държави. Параграф 1, букви б), в) и г) се прилагат също по отношение на входящи повиквания от трети държави.

4. Когато предлагат показване на идентификацията на повикващата или свързаната линия, доставчиците на обществено достъпни междуличностни съобщителни услуги посредством номер предоставят информация на обществеността за възможностите, посочени в параграф 1, букви а), б), в) и г).

Член 13

Изключения от показването и ограничаването на идентификацията на повикваща и свързана линия

1. Независимо дали повикващият краен ползвател е спрял показването на идентификацията на повикващата линия, когато се осъществява повикване към служби за спешно реагиране, доставчиците на обществено достъпни междуличностни съобщителни услуги посредством номер отменят тази настройка и отказа или липсата на съгласие на краен ползвател за обработка на метаданни на база отделна линия за организации, работещи със спешни съобщения, включително центрове за приемане на спешни повиквания.

2. Държавите членки въвеждат по-конкретни разпоредби по отношение на определянето на процедури и обстоятелствата, при които доставчиците на обществено достъпни междуличностни съобщителни услуги отменят временно спряното показване на идентификацията на повикващата линия, когато крайните ползватели поискат проследяване на злонамерени или досадни повиквания.

Член 14

Блокиране на входящи повиквания

Доставчиците на обществено достъпни междуличностни съобщителни услуги посредством номер въвеждат мерки на високо техническо равнище за ограничаване на приемането на нежелани повиквания от крайните ползватели и също така предоставят на повикания краен ползвател безплатно следните възможности:

а) да блокира входящи повиквания от конкретни номера или от анонимни източници;

б) да спре автоматичното препращане на повикването от трета страна до неговото крайно устройство.

Член 15

Обществено достъпни указатели

1. Доставчиците на обществено достъпни указатели получават съгласието на крайните ползватели, които са физически лица, да включат техните данни в указателя, и съответно съгласието на тези крайни ползватели за включване на данни по категория лични данни, доколкото те са от значение за целите на указателя, както са определени от неговия доставчик. Доставчиците предоставят на крайните ползватели, които са физически лица, възможност да проверят, поправят или заличат такива данни.

2. Доставчиците на обществено достъпни указатели информират крайните ползватели, които са физически лица, чиито лични данни се намират в указателя, за наличните в него функции за търсене и получаване на съгласието на крайните ползватели преди да активират такива функции за търсене по отношение на техните собствени данни.

3. Доставчиците на обществено достъпни указатели предоставят на крайните ползватели, които са юридически лица, възможността да възразят срещу включването в указателя на данни, които се отнасят до тях. Доставчиците предоставят на крайните ползватели, които са юридически лица, възможност да проверят, поправят или заличат такива данни.

4. Възможността за проверка, поправка или заличаване на свързаните с тях данни или за отказ от включване в обществено достъпен указател, се предоставя на крайните ползватели безплатно.

Член 16

Нежелани съобщения

1. Физическите или юридическите лица могат да използват електронни съобщителни услуги за целите на изпращане на съобщения на директния маркетинг до крайните ползватели, които са физически лица, дали съгласието си за това.

2. Когато дадено физическо или юридическо лице получи електронни данни за контакт за електронна поща от свой клиент в контекста на продажбата на продукт или услуга съгласно Регламент (ЕС) 2016/679, това физическо или юридическо лице може да използва тези електронни данни за контакт за директен маркетинг на неговите собствени подобни продукти или услуги само ако на клиентите ясно и недвусмислено е дадена възможност да възразят, безплатно и по лесен начин, срещу подобна употреба. Правото на възражение следва да се предостави в момента на събирането на данни и всеки път, когато се изпраща съобщение.

3. Без да се засягат параграфи 1 и 2, физическите или юридическите лица, които използват електронни съобщителни услуги за повиквания за целите на директния маркетинг:

а) представят идентификация на линията, на която може да се осъществи връзка с тях; или

б) представят специфичен код, който да идентифицира повикването като рекламно.

4. Независимо от параграф 1, държавите членки могат да предвидят със закон, че осъществяването на гласови повиквания на директния маркетинг към крайни ползватели, които са физически лица, е разрешено само по отношение на крайни ползватели, които са физически лица и не са възразили срещу получаването на такива съобщения.

5. В рамките на законодателството на Съюза и приложимото национално законодателство държавите членки гарантират, че законните интереси на крайни ползватели, които са юридически лица по отношение на нежелани съобщения, изпратени чрез посочените в параграф 1 средства, са достатъчно защитени.

6. Всяко физическо или юридическо лице, което използва електронни съобщителни услуги за предаване на съобщения на директния маркетинг, информира крайните ползватели за търговското естество на съобщението и самоличността на физическото или юридическото лице, от името на което се предава съобщението, и предоставят на получателите необходимата информация, за да могат те да упражнят правото си да оттеглят по лесен начин своето съгласие за получаването на по-нататъшни маркетингови съобщения.

