2024/1773

25.6.2024 г.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2024/1773 НА КОМИСИЯТА

от 13 март 2024 година

за допълнение на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти, с които се доуточнява подробното съдържание на политиката по отношение на договорните споразумения за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 ([1]), и по-специално член 28, параграф 10, третата алинея от него,

като има предвид, че:

(1) Рамката за оперативна устойчивост на цифровите технологии във финансовия сектор, установена с Регламент (ЕС) 2022/2554, изисква финансовите субекти да определят някои основни принципи за управление на риска в областта на ИКТ, пораждан от трета страна, които са особено важни, когато финансовите субекти прибягват до трети страни доставчици на услуги в областта на ИКТ, за да поддържат изпълняваните от тях критични или важни функции.

(2) Като част от своята рамка за управление на риска в областта на ИКТ финансовите субекти трябва да приемат и редовно да преразглеждат стратегия за риска в областта на ИКТ, пораждан от трети страни. В съответствие с член 28, параграф 2 от Регламент (ЕС) 2022/2554 тази стратегия трябва да включва политика за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ. Тя трябва да се прилага както на индивидуална основа, така и, според случая, на подконсолидирана и консолидирана основа.

(3) Финансовите субекти се различават значително по размера, структурата и вътрешната си организация, както и по естеството и сложността на своите дейности и операции. Необходимо е да се вземе предвид това разнообразие, като същевременно при разработването на политиката относно договорните споразумения за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ („политиката“), бъдат наложени определени основни регулаторни изисквания, които са подходящи за всички финансови субекти, както и да се гарантира, че тези изисквания се прилагат по пропорционален начин.

(4) Следователно, когато финансовите субекти са част от група, предприятието майка, което отговаря за предоставянето на консолидираните или подконсолидираните финансови отчети на групата, следва да се увери, че политиката се прилага последователно и съгласувано в рамките на групата.

(5) При прилагането на политиката вътрешногруповите доставчици на услуги в областта на ИКТ, включително изцяло или колективно притежаваните от финансови субекти в рамките на една и съща институционална защитна схема, следва да се смятат за трети страни доставчици на услуги в областта на ИКТ. Рисковете, породени от вътрешногрупови доставчици на услуги в областта на ИКТ, може да са различни, но приложимите за тях изисквания са същите като определените в Регламент (ЕС) 2022/2554. По подобен начин политиката следва да се прилага за подизпълнители, които предоставят услуги в областта на ИКТ, поддържащи критични или важни функции или съществени части от тях, на трети страни доставчици на услуги в областта на ИКТ, когато съществува верига от трети страни доставчици на услуги в областта на ИКТ.

(6) Крайната отговорност на ръководния орган на финансовия субект при управлението на риска в областта на ИКТ е основополагащ принцип, който се прилага и по отношение на използването на трети страни доставчици на услуги в областта на ИКТ. Тази отговорност следва да се превърне в непрекъсната ангажираност на ръководния орган с контрола и наблюдението на управлението на риска в областта на ИКТ, включително с приемането и преразглеждането на политиката най-малко веднъж годишно.

([1]) ОВ L 333, 27.12.2022 г., стр. 1, ELI: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

(7) За да се гарантира подходящо докладване пред ръководния орган, в политиката следва ясно да се уточнят и определят вътрешните отговорности за одобряването, управлението, контрола и документирането на договорните споразумения за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ („договорни споразумения“), включително услугите в областта на ИКТ, предоставяни по договорни споразумения, посочени в член 28, параграф 1, буква а) от Регламент (ЕС) 2022/2554.

(8) За да се вземат предвид всички възможни рискове, които може да възникнат при договарянето на услуги в областта на ИКТ, поддържащи критична или важна функция, е уместно структурата на политиката да следва всички стъпки на всяка основна фаза от жизнения цикъл на договорните споразумения с трети страни доставчици.

(9) С цел да се намалят идентифицираните рискове, в политиката следва да се предвиди планирането на договорните споразумения, включително оценката на риска, надлежната проверка и процедурата за одобряване на нови или съществени промени в тези договорни споразумения. За да се управляват рисковете, които може да възникнат преди сключването на договорно споразумение с трета страна доставчик на услуги в областта на ИКТ, в политиката следва да се уточни подходящ и пропорционален процес на подбор и оценка на пригодността на бъдещите трети страни доставчици на услуги в областта на ИКТ и от финансовия субект да се изисква да взема предвид неизчерпателен списък от елементи, с които третите страни доставчици на услуги в областта на ИКТ трябва да разполагат. Списъкът следва да включва елементи, свързани с бизнес репутацията на доставчиците на услуги, с финансовите, с човешките и с техническите им ресурси, с тяхната информационна сигурност, организационна структура, включително управлението на риска, и с техния вътрешен контрол.

