EIOPA-BoS-20-002

Насоки за възлагане на дейности на доставчици на облачни услуги

Съдържание

Въведение 3
Определения 4
Дата на прилагане 4
Насока 1 — Облачни услуги и възлагане на дейности на външни изпълнители 6
Насока 2 — Общи принципи на управление при възлагане 6
на облачни услуги на външни доставчици 6
Насока 3 — Актуализиране на писмената политика за възлагане на дейности на външни изпълнители 7
Насока 4 — Писмено уведомление до надзорния орган 7
Насока 5 — Изисквания относно документацията 8
Насока 6 — Анализ преди възлагането на дейности на външни изпълнители 9
Насока 7 — Оценка на критични или важни оперативни функции и дейности 9
Насока 8 — Оценка на риска във връзка с възлагането на облачни услуги на външни доставчици 11
Насока 9 — Надлежна проверка на доставчик на облачни услуги 12
Насока 10 — Договорни изисквания 13
Насока 11 — Права на достъп и одит 14
Насока 12 — Сигурност на данните и системите 16
Насока 13 — Възлагане на подизпълнител на критични или важни оперативни функции или дейности 17
Насока 14 — Наблюдение и надзор върху споразумения за възлагане на облачни услуги на външни доставчици 17
Насока 15 — Права на прекратяване и стратегии за изход 18
Насока 16 — Надзор от надзорни органи върху споразумения за възлагане на облачни услуги на външни доставчици 19
Правила за нормативно съответствие и за докладване 20
Заключителна разпоредба относно преразглежданията 20

Въведение

1. В съответствие с член 16 от Регламент (ЕС) № 1094/2010[1] EIOPA (Европейски орган за застраховане и професионално пенсионно осигуряване) издава насоки за предоставяне на напътствия на застрахователните и презастрахователните дружества относно начина, по който следва да се прилагат разпоредбите за възлагане на дейности на външни изпълнители, посочени в Директива 2009/138/ЕО[2] (директива „Платежоспособност II") и в Делегиран регламент (ЕС) № 2015/35 на Комисията [3] („делегиран регламент") в случай на възлагане на дейности на доставчици на облачни услуги.

2. Настоящите насоки се основават на членове 13 (28), 38 и 49 от директива „Платежоспособност II" и член 274 от делегирания регламент. Освен това настоящите насоки се основават и на напътствията, предоставени от Насоките на EIOPA за системата на управление (EIOPA-BoS-14/253).

3. Настоящите насоки са предназначени за компетентните органи, за да предоставят напътствия за това как застрахователните и презастрахователните дружества (нарични заедно „предприятие (а)") следва да прилагат изискванията за възлагане на дейности на външни изпълнители, предвидени в посочените по-горе правни актове в контекста на възлагането на дейности на доставчици на облачни услуги.

4. Насоките се прилагат както към отделни дружества, така и *mutatis mutandis* към групи[4].

   Субектите, подлежащи на други секторни изисквания, които са част от група, са изключени от обхвата на настоящите насоки на индивидуално равнище, тъй като те трябва да следват специфичните за отделните сектори изисквания, както и съответните насоки, издадени от Европейския орган за ценни книжа и пазари и Европейския банков орган.

5. В случай на възлагане на дейности в рамките на групата и възлагане за подизпълнение на доставчици на облачни услуги, настоящите насоки следва да се прилагат във връзка с разпоредбите на Насоките на EIOPA за системата на управление относно възлагане на дейности на външни изпълнители в рамките на групата.

6. Когато спазват или упражняват надзор върху спазването на настоящите насоки, дружествата и компетентните органи следва да вземат предвид принципа на пропорционалност[5] и критичността или важността на услугата, възлагана на доставчиците на облачни услуги. Принципът на пропорционалност следва да гарантира, че правилата за управление, включително тези, свързани с възлагането на доставчици на облачни услуги, са пропорционални на естеството, мащаба и сложността на базовите рискове.

---

[1] 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).

[2] Директива 2009/138/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. относно започването и упражняването на застрахователна и презастрахователна дейност (Платежоспособност II), (ОВ L 335, 17.12.2009 г., стр. 1).

[3] Делегиран регламент (ЕС) № 2015/35 на Комисията от 10 октомври 2014 г. за допълнение на Директива 2009/138/ЕО на Европейския парламент и на Съвета относно започването и упражняването на застрахователна и презастрахователна дейност (Платежоспособност II) (ОВ L 12, 17.1.2015 г., стр. 1).

[4] Член 212, параграф 1 от директива „Платежоспособност II".

[5] Член 29, параграф 3 от директива „Платежоспособност II".

7. Настоящите насоки следва да се разглеждат във връзка със и без да се засягат Насоките на EIOPA за системата на управление и регулаторните задължения, изброени в параграф 1.

Определения

8. В случай че в насоките не е указано друго, термините имат значението, дефинирано в посочените във въведението правни актове.