7. На Комисията се предоставят правомощия да приема мерки за изпълнение в съответствие с член 26, параграф 2 за уточняване на код за идентифициране на маркетингови повиквания съгласно параграф 3, буква б).

Член 17
Информация за установени рискове за сигурността

В случай на особен риск, който може да компрометира сигурността на мрежите и електронните съобщителни услуги, доставчикът на електронни съобщителни услуги информира крайните ползватели за такъв риск, а когато рискът е извън обхвата на мерките, които взема доставчикът на услугите, той информира крайните ползватели за всички възможни средства за отстраняването му, включително за евентуалните разходи.

ГЛАВА IV
НЕЗАВИСИМИ НАДЗОРНИ ОРГАНИ И ПРАВОПРИЛАГАНЕ

Член 18
Независими надзорни органи

1. Независимите надзорни органи, които отговарят за наблюдението на прилагането на Регламент (ЕС) 2016/679, отговарят също така за наблюдението на прилагането на настоящия регламент. Глави VI и VII от Регламент (ЕС) 2016/679 се прилагат *mutatis mutandis*. Задачите и правомощията на надзорните органи се упражняват по отношение на крайните ползватели.

2. Надзорните органи, посочени в параграф 1, си сътрудничат по целесъобразност с националните регулаторни органи, създадени съгласно [Директивата за установяване на Европейски кодекс за електронните съобщения].

Член 19

Европейски комитет по защита на данните

Европейският комитет по защита на данните, установен по силата на член 68 от Регламент (ЕС) 2016/679, има компетентността да гарантира последователното прилагане на настоящия регламент. За тази цел Европейският комитет по защита на данните изпълнява задачите, определени в член 70 от Регламент (ЕС) 2016/679. Комитетът има също така следните задачи:

а) да съветва Комисията относно всяко предложение за изменение на настоящия регламент;

б) да разглежда по своя собствена инициатива, по искане на някой от своите членове или по искане на Комисията всеки въпрос, който се отнася до прилагането на настоящия регламент, и да издава насоки, препоръки и най-добри практики с цел насърчаване на съгласуваното прилагане на настоящия регламент;

Член 20

Процедури за сътрудничество и съгласуване

Всеки надзорен орган допринася за последователното прилагане на настоящия регламент в рамките на Съюза. За тази цел надзорните органи си сътрудничат помежду си и с Комисията съгласно глава VII от Регламент (ЕС) 2016/679 по въпроси от обхвата на настоящия регламент.

ГЛАВА V
СРЕДСТВА ЗА ПРАВНА ЗАЩИТА, ОТГОВОРНОСТ ЗА ПРИЧИНЕНИ ВРЕДИ И САНКЦИИ

Член 21

Средства за правна защита

1. Без да се засягат които и да било други средства за административна или правна защита, всеки от крайните ползватели на електронни съобщителни услуги разполага със същите средства за правна защита, предвидени в членове 77, 78 и 79 от Регламент (ЕС) 2016/679.

2. Всяко физическо или юридическо лице, различно от крайните ползватели, понесло вреди вследствие на нарушения на настоящия регламент и което има законен интерес от преустановяване или забрана на предполагаеми нарушения, включително доставчик на електронни съобщителни услуги, защитаващ своите законни търговски интереси, има правото да завежда съдебни производства по отношение на такива нарушения.

Член 22

Право на компенсация и отговорност за причинени вреди

Всеки краен ползвател на електронни съобщителни услуги, който е претърпял материални или нематериални вреди в резултат на нарушение на настоящия регламент, има право да получи обезщетение от нарушителя за понесените вреди, освен ако

нарушителят докаже, че по никакъв начин не е отговорен за събитието, породило вредите, съгласно член 82 от Регламент (ЕС) 2016/679.

Член 23

Общи условия за налагане на административни наказания „глоба“ или „имуществена санкция“

1. За целите на настоящия член по отношение на нарушенията на настоящия регламент се прилага глава VII от Регламент (ЕС) 2016/679.

2. Нарушенията на посочените по-долу разпоредби подлежат, в съответствие с параграф 1, на административно наказание „глоба“ или „имуществена санкция“ в размер до 10 000 000 евро или, в случай на предприятие — до 2 % от общия му годишен световен оборот за предходната финансова година, като се взема по-високата сума:

а) задълженията на всяко юридическо или физическо лице, което обработва данни от електронни съобщения съгласно член 8;

б) задълженията на доставчика на софтуер за осъществяване на електронни съобщения съгласно член 10;

в) задълженията на доставчика на обществено достъпни указатели съгласно член 15;

г) задълженията на всяко юридическо или физическо лице, което използва електронни съобщителни услуги съгласно член 16.