(10) За да се осигури добро управление на риска при предоставянето на услуги в областта на ИКТ, поддържащи критични или важни функции, от трети страни доставчици на услуги в областта на ИКТ, политиката следва да съдържа информация относно изпълнението, наблюдението и управлението на договорните споразумения, включително на консолидирано и подконсолидирано равнище, според случая. Това включва изисквания за договорните клаузи относно взаимните задължения на финансовите субекти и третите страни доставчици на услуги в областта на ИКТ, които следва да бъдат изложени в писмен вид. С цел да се осигури ефективен надзор и да се насърчи устойчивостта в случай на промени в бизнес модела или бизнес средата, в политиката следва да се гарантират правата на финансовите субекти или на определените трети страни и на компетентните органи за проверки и достъп до информация, както и да се доуточнят изходните стратегии и процедурите за прекратяване.

(11) Доколкото личните данни се обработват от трети страни доставчици на услуги в областта на ИКТ, тази политика и всички договорни споразумения не трябва да засягат и следва да допълват задълженията по Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([2]), като например въвеждането на писмен договор, в който се описва обработването на личните данни, изискването за гарантиране на сигурността на обработването на личните данни и определянето на всички други елементи съгласно изискванията на посочения регламент.

([2]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

(12) Съвместният комитет на европейските надзорни органи, посочен в член 54 от Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета ([3]), в член 54 от Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета ([4]) и в член 54 от Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета ([5]), проведе открити обществени консултации по проектите на регулаторни технически стандарти, въз основа на които е изготвен настоящият регламент, анализира потенциалните разходи и ползи от предложените стандарти и поиска мнението на Групата на участниците от банковия сектор, създадена в съответствие с член 37 от Регламент (ЕС) № 1093/2010, Групата на участниците от сектора на застраховането и презастраховането, създадена в съответствие с член 37 от Регламент (ЕС) № 1094/2010, и Групата на участниците от сектора на ценните книжа и пазарите, създадена в съответствие с член 37 от Регламент (ЕС) № 1095/2010.

(13) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([6]) беше проведена консултация с Европейския надзорен орган по защита на данните, който прие становище на 24 януари 2024 г.,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Цялостен рисков профил и сложност

В политиката за използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ („политиката“), се вземат предвид размерът и цялостният рисков профил на финансовия субект, както и естеството, мащабът и елементите на повишена или намалена сложност на неговите услуги, дейности и операции, включително елементите, свързани с:

а) вида на услугите в областта на ИКТ, включени в договорното споразумение относно използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ („договорното споразумение“) между финансовия субект и третата страна доставчик на услуги в областта на ИКТ;

б) мястото на третата страна доставчик на услуги в областта на ИКТ или мястото на нейното предприятие майка;

в) дали услугите в областта на ИКТ, поддържащи критични или важни функции, се предоставят от трета страна доставчик на услуги в областта на ИКТ, намираща се в държава членка или в трета държава, като се има предвид както мястото, от което се предоставят услугите в областта на ИКТ, така и мястото, в което се обработват и съхраняват данните;

г) естеството на данните, споделени с третата страна доставчик на услуги в областта на ИКТ;

д) дали третата страна доставчик на услуги в областта на ИКТ е част от същата група като финансовия субект, на който се предоставят услугите;

([3]) Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 12, ELI: https://eur-lex.europa.eu/eli/reg/2010/1093/oj).

([4]) Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за застраховане и професионално пенсионно осигуряване), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/79/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 48, ELI: https://eur-lex.europa.eu/eli/reg/2010/1094/oj).

([5]) Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за ценни книжа и пазари), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/77/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 84, ELI: https://eur-lex.europa.eu/eli/reg/2010/1095/oj).