9. В допълнение, за целите на настоящите насоки се прилагат следните определения:

Доставчик на услуга	означава субект трета страна, който извършва процес, услуга или дейност или части от тях по силата на споразумение за възлагане на дейности на външни изпълнители.
Доставчик на облачни услуги	означава доставчик на услуга, съгласно определението по-горе, който е отговорен за доставянето на облачни услуги по силата на споразумение за възлагане на дейности на външни изпълнители.
Облачни услуги	означава услуги, предоставяни чрез обработка на данни в облачно пространство, а именно — модел за реализиране на повсеместен, удобен мрежов достъп по заявка до споделен набор от изчислителни ресурси с възможност за конфигуриране (напр. мрежи, сървъри, хранилища, приложения и услуги), които бързо могат да бъдат обезпечавани и реализирани с минимални усилия за управление или взаимодействие с доставчика на услуги.
Публично облачно пространство	означава инфраструктура за облачни услуги, която може открито да се използва от широката общественост.
Частно облачно пространство	означава инфраструктура за облачни услуги, която може да се използва само от едно предприятие.
Общностно облачно пространство	означава инфраструктура за облачни услуги, която може да се използва само от конкретна общност от дружества, включително няколко дружества, принадлежащи към една група.
Хибридно облачно пространство	означава инфраструктура за облачни услуги, която е съставена от две или повече обособени инфраструктури за облачни услуги.

Дата на прилагане

10. Настоящите насоки се прилагат от 1 януари 2021 г. спрямо всички споразумения за възлагане на облачни услуги на външни доставчици, сключени или изменени на или след тази дата.

11. Дружествата следва да преразгледат и изменят съответно съществуващите споразумения за възлагане на облачни услуги на външни доставчици, свързани с критични или важни оперативни функции или дейности, с цел да се гарантира спазването на настоящите насоки до 31 декември 2022 г.

12. Ако до 31 декември 2022 г. не бъде приключен прегледът на споразуменията за възлагане на облачни услуги на външни доставчици, свързани с критични или важни оперативни функции или дейности, дружествата следва да информират своя надзорен орган[6] за този факт, включително за планираните мерки за приключване на прегледа или на евентуалната стратегия за изход. Надзорният орган може да се договори с предприятието за удължен срок за завършване на този преглед, когато това е целесъобразно.

13. Актуализирането (когато е необходимо) на политиките и вътрешните процедури на предприятието следва да бъде извършено до 1 януари 2021 г., а изискванията относно документацията за споразуменията за възлагане на облачни услуги на външни доставчици, свързани с критични или важни оперативни функции или дейности, следва да бъдат изпълнени до 31 декември 2022 г.

[6] Член 13, параграф 10 от директива „Платежоспособност II".

Насока 1 — Облачни услуги и възлагане на дейности на външни изпълнители

14. Дружеството следва да установи дали споразумение с доставчик на облачни услуги попада в обхвата на определението за възлагане на дейности на външни изпълнители съгласно директива „Платежоспособност II". В рамките на оценката следва да се вземе предвид:

a. дали оперативната функция или дейност (или част от нея), която се възлага на външен изпълнител, се извършва периодично или постоянно;

b. дали тази оперативна функция или дейност (или част от нея) обикновено попада в обхвата на оперативните функции или дейности, които предприятието би или би могло да осъществява в хода на обичайната си стопанска дейност, дори ако предприятието не е осъществявало тази оперативна функция или дейност в миналото.

15. Когато споразумение с доставчик на услуги обхваща множество оперативни функции или дейности, предприятието следва да вземе предвид всички аспекти на споразумението в рамките на своята оценка.

16. В случаите, когато предприятието възлага оперативни функции или дейности на доставчици на услуги, които не са доставчици на облачни услуги, но разчитат в значителна степен на инфраструктурата за облачни услуги, за да предоставят услугите си (напр. когато доставчикът на облачни услуги е част от верига от подизпълнители), споразумението за подобно възлагане на дейности на външни изпълнители попада в обхвата на настоящите насоки.

Насока 2 — Общи принципи на управление при възлагане

на облачни услуги на външни доставчици

17. Без да се засяга член 274, параграф 3 от делегирания регламент, административният, управителният или надзорният орган на предприятието („АУНО") следва да гарантира, че всяко решение за възлагане на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги се основава на задълбочена оценка на риска, включваща всички съответни рискове, произтичащи от споразумението, като информационни и комуникационни технологии („ИКТ"), непрекъснатост на стопанската дейност, правни рискове и рискове, свързани със спазване на изискванията, рискове от концентрация, други оперативни рискове и рискове, свързани с миграцията на данните и/или етапа на изпълнение, когато е приложимо.

18. В случай на възлагане на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги, когато е целесъобразно, предприятието следва да отрази в своята собствена оценка на риска и платежоспособността („СОРП") промените в рисковия си профил, които се дължат на сключените от него споразумения за възлагане на облачни услуги на външни доставчици.

19. Използването на облачни услуги следва да бъде в съответствие със стратегиите на предприятието (напр. стратегия в областта на ИКТ, стратегия за информационна сигурност, стратегия за управление на операционния риск) и с вътрешните политики и процеси, които при необходимост следва да бъдат актуализирани.