3. Нарушенията на принципа на поверителност на съобщенията, на позволената обработка на данните от електронни съобщения или на сроковете за заличаване съгласно членове 5, 6 и 7 в съответствие с параграф 1 подлежат на административно наказание „глоба“ или „имуществена санкция“ в размер до 20 000 000 евро или, в случай на предприятие — до 4 % от общия му годишен световен оборот за предходната финансова година, като се взема по-високата сума:

4. Държавите членки установяват правилата относно санкциите за нарушаване на разпоредбите на членове 12, 13, 14 и 17.

5. Нарушенията на посочените по-долу разпоредби подлежат, в съответствие с параграф 18, на административно наказание „глоба“ или „имуществена санкция“ в размер до 20 000 000 EUR или, в случай на предприятие — до 4 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока:

6. Без да се засягат корективните правомощия на надзорните органи съгласно член 18, всяка държава членка може да определя правила за това дали и до каква степен могат да бъдат налагани административни наказания „глоба“ или „имуществена санкция“ на публични органи и структури, установени в тази държава членка.

7. Упражняването от надзорния орган на правомощията му по настоящия член зависи от съответните процедурни гаранции в съответствие с правото на Съюза и правото на държавата членка, включително ефективна съдебна защита и справедлив съдебен процес.

8. Когато в правната система на държавата членка не са предвидени административни наказания „глоба“ или „имуществена санкция“, настоящият член може да се прилага по такъв начин, че глобата да се инициира от компетентния назорен орган и да се налага от компетентните национални съдилища, като в същото време се гарантира, че тези правни средства за защита са ефективни и имат ефект, равностоен на административните наказания „глоба“ или „имуществена санкция“, налагани от надзорните органи. Във всички случаи наложените глоби или имуществени санкции са ефективни, пропорционални и възпиращи. Посочените държави членки уведомяват Комисията за разпоредбите в правото си, които примат съгласно настоящия параграф, най-късно до [xxx], и я уведомяват незабавно за всеки последващ закон за изменение или за всяко изменение, които ги засягат.

Член 24
Санкции

1. Държавите членки определят правила за други санкции, приложими за нарушения на настоящия регламент, и по-специално за нарушения, които не подлежат на административно наказание „глоба“ или „имуществена санкция“ съгласно член 23, и вземат всички необходими мерки за гарантиране на тяхното прилагане. Тези санкции са ефективни, пропорционални и възпиращи.

2. Всяка държава членка уведомява Комисията за тези разпоредби в своето право, които приема съгласно параграф 1, не по-късно от 18 месеца след датата, посочена в член 29, параграф 2, и я уведомява незабавно за всяко последващо изменение, което ги засяга.

ГЛАВА VI
ДЕЛЕГИРАНИ АКТОВЕ И АКТОВЕ ЗА ИЗПЪЛНЕНИЕ

Член 25
Упражняване на делегираните правомощия

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.

2. Правомощието да приема делегирани актове, посочено в член 8, параграф 4, се предоставя на Комисията за неопределен срок, считано от [датата на влизане в сила на настоящия регламент].

3. Делегирането на правомощия, посочено в член 8, параграф 4, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. Оттеглянето поражда действие в деня след публикуването на решението в Официален вестник на Европейския съюз или на по-късна дата, посочена в решението. То не засяга действителността на делегираните актове, които вече са в сила.

4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 г.

5. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.

6. Делегиран акт, приет съгласно член 8, параграф 4, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца след нотифицирането на акта на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок може да се удължи с два месеца по инициатива на Европейския парламент или на Съвета.

Член 26
Комитет

1. Комисията се подпомага в работата си от Комитета за регулиране на съобщенията, създаден по силата на член 110 от [Директивата за установяване на Европейски кодекс за електронни съобщения]. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011[12].

2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) № 182/2011.

ГЛАВА VII
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 27
Отмяна

1. Директива 2002/58/ЕО се отменя, считано от 25 май 2018 г.

2. Позоваванията на отменената директива се считат за позовавания на настоящия регламент.

Член 28
Клауза за наблюдение и оценка

Най-късно до 1 януари 2018 г. Комисията изготвя подробна програма за наблюдение на ефективността на настоящия регламент.

Не по-късно от три години след влизането в сила на настоящия регламент и на всеки три години след това Комисията прави оценка на регламента и представя основните констатации на Европейския парламент, Съвета и Европейския икономически и социален комитет. Когато е необходимо, оценката съдържа предложение за изменение или отмяна на настоящия регламент с оглед на правното, техническото и икономическото развитие.

[12] Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр.13—18).

Член 29

Влизане в сила и прилагане

1. Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

2. Той се прилага от 25 май 2018 г.

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

Съставено в Брюксел на година.

За Европейския парламент	*За Съвета*
Председател	*Председател*