([6]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

е) използването на трети страни доставчици на услуги в областта на ИКТ, които са лицензирани, регистрирани или обект на надзор от компетентен орган в държава членка, или са обхванати от надзорната рамка съгласно глава V, раздел II от Регламент (ЕС) 2022/2554, и използването на трети страни доставчици на услуги в областта на ИКТ, които не са;

ж) използването на трети страни доставчици на услуги в областта на ИКТ, които са лицензирани, регистрирани или обект на надзор от компетентен орган в трета държава, и използването на трети страни доставчици на услуги в областта на ИКТ, които не са;

з) дали предоставянето на услуги в областта на ИКТ, поддържащи критични или важни функции, е съсредоточено само в една трета страна доставчик на услуги в областта на ИКТ или в малък брой такива доставчици на услуги;

и) възможността за прехвърляне на услугите в областта на ИКТ, поддържащи критични или важни функции, към друга трета страна доставчик на услуги в областта на ИКТ, включително в резултат на технологични специфики;

й) потенциалното въздействие на смущения в предоставянето на услуги в областта на ИКТ, поддържащи критични или важни функции, върху непрекъснатостта на дейностите на финансовия субект и върху наличността на неговите услуги.

Член 2

Прилагане при група

Когато настоящият регламент се прилага на подконсолидирана или консолидирана основа, предприятието майка, което отговаря за предоставянето на консолидираните или подконсолидираните финансови отчети на групата, гарантира, че политиката се прилага последователно във всички финансови субекти, които са част от групата, и е подходяща за ефективното прилагане на настоящия регламент на всички съответни нива в рамките на групата.

Член 3

Правила за управление

1. Ръководният орган преразглежда политиката поне веднъж годишно и я актуализира, когато е необходимо. Направените промени в политиката се прилагат своевременно и възможно най-скоро в рамките на съответните договорни споразумения. Финансовият субект документира планирания график за прилагането.

2. В политиката се установява или се прави позоваване на методика за определяне на услугите в областта на ИКТ, поддържащи критични или важни функции. Освен това в политиката се посочва кога тази оценка трябва да бъде извършена и преразгледана.

3. В политиката са разпределят ясно вътрешните отговорности за одобряването, управлението, контрола и документирането на съответните договорни споразумения и се гарантира, че финансовият субект поддържа подходящи умения, опит и знания за осъществяване на ефективен надзор на съответните договорни споразумения, включително на услугите в областта на ИКТ, предоставяни съгласно тези договорености.

4. Без да се засяга крайната отговорност на финансовия субект за ефективен надзор на съответните договорни споразумения, в политиката се поставят изисквания за оценка на третата страна доставчик на услуги в областта на ИКТ относно това дали разполага с достатъчно ресурси, за да гарантира спазването от финансовия субект на всички законови и регулаторни изисквания по отношение на предоставяните услуги в областта на ИКТ, поддържащи критични или важни функции.

5. В политиката ясно се определя ролята или членът на висшето ръководство, които отговарят за наблюдението на съответните договорни споразумения. В политиката се уточнява начинът, по който тази роля или този член на висшето ръководство си сътрудничат с функциите за контрол, освен ако не е част от тях, и се определя йерархичната линия на докладване пред ръководния орган, включително естеството на докладваната информация и предоставяните документи. Освен това в нея се посочва и честотата на това докладване.

6. В политиката се гарантира, че договорните споразумения са в съответствие със следното:

а) с рамката за управление на риска в областта на ИКТ, посочена в член 6 от Регламент (ЕС) 2022/2554;

б) с политиката за информационна сигурност, посочена в член 9, параграф 4 от Регламент (ЕС) 2022/2554;

в) с политиката за непрекъснатост на дейността в областта на ИКТ, посочена в член 11 от Регламент (ЕС) 2022/2554;

г) с изискванията за докладване на инциденти, посочени в член 19 от Регламент (ЕС) 2022/2554.

7. В политиката се поставят изисквания услугите в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ, да бъдат предмет на независим преглед и да бъдат включени в одитния план.

8. В политиката се посочва изрично, че договорните споразумения:

а) не освобождават финансовия субект и ръководния му орган от регулаторните му задължения и от отговорностите към клиентите му;

б) не трябва да възпрепятстват ефективния надзор на финансовия субект и да противоречат на надзорните ограничения по отношение на услугите и дейностите;

в) трябва да съдържат изисквания към третите страни доставчици на услуги в областта на ИКТ за сътрудничество с компетентните органи;

г) трябва да съдържат изисквания за ефективен достъп от страна на финансовия субект, неговите одитори и компетентните органи до данните и помещенията, свързани с използването на услугите в областта на ИКТ, поддържащи критични или важни функции.