Насока 3 — Актуализиране на писмената политика за възлагане на дейности на външни изпълнители

20. В случай на възлагане на външни доставчици на облачни услуги, предприятието следва да актуализира писмената политика за възлагане на дейности на външни изпълнители (напр. чрез извършване на преглед на същата, добавяне на отделно приложение или разработване на нови специални политики) и другите съответни вътрешни политики (напр. за информационната сигурност), като се вземат предвид спецификите на възлагането на облачни услуги на външни доставчици най-малко в следните области:

a. ролите и отговорностите на съответните функции на предприятието, по-специално АУНО и функциите, отговарящи за ИКТ, информационната сигурност, спазването на изискванията, управлението на риска и вътрешния одит;

b. процесите и отчетните процедури, необходими за одобряване, изпълнение, наблюдение, управление и подновяване, когато е приложимо, на споразуменията за възлагане на облачни услуги на външни доставчици, свързани с критични или важни оперативни функции или дейности;

c. надзорът върху облачните услуги в съответствие с естеството, мащаба и сложността на рисковете, присъщи на предоставяните услуги, включително i) оценка на риска във връзка със споразуменията за възлагане на облачни услуги на външни доставчици и надлежна проверка на доставчиците на облачни услуги, включително честотата на оценката на риска; ii) наблюдение и контрол върху управлението (напр. проверка на споразумението за нивото на услугите); iii) стандарти и проверки за сигурност;

d. по отношение на възлагането на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги следва да се направи позоваване на договорните изисквания, описани в насока 10;

e. изисквания относно документацията и писмено уведомление до надзорния орган във връзка с възлагането на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги;

f. по отношение на всяко споразумение за възлагане на облачни услуги на външни доставчици, което обхваща критични или важни оперативни функции или дейности, изискване за документирана и, когато е целесъобразно, изпитана в достатъчна степен „стратегия за изход", която е пропорционална на естеството, мащаба и сложността на рисковете, присъщи на предоставяните услуги. Стратегията за изход може да включва набор от процеси за прекратяване, включващи, но не непременно ограничаващи се до прекратяване, реинтеграция или прехвърляне на услугите, включени в споразумението за възлагане на облачни услуги на външни доставчици.

Насока 4 — Писмено уведомление до надзорния орган

21. Изискванията за писмено уведомление, определени в член 49, параграф 3 от директива „Платежоспособност II" и по-подробно изложени в Насоките на EIOPA за системата на управление, са приложими спрямо всяко възлагане на критични или важни оперативни функции и дейности на външни доставчици на облачни услуги. В случай че дадена оперативна функция или дейност, възложена на външен изпълнител, която преди това е била класифицирана като некритична

или неважна стане критична или важна, предприятието следва да уведоми надзорния орган за това.

22. В писменото уведомление от предприятието следва да се съдържа, с оглед на принципа на пропорционалност, най-малко следната информация:

a. кратко описание на възложената на външен изпълнител оперативна функция или дейност;

b. началната дата и, ако е целесъобразно, следващата дата на подновяване на договора, крайната дата и/или периодите на предизвестие за доставчика на облачни услуги и за предприятието;

c. приложимото право към споразумението за възлагане на облачни услуги на външни доставчици;

d. името на доставчика на облачни услуги, регистрационен номер, с който той е вписан в търговския регистър, идентификационен код на правния субект (ако има такъв), седалище и други относими данни за контакт, както и наименованието на неговото дружество майка (ако има такова); в случай на групи, информация за това дали доставчикът на облачни услуги е част от групата или не;

e. облачните услугиа и моделите на функциониране на облачната среда (т.е. публични/частни/хибридни/общностни) и специфичното естество на данните, които трябва да се съхраняват, и местоположението (т.е. държави или региони), където ще се съхраняват такива данни;

f. кратко обобщение на причините, поради които възложената на външен изпълнител функция или дейност се счита за критична или важна;

g. датата на последната оценка на критичността или важността на възложената на външен изпълнител функция или дейност.

Насока 5 — Изисквания относно документацията

23. Като част от своята система на управление и управление на риска предприятието следва да документира своите споразумения за възлагане на облачни услуги на външни доставчици, например под формата на специален регистър, който се актуализира с течение на времето. Предприятието следва също така да води регистър на прекратените споразумения за възлагане на облачни услуги на външни доставчици, който да се съхранява за подходящ период от време, при спазване на националните разпоредби.

24. В случай на възлагане на критични или важни оперативни функции или дейности предприятието следва да документира цялата посочена по-долу информация:

a. информацията, за която следва да бъде уведомяван надзорният орган, посочена в насока 4;

b. в случай на групи, застрахователните или презастрахователните дружества и други дружества, попадащи в обхвата на пруденциалната консолидация, които използват облачните услуги;

c. датата на последната оценка на риска и кратко обобщение на основните резултати;

d. лицето или органът за вземане на решения (напр. АУНО) в предприятието, което е одобрило споразумението за възлагане на облачни услуги на външни доставчици;

e. датите на последните и следващите планирани одити, ако е приложимо;

f. имената на всички подизпълнители, на които са възложени за подизпълнение съществени части от критична или важна оперативна функция или дейност, включително държавите, в които са регистрирани подизпълнителите, в които ще се извършва услугата и, ако е приложимо, местоположенията (т.е. държавите или регионите), където ще се съхраняват данните;

g. резултат от оценката на заменяемостта на доставчика на облачни услуги (напр. лесна, трудна или невъзможна);

h. дали възложената на външни изпълнители критична или важна оперативна функция или дейност подпомага бизнес операции, които са критични по отношение на бързината на изпълнение;

i. прогнозните годишни бюджетни разходи;

j. дали предприятието има стратегия за изход в случай на прекратяване от която и да е страна или нарушаване на предоставянето на услугите от доставчика на облачни услуги.