Член 4

Основни фази от жизнения цикъл за приемането и използването на договорните споразумения

В политиката се определят изискванията, включително правилата, отговорностите и процесите, за всяка основна фаза от жизнения цикъл на договорното споразумение, като се обхваща най-малко следното:

а) отговорностите на ръководния орган, включително участието му, според случая, в процеса на вземане на решения относно използването на услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ;

б) планирането на договорните споразумения, включително оценката на риска, надлежната проверка, както е посочено в членове 5 и 6, и процеса на одобряване по отношение на нови или съществени промени в договорните споразумения, както е посочено в член 8, параграф 4;

в) участието на бизнес звената, вътрешния контрол и други съответни звена по отношение на договорните споразумения;

г) изпълнението, наблюдението и управлението на договорните споразумения, както е посочено в членове 7, 8 и 9, включително на консолидирана и подконсолидирана основа, според случая;

д) документирането и воденето на регистри, като се вземат предвид изискванията по отношение на информационния регистър, посочени в член 28, параграф 3 от Регламент (ЕС) 2022/2554;

е) изходните стратегии и процесите на прекратяване, посочени в член 10.

Член 5

Предварителна оценка на риска

1. Политиката съдържа изискване за определяне на бизнес нуждите на финансовия субект преди сключването на договорно споразумение.

2. Политиката съдържа изискване за извършване на оценка на риска на равнище финансов субект и когато е приложимо, на консолидирано и подконсолидирано равнище, преди да бъде сключено договорно споразумение.

При оценката на риска се вземат предвид всички съответни изисквания, установени в Регламент (ЕС) 2022/2554 и приложимото секторно законодателство на Съюза. В нея се разглеждат по-специално въздействието върху финансовия субект на предоставянето на услуги в областта на ИКТ, поддържащи критични или важни функции, от трети страни доставчици на услуги в областта на ИКТ, както и всички рискове, свързани с предоставянето на тези услуги в областта на ИКТ, поддържащи критични или важни функции, от трети страни доставчици на услуги в областта на ИКТ, включително следното:

а) операционни рискове;

б) правни рискове;

в) рискове в областта на ИКТ;

г) репутационни рискове;

д) рискове, свързани със защитата на поверителни или лични данни;

е) рискове, свързани с наличието на данни;

ж) рискове, свързани с мястото, където се обработват и съхраняват данните;

з) рискове, свързани с мястото на третата страна доставчик на услуги в областта на ИКТ;

и) рискове от концентрация на ИКТ на равнище субект.

Член 6

Надлежна проверка

1. В политиката се определя подходящ и пропорционален процес на подбор и оценка на бъдещите трети страни доставчици на услуги в областта на ИКТ, като се взема предвид дали третата страна доставчик на услуги в областта на ИКТ е вътрешногрупов доставчик на услуги в областта на ИКТ, или не, а от финансовия субект се изисква да оцени, преди сключването на договорно споразумение, дали третата страна доставчик на услуги в областта на ИКТ:

а) има бизнес репутацията, достатъчни способности, експертен опит и подходящи финансови, човешки и технически ресурси, стандарти за информационна сигурност, подходяща организационна структура, управление на риска и вътрешен контрол, и ако е приложимо, необходимите разрешения или регистрации за предоставяне на услуги в областта на ИКТ, поддържащи критичната или важната функция по надежден и професионален начин;

б) има способността да наблюдава съответните технологични разработки и да идентифицира водещи практики за сигурност в областта на ИКТ и да ги прилага, когато е подходящо, за да разполага с ефективна и стабилна рамка за оперативна устойчивост на цифровите технологии;

в) използва или възнамерява да използва подизпълнители в областта на ИКТ за извършване на услуги в областта на ИКТ, поддържащи критични или важни функции или съществени части от тях;

г) се намира в трета държава, или обработва или съхранява данните в трета държава, и ако това е така, дали тази практика засяга нивото на оперативния или репутационния риск или риска от това да бъде засегната от ограничителни мерки, включително ембарго и санкции, които могат да повлияят на способността на третата страна доставчик на услуги в областта на ИКТ да предоставя услугите в областта на ИКТ или на финансовия субект да получава тези услуги в областта на ИКТ;

д) дава съгласието си за сключване на договорни споразумения, в които се гарантира, че е действително възможно да се извършват одити на третата страна доставчик на услуги в областта на ИКТ, включително на място, от самия финансов субект, от определени трети страни и от компетентните органи;

е) действа по етичен и социално отговорен начин, зачита човешките права и правата на децата, включително забраната на детския труд, зачита приложимите принципи за опазване на околната среда и осигурява подходящи условия на труд.

2. В политиката се определя необходимото ниво на сигурност по отношение на ефективността на рамката за управление на риска на трети страни доставчици на услуги в областта на ИКТ за услугите в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трета страна доставчик на услуги в областта на ИКТ. В политиката се изисква процесът на надлежна проверка да включва оценка на наличието на мерки за намаляване на риска и непрекъснатост на дейността и как се осигурява тяхното функциониране в рамките на третата страна доставчик на услуги в областта на ИКТ.

3. В политиката се определя процесът на надлежна проверка за подбор и оценка на бъдещите трети страни доставчици на услуги в областта на ИКТ и се посочва кои от следните елементи трябва да се използват за изискваното ниво на сигурност относно ефективността на третата страна доставчик на услуги в областта на ИКТ:

а) одити или независими оценки, извършвани от самия финансов субект или от негово име;

б) използване на независими одитни доклади, изготвени по искане на третата страна доставчик на услуги в областта на ИКТ;

в) използване на одитни доклади, изготвяни от функцията за вътрешен одит на третата страна доставчик на услуги в областта на ИКТ;

г) използване на подходящи удостоверения на трети страни;

д) използване на друга съответна информация, достъпна за финансовия субект, или друга информация, предоставяна от третата страна доставчик на услуги в областта на ИКТ.

4. Финансовите субекти осигуряват подходящо ниво на увереност относно ефективността на третата страна доставчик на услуги в областта на ИКТ, като вземат предвид елементите, изброени в параграф 3, букви а)—д). Когато е целесъобразно, се използва повече от един елемент, изброен в тези букви.

Член 7

Конфликти на интереси

1. В политиката се посочват подходящите мерки за идентифициране, предотвратяване и управление на действителни или потенциални конфликти на интереси, произтичащи от използването на трети страни доставчици на услуги в областта на ИКТ, които трябва да бъдат предприети преди сключването на съответните договорни споразумения, и се предвижда текущо наблюдение на такива конфликти на интереси.

2. Когато услугите в областта на ИКТ, поддържащи критични или важни функции, се предоставят от вътрешногрупови доставчици на услуги в областта на ИКТ, в политиката се посочва, че решенията относно условията, включително финансовите условия, за услугите в областта на ИКТ трябва да се вземат обективно.

Член 8

Договорни клаузи

1. В политиката се посочва, че съответното договорно споразумение трябва да бъде в писмена форма и да включва всички елементи, посочени в член 30, параграфи 2 и 3 от Регламент (ЕС) 2022/2554. Политиката включва също така елементи, свързани с изискванията, посочени в член 1, параграф 1, буква а) от Регламент (ЕС) 2022/2554, както и други съответни разпоредби на правото на Съюза и на националното право.

2. В политиката се посочва, че съответните договорни споразумения трябва да включват правото на финансовия субект на достъп до информация, да извършва проверки и одити, както и тестове на ИКТ. За тази цел в политиката се изисква финансовият субект да използва следните методи, без да се засяга крайната отговорност на финансовия субект:

а) собствения си вътрешен одит или одит от определена за целта трета страна;

б) когато е целесъобразно, съвкупни одити и съвкупни тестове на ИКТ, включително тестове за проникване, които се организират съвместно с други финансови субекти или фирми възложители, които използват услуги в областта на ИКТ на същата трета страна доставчик на услуги в областта на ИКТ, и които се извършват от тези финансови субекти или фирми възложители или от определена от тях за целта трета страна;

в) когато е целесъобразно, използването на удостоверения на трети страни;

г) когато е целесъобразно, вътрешни одитни доклади или одитни доклади на трета страна, предоставени от третата страна доставчик на услуги в областта на ИКТ.

3. С течение на времето финансовият субект не може да се позовава единствено на удостоверенията, посочени в параграф 2, буква в), или на одитните доклади, посочени в буква г) от същия параграф. В политиката се разрешава единствено използването на методите, посочени в параграф 2, букви в) и г), като финансовият субект:

а) е удовлетворен от плана за одит на третата страна доставчик на услуги в областта на ИКТ по отношение на съответните договорни споразумения;

б) гарантира, че обхватът на удостоверенията или одитните доклади включва идентифицираните от него системи и ключови контролни механизми и осигурява спазването на съответните регулаторни изисквания;

в) извършва задълбочена текуща оценка на съдържанието на удостоверенията или одитните доклади и проверява дали докладите или удостоверенията не са остарели;