25. В случай на възлагане на външни изпълнители на некритични или незначими оперативни функции или дейности предприятието следва да определи информацията, която следва да се документира въз основа на естеството, мащаба и сложността на рисковете, присъщи на услугите, предоставяни от доставчика на облачни услуги.

26. При поискване предприятието следва да предоставя на надзорния орган цялата информация, необходима за упражняване на надзор върху предприятието, включително копие от споразумението за възлагане на дейности на външни изпълнители.

Насока 6 — Анализ преди възлагането на дейности на външни изпълнители

27. Преди да сключи каквото и да било споразумение с доставчиците на облачни услуги, предприятието следва:

a. да прецени дали споразумението за възлагане на облачни услуги на външни доставчици се отнася за критична или важна оперативна функция или дейност в съответствие с насока 7;

b. да идентифицира и оцени всички относими рискове, свързани със споразумението за възлагане на облачни услуги на външни доставчици в съответствие с насока 8;

c. да извърши подходяща надлежна проверка на потенциалния доставчик на облачни услуги в съответствие с насока 9;

d. да установява и оценява конфликти на интереси, до които може да доведе възлагането на дейности на външни изпълнители съгласно изискванията на член 274, параграф 3, буква б) от делегирания регламент.

Насока 7 — Оценка на критични или важни оперативни функции и дейности

28. Преди сключването на каквото и да било споразумение за възлагане на дейности на външни изпълнители с доставчиците на облачни услуги, предприятието следва да прецени дали споразумението за възлагане на облачни услуги на външни доставчици е свързано с оперативна функция или

дейност, която е критична или важна. При извършването на такава оценка, когато е уместно, предприятието следва да обмисли дали споразумението има потенциала да стане критично или важно в бъдеще. Предприятието следва също така да извърши повторна оценка на критичността или значението на оперативната функция или дейност, която преди това е била възложена на доставчиците на облачни услуги, ако естеството, мащабът и сложността на рисковете, присъщи на споразумението се променят съществено.

29. При оценката предприятието следва да вземе под внимание най-малко следните фактори, заедно с резултата от оценката на риска:

a. потенциалното въздействие на всяко съществено прекъсване на възложената на външен изпълнител оперативна функция или дейност или невъзможността на доставчика на облачни услуги да предоставя услугите на договорените нива на обслужване върху:

   i. непрекъснатото спазване от предприятието на неговите регулаторни задължения;

   ii. краткосрочната и дългосрочната устойчивост и жизнеспособност на финансовите пазари и платежоспособност на предприятието;

   iii. непрекъснатостта на стопанските дейности и оперативната устойчивост на предприятието;

   iv. операционния риск на предприятието, включително поведенческия риск, риска, свързан с ИКТ и правния риск;

   v. рисковете, свързани с репутацията на предприятието.

b. потенциалното въздействие на споразумението за възлагане на облачни услуги на външни доставчици върху способността на предприятието да:

   i. идентифицира, наблюдава и управлява всички относими рискове;

   ii. да спазват всички правни и регулаторни изисквания;

   iii. да провежда подходящи одити във връзка с възложената на външни изпълнители оперативна функция или дейност;

c. общата експозиция на предприятието (и/или на групата, когато е приложимо) към един и същ доставчик на облачни услуги и потенциалното кумулативно въздействие на споразуменията за възлагане на дейности на външни изпълнители в една и съща сфера на дейност;

d. размера и сложността на която и да било сфера на дейност на предприятието, засегнати от споразумението за възлагане на облачни услуги на външни доставчици;

e. способността, ако е необходимо или желателно, да се прехвърли предложеното споразумение за възлагане на облачни услуги на външни доставчици на друг доставчик на облачни услуги или да се реинтегрират услугите („заменяемост“);

f. защитата на личните и неличните данни и потенциалното въздействие върху предприятието, притежателите на полици или други съответни субекти на нарушение на поверителност или липса на гаранции за наличието и целостта на данните въз основа, *inter alia*, на Регламент (ЕС)

2016/679[7]. Предприятието следва по-специално да вземе предвид данни, които представляват търговска тайна и/или чувствителна информация (напр. данни за здравословното състояние на притежателите на полици).

Насока 8 — Оценка на риска във връзка с възлагането на облачни услуги на външни доставчици

30. По принцип предприятието следва да възприеме подход, пропорционален на естеството, мащаба и сложността на рисковете, присъщи на услугите, възложени на доставчици на облачни услуги. Това включва оценка на потенциалното въздействие на възлагането на облачни услуги на външни доставчици, по-специално върху техните операционни и свързани с репутацията рискове.

31. При възлагане на критични или важни оперативни функции или дейности на доставчици на облачни услуги, предприятието следва:

a. да отчита очакваните ползи от и разходи, свързани с предложеното споразумение за възлагане на облачни услуги на външни доставчици, включително да претегля всички значителни рискове, които могат да бъдат намалени или по-добре управлявани спрямо всички значителни рискове, които могат да възникнат в резултат на предложеното споразумение за възлагане на облачни услуги на външни доставчици.

b. да оценява, където е приложимо и целесъобразно, рисковете, включително правните рискове, рисковете, свързани с ИКТ, рисковете, свързани със спазването на изискванията и репутацията, както и ограниченията по отношение на надзора, произтичащи от:

   i. избраната облачна услуга и моделите на функциониране на облачната среда (т.е. публични/частни/хибридни/общностни);

   ii. миграцията и/или изпълнението;

   iii. дейностите и свързаните с тях данни и системи, за които се обмисля да бъдат възложени на външни изпълнители (или са възложени на външни изпълнители), както и тяхната чувствителност и необходимите мерки за сигурност;

   iv. политическата стабилност и положението със сигурността на държавите (в рамките на ЕС или извън него), в които възложените на външен изпълнител услуги се предоставят или могат да се предоставят и в които данните се съхраняват или е вероятно да се съхраняват. При оценката следва да се вземат предвид:

      1. действащото законодателство, включително законите за защита на данните;

      2. действащите разпоредби относно принудителното изпълнение;

      3. правните разпоредби в областта на несъстоятелността, които биха били приложими в случай на неизпълнение на задълженията на доставчик на услуги и всички ограничения, които биха възникнали във връзка със спешното възстановяване на данните на предприятието;

[7] 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).

v. възлагането на подизпълнители, включително допълнителните рискове, които могат да възникнат, ако подизпълнителят е разположен в трета държава или в различна държава от доставчика на облачни услуги, както и риска, свързан с това че дългите и сложни вериги от подизпълнители намаляват способността на предприятието да наблюдава своите критични или важни оперативни функции или дейности и способността на надзорните органи да упражняват ефективен надзор върху тях;

vi. цялостния риск от концентрация на предприятието спрямо един и същ доставчик на облачни услуги, включително възлагане на външен доставчик на облачни услуги, който не е лесно взаимозаменяем или множество споразумения за възлагане на дейности на външни изпълнители с един и същ доставчик на облачни услуги. При оценката на риска от концентрация предприятието (и/или групата, когато е приложимо) следва да вземе предвид всички свои споразумения за възлагане на облачни услуги на външни доставчици с този доставчик на облачни услуги.

32. Оценката на риска следва да бъде извършена преди да се пристъпи към възлагане на облачни услуги на външни доставчици. Ако предприятието узнае за значителни неизправности и/или значителни промени в предоставените услуги или в положението на доставчика на облачни услуги, оценката на риска следва да бъде незабавно преразгледана или повторно извършена. В случай на подновяване на споразумение за възлагане на облачни услуги на външни доставчици по отношение на неговите съдържание и приложно поле (напр. разширяване на приложното поле или включване в приложното поле на критични или важни оперативни функции, които преди това не са били включени), оценката на риска следва да бъде повторно извършена.

Насока 9 — Надлежна проверка на доставчик на облачни услуги

33. Дружеството следва да гарантира в своя процес на подбор и оценка, че доставчикът на облачни услуги е подходящ съгласно критериите, определени в неговата писмена политика за възлагане на дейности на външни изпълнители.

34. Надлежната проверка на доставчика на облачни услуги следва да се извършва преди възлагането на която и да било оперативна функция или дейност. В случай че предприятието сключи второ споразумение с доставчик на облачни услуги, което вече е било оценено, предприятието следва да определи, при основан на риска подход, дали е необходима втора надлежна проверка. Ако предприятието узнае за значителни неизправности и/или значителни промени в предоставените услуги или в положението на доставчика на облачни услуги, надлежната проверка следва да бъде незабавно преразгледана или повторно извършена.

35. В случай на възлагане на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги надлежната проверка следва да включва оценка на пригодността на доставчика на облачни услуги (напр. умения, инфраструктура, икономическо положение, корпоративно и регулаторно състояние). Когато е целесъобразно, в подкрепа на извършените надлежни проверки предприятието може да използва доказателства, удостоверения въз основа на международни стандарти, одитни доклади на признати трети страни или доклади за вътрешен одит.

Насока 10 — Договорни изисквания

36. Съответните права и задължения на предприятието и на доставчика на облачни услуги се разпределят ясно и се излагат в писмено споразумение.

37. Без да се засягат изискванията, определени в член 274 от делегирания регламент, при възлагане на критични или важни оперативни функции или дейности на външен доставчик на облачни услуги, в писменото споразумение между предприятието и доставчика на облачни услуги следва да се съдържат:

a. кратко описание на възложената функция, която ще бъде осъществена (облачни услуги, включително и вида на помощните услуги);

b. началната и крайната дата, ако е приложимо, на споразумението и сроковете на предизвестие за доставчика на облачни услуги и за предприятието;

c. компетентността на съдилищата и приложимото право към споразумението;

d. финансовите задължения на страните;

e. дали е разрешено възлагането на подизпълнител на критична или важна оперативна функция или дейност (или на съществена част от нея) и ако е така, условията, на които се подчинява възлагането на подизпълнител на значителни оперативни функции или дейности (вж. насока 13);

f. местоположението(ята) (т.е. региони или държави), където съответните данни ще се съхраняват и обработват (местоположение на центровете за данни), както и условията, които трябва да бъдат изпълнени, включително изискване за уведомяване на предприятието, ако доставчикът на услуги предлага промяна на местоположението(ята);

g. разпоредби относно достъпността, наличността, целостта, поверителността, неприкосновеността на личния живот и безопасността на съответните данни, като се вземе предвид посоченото в насока 12;

h. правото на предприятието да наблюдава редовно дейността на доставчика на облачни услуги;

i. договорените нива на обслужване, които следва да включват точни количествени и качествени показатели за изпълнение за възложената на външни изпълнители функция, за да се даде възможност за своевременно наблюдение, така че да могат да се предприемат своевременно подходящи коригиращи действия, ако договорените нива на обслужване не са изпълнени;

j. задълженията за докладване от доставчика на облачни услуги на предприятието, включително, ако е целесъобразно, задълженията за представяне на доклади, свързани със сигурността и ключови функции на предприятието, например доклади за функцията за вътрешен одит на доставчика на облачни услуги;

k. дали доставчикът на облачни услуги следва да направи задължителна застраховка срещу определени рискове и, ако е приложимо, необходимото ниво на застрахователното покритие;

l. изискванията за въвеждане и тестване на планове за действие при извънредни ситуации;

m. изискването доставчикът на облачни услуги да предостави на предприятието, на надзорните му органи и на всяко друго лице, назначено от предприятието или надзорните органи, следното:

i. пълен достъп до всички относими търговски помещения (централни офиси и оперативни центрове), включително пълния обхват на съответните устройства, системи, мрежи, информация и данни, използвани за предоставяне на възложената на външния изпълнител функция, включително свързана финансова информация, до персонала и външните одитори на доставчика на облачни услуги („права на достъп“);

ii. неограничени права за проверка и одит, свързани със споразумението за възлагане на облачни услуги на външни доставчици („права на одит“), за да им се даде възможност да извършват наблюдение на споразумението за възлагане на дейности на външен изпълнител, и да се гарантира спазването на всички приложими регулаторни и договорни изисквания;

n. разпоредби, с които се гарантира, че данните, собственост на предприятието могат да бъдат незабавно възстановени от него в случай на несъстоятелност, преструктуриране или прекратяване на стопанската дейност на доставчика на облачни услуги.

Насока 11 — Права на достъп и одит

38. Споразумението за възлагане на облачни услуги на външни доставчици не следва да ограничава ефективното упражняване на правото на достъп и правото на одит на предприятието, както и възможностите за контрол на облачните услуги с цел изпълнение на регулаторните му задължения.

39. Предприятието следва да упражнява своите права на достъп и одит, да определя честотата на одитите, както и областите и услугите, които да бъдат одитирани въз основа на основан на риска подход, в съответствие с раздел 8 от Насоките на EIOPA за системата на управление.

40. При определяне на честотата и обхвата на упражняването на правото на достъп или правото на одит предприятието следва да прецени дали възлагането на облачни услуги на външен доставчик е свързано с критична или важна оперативна функция или дейност, естеството и степента на риска и въздействието върху предприятието, произтичащи от споразуменията за възлагане на облачни услуги на външни доставчици.

41. Ако упражняването от предприятието на неговите права на достъп или одит или използването на определени одитни техники създава риск за средата на доставчика на облачни услуги и/или клиент на друг доставчик на облачни услуги (напр. въздействието върху нивата на обслужване, наличието на данни, аспектите, свързани с поверителността), предприятието и доставчикът на облачни услуги следва да се споразумеят относно алтернативни начини за осигуряване на сходно ниво на увереност и обслужване на предприятието (напр. включването на специфични контролни мерки, подлежащи на изпитване, което е документирано в конкретен доклад/сертификат, предоставен от доставчика на облачни услуги).

42. Без да се засяга окончателната им отговорност по отношение на дейностите, извършвани от техните доставчици на облачни услуги, с цел по-ефективно използване на одитните ресурси и намаляване на организационната тежест за доставчика на облачни услуги и неговите клиенти, дружествата могат да използват:

a. сертификати и доклади от вътрешен одит на трети страни, предоставени от доставчика на облачни услуги;

b. обединени одити (т.е. одити, извършени съвместно с други клиенти на един и същ доставчик на облачни услуги) или обединени одити, извършени от назначени от тях трети лица.

43. В случай на възлагане на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги, дружествата следва да използват метода, посочен в точка 42, буква а), само ако те:

a. гарантират, че обхватът на сертификата или одиторския доклад обхваща системите (напр. процеси, приложения, инфраструктура, центрове за данни и др.) и контролните механизми, установени от предприятието и оценява спазването на съответните регулаторни изисквания;

b. извършват редовно задълбочена оценка на съдържанието на новите сертификати или одитни доклади и проверяват дали сертификатите или докладите не са неактуални;

c. гарантират, че ключовите системи и контролни механизми ще бъдат обхванати в бъдещите версии на сертификата или одиторския доклад;

d. са удовлетворени от правоспособността на сертифициращата или одитиращата страна (напр. по отношение на редуването на сертифициращото или одиторското предприятие, квалификациите, експертния опит, повторното изпълнение/потвърждаването на доказателствата в базисния одитен файл);

e. се уверяват, че сертификатите се издават, а одитите се извършват въз основа на подходящи стандарти и включват проверка на оперативната ефективност на въведените основни контролни механизми;

f. имат договорно право да изискват разширяване на обхвата на сертификатите или одитните доклади, за да включат в него други съответни системи и контролни механизми; броят и честотата на подобни искания за промяна на обхвата следва да бъдат разумни и законосъобразни от гледна точка на управлението на риска;

g. запазват договорното си право да извършват индивидуални одити на място по тяхна преценка по отношение на възлагането на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги; това право следва да се упражнява в случай на специфични нужди, които не са възможни чрез други видове взаимодействия с доставчика на облачни услуги.

44. Във връзка с възлагането на критични или важни оперативни функции, предприятието следва да преценя дали сертификатите и докладите на трети страни, посочени в точка 42, буква а), са подходящи и достатъчни, за да отговарят на неговите регулаторни задължения, и с оглед на основан на риска подход, не следва да разчитат единствено на такива доклади и сертификати с течение на времето.

45. Преди планирано посещение на място страната, която ще упражнява правото си на достъп (предприятие, одитор или трето лице, действащо от името на предприятието/ата) следва да даде предизвестие в разумен срок, освен когато е било невъзможно даване на ранно предизвестие поради извънредна или кризисна ситуация. В това предизвестие следва да са посочени мястото и целта на посещението и персоналът, който ще участва в посещението.

46. Предвид че решенията за облачни услуги имат високо ниво на техническа сложност, предприятието трябва да се увери, че персоналът, който провежда одита — независимо дали се състои от вътрешни одитори или от съвместни

одитори, действащи от негово име или одитори, определени от доставчика на облачни услуги — или съответно персоналът, който преглежда сертификатите от трета страна или докладите от одит на доставчика на облачни услуги, притежава подходящи умения и знания за провеждане на практически значимите одити и/или оценки.

Насока 12 — Сигурност на данните и системите

47. Предприятието следва да гарантира, че доставчиците на облачни услуги спазват европейски и национални разпоредби, както и подходящи стандарти за сигурност на ИКТ.

48. При възлагане на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги, в допълнение предприятието следва да определи специфични изисквания за информационна сигурност в споразумението за възлагане на дейности на външни изпълнители и да наблюдава редовно спазването на тези изисквания.

49. За целите на точка 48, в случай на възлагане на критични или важни оперативни функции или дейности на доставчици на облачни услуги, предприятието, като прилага основан на риска подход и при отчитане на своите отговорности и отговорностите на доставчика на облачни услуги, следва да:

a. постигне споразумение за ясни роли и отговорности между доставчика на облачни услуги и предприятието по отношение на оперативните функции или дейности, които са засегнати от възлагането на облачни услуги на външни доставчици и следва да са ясно разделени;

b. определи и избере подходящо ниво за защита на поверителността на данните, непрекъснатост на възлаганите дейности, цялост и проследяемост на данните и системите в контекста на планираното възлагане на облачни услуги на външни доставчици;

c. обмисли конкретни мерки, когато е необходимо, по отношение на данните в движение, данните в паметта и данните в хранилище, например употребата на криптиращи технологии в комбинация с подходящо управление на ключове;

d. обмисли механизмите за интегриране на облачните услуги със системите на дружествата, например приложно-програмни интерфейси и стабилен процес на управление на потребителите и достъпа;

e. гарантира по силата на договор, че разполагаемостта на мрежовия трафик и очакваният капацитет отговарят на изискванията за непрекъснатост, когато това е приложимо и осъществимо;

f. определи и вземе решение за подходящи изисквания за непрекъснатост, гарантиращи подходящи нива на всяко ниво от технологичната верига, когато е приложимо;

g. разполага със солиден и добре документиран процес на управление на инциденти, включващ съответните отговорности, например чрез определяне на модел на сътрудничество в случай на възникване на действителни или предполагаеми инциденти;

h. възприеме основан на риска подход по отношение на местата за съхранение и обработка на данни (т.е. държава или регион) и съображения за сигурност на информацията;

i. наблюдава изпълнението на изискванията, свързани с ефективността и ефикасността на механизмите за контрол, прилагани от доставчика на

облачни услуги, които биха смекчили рисковете, свързани с предоставяните услуги.

Насока 13 — Възлагане на подизпълнител на критични или важни оперативни функции или дейности

50. Ако възлагането на подизпълнител на критични или важни оперативни функции или дейности (или част от тях) е разрешено, в споразумението за възлагане на облачни услуги на външни доставчици между предприятието и доставчика на облачни услуги следва:

a. да се посочват всички видове дейности, които са изключени от потенциално възлагане на подизпълнители;

b. да се посочват условията, които трябва да бъдат изпълнени в случай на възлагане на подизпълнител (напр. подизпълнителят също ще изпълни изцяло съответните задължения на доставчика на облачни услуги). Тези задължения включват правата на одит и достъп и сигурността на данните и системите;

c. да се посочва, че доставчикът на облачни услуги запазва пълната си отговорност за и надзор върху услугите, възложени на външни изпълнители;

d. да включва задължение доставчикът на облачни услуги да уведомява дружествата за всички планирани значителни промени на подизпълнителите или услугите възложени за подизпълнение, които могат да повлияят върху способността на доставчика на услуги да изпълнява задълженията си съгласно споразумението за възлагане на облачни услуги на външни доставчици. Периодът за уведомление относно такива промени следва да дава възможност на предприятието най-малко да извърши оценка на риска за ефектите от предложените промени, преди да влезе в сила действителната промяна на подизпълнителите или услугите, възложени за подизпълнение;

e. да гарантира, когато доставчик на облачни услуги планира промени на подизпълнителите или услугите, възложени за подизпълнение, които биха оказали неблагоприятно въздействие върху оценката на риска на договорените услуги, че предприятието има право да възрази срещу тези промени и/или да прекрати договора и да се откаже от него.

Насока 14 — Наблюдение и надзор върху споразумения за възлагане на облачни услуги на външни доставчици

51. Предприятието следва да наблюдава редовно изпълнението на дейностите, мерките за сигурност и придържането към договореното ниво на обслужване от неговите доставчици на облачни услуги съгласно основан на риска подход. Основният акцент следва да бъде поставен върху възлагането на критични и важни оперативни функции на външни доставчици на облачни услуги.

52. За тази цел предприятието следва да създаде механизми за наблюдение и надзор, които следва да отчитат, когато е възможно и целесъобразно, наличието на възлагане на подизпълнители на критични или важни оперативни функции или част от тях.

53. АУНО следва периодично да получава актуална информация относно рисковете, установени при възлагане на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги.

54. За да се гарантира адекватното наблюдение и надзор върху техните споразумения за възлагане на облачни услуги на външни доставчици, дружествата следва да използват достатъчно ресурси с подходящи умения и знания, за да наблюдават услугите, възложени на външни доставчици на облачни услуги. Персоналът на предприятието, отговорен за тези услуги следва да има както познания в областта на ИКТ, така и бизнес познания, доколкото те се считат за необходими.

Насока 15 — Права на прекратяване и стратегии за изход

55. При възлагане на критични или важни оперативни функции или дейности на външни доставчици на облачни услуги, в споразумението за възлагане на облачни услуги на външни доставчици, за предприятието следва да има предвидена ясно определена клауза за изход, гарантираща че то може да прекрати споразумението, ако това е необходимо. Прекратяването следва да бъде възможно без да вреди на непрекъснатостта и качеството на услугите, предоставяни от него на титулярите на полици. За да постигне това, предприятието следва:

a. да разработи планове за изход, които са всеобхватни, основани на услуги, документирани и изпитани в достатъчна степен (напр. чрез извършване на анализ на потенциалните разходи, въздействия, ресурси и отчитане във времето на различните потенциални възможности за изход);

b. да идентифицира алтернативни решения и да разработи подходящи и осъществими планове за преход, за да се даде възможност на предприятието да отнеме съществуващите дейности и данни от доставчика на облачни услуги и да ги прехвърли на алтернативни доставчици на услуги или обратно на предприятието. Тези решения следва да бъдат определени по отношение на предизвикателствата, които могат да възникнат поради местоположението на данните, като се предприемат необходимите мерки за осигуряване на непрекъснатост на дейността по време на преходния период;

c. да гарантира, че доставчикът на облачни услуги оказва адекватна подкрепа на предприятието при прехвърлянето на възложените на подизпълнител данни, системи или приложения на друг доставчик на услуги или пряко на предприятието;

d. да се споразумее с доставчика на облачни услуги, че веднага след повторното им прехвърляне на предприятието, неговите данни ще бъдат изцяло и сигурно заличени от доставчика на облачни услуги във всички региони.

56. При разработване на стратегии за изход предприятието трябва да има предвид следното:

a. да определи целите на стратегията за изход;

b. да определи активиращите събития (напр. ключови показатели за риска за докладване на неприемливо ниво на обслужване), които биха могли да задействат стратегията за излизане;

c. да извърши анализ на въздействието върху работния процес, съизмеримо с възложените на външни изпълнители дейности, за установяване на

необходимото време, човешки и други ресурси за прилагане на плана за изход;

d. да възложи роли и отговорности за управление на плановете за изход и преходните дейности;

e. да определи критерии за успешен преход.

Насока 16 — Надзор от надзорни органи върху споразумения за възлагане на облачни услуги на външни доставчици

57. Като част от своя процес на надзорен преглед надзорните органи следва да извършват анализ на въздействията, произтичащи от споразуменията за възлагане на облачни услуги на външни доставчици, сключени от дружествата. В анализа на въздействието следва да се поставя акцент по-специално върху споразуменията, свързани с възлагането на критични или важни оперативни функции или дейности на външни изпълнители.

58. Надзорните органи следва да отчитат следните рискове при надзора върху