г) гарантира, че ключовите системи и контролни механизми са обхванати в бъдещите версии на удостоверенията или одитните доклади;

д) е удовлетворен от компетентността на издаващата удостоверенията страна или на одитната страна;

е) е удовлетворен, че удостоверенията са издадени и одитите са извършени съгласно общопризнати съответни професионални стандарти и включват тест за оперативна ефективност на ключовите контролни механизми;

ж) има договорното право да изисква, с честота, която е разумна и законна от гледна точка на управлението на риска, промени в обхвата на удостоверенията или одитните доклади спрямо други съответни системи и контролни механизми;

з) има договорното право да извършва индивидуални и съвкупни одити по свое усмотрение по отношение на договорните споразумения и да упражнява тези права в съответствие с договорената честота.

4. В политиката се гарантира, че съществените промени в договорното споразумение ще бъдат формализирани в писмен документ, върху който всяка страна поставя дата и подпис, и се уточнява процесът на подновяване на договорните споразумения.

Член 9

Наблюдение на договорните споразумения

1. В политиката се поставят изисквания договорните споразумения да съдържат мерките и ключовите показатели за текущо наблюдение на ефективността на третите страни доставчици на услуги в областта на ИКТ, включително мерки за наблюдение на спазването на изискванията по отношение на поверителността, наличността, целостта и автентичността на данните и информацията и съответствието на третите страни доставчици на услуги в областта на ИКТ със съответните политики и процедури на финансовия субект. В политиката също така се определят мерките, които да се прилагат, когато споразуменията за ниво на обслужване не се спазват, включително договорни неустойки, когато е необходимо.

2. В политиката се посочва как финансовият субект трябва да оценява дали третите страни доставчици на услуги в областта на ИКТ, използвани за услугите в областта на ИКТ, поддържащи критични или важни функции, отговарят на подходящи стандарти за ефективност и качество в съответствие с договорното споразумение и собствените политики на финансовия субект. В политиката се гарантира по-специално следното:

а) че третите страни доставчици на услуги в областта на ИКТ предоставят на финансовия субект подходящи доклади за своите дейности и услуги, включително периодични доклади, доклади за инциденти, доклади за предоставянето на услуги, доклади за сигурността на ИКТ и доклади за мерките и тестовете за непрекъснатост на дейността;

б) че ефективността на третите страни доставчици на услуги в областта на ИКТ се оценява с ключови показатели за ефективност, ключови показатели за контрол, одити, декларации и независими прегледи в съответствие с рамката на финансовия субект за управление на риска в областта на ИКТ;

в) че финансовият субект получава друга подходяща информация от третите страни доставчици на услуги в областта на ИКТ;

г) че финансовият субект бива уведомяван, когато е уместно, за инциденти, свързани с ИКТ, и инциденти, свързани с оперативната дейност или със сигурността на плащанията;

д) че се извършват независими прегледи и одити за проверка на спазването на законовите и регулаторните изисквания и политики.

3. В политиката се предвижда, че оценката, посочена в параграф 2, трябва да бъде документирана и резултатите от нея да се използват за актуализиране на оценката на риска на финансовия субект, посочена в член 6.

4. В политиката се определят подходящите мерки, които финансовият субект трябва да предприеме, ако установи недостатъци на третите страни доставчици на услуги в областта на ИКТ, включително инциденти, свързани с ИКТ, и инциденти, свързани с оперативната дейност или със сигурността на плащанията, при предоставянето на услуги в областта на ИКТ, поддържащи критични или важни функции, или при спазването на договорни споразумения или законови изисквания. В нея се посочва също така как да се наблюдава изпълнението на тези мерки, за да се гарантира, че те се спазват ефективно в рамките на определен срок, като се отчита съществеността на недостатъците.

Член 10

Излизане от и прекратяване на договорните споразумения

Политиката съдържа изисквания за документиран изходен план за всяко договорно споразумение и за периодичен преглед и тестване на документирания изходен план. При съставянето на изходния план се взема предвид следното:

а) непредвидени и системни прекъсвания на услугата;

б) неподходящо или неуспешно предоставяне на услугата;

в) неочаквано прекратяване на договорното споразумение.

Изходният план трябва да бъде реалистичен, изпълним, основан на правдоподобни сценарии и разумни допускания и да има планиран график за изпълнение, съвместим с условията за излизане и прекратяване, определени в договорните споразумения.

Член 11

Влизане в сила

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

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

Съставено в Брюксел на 13 март 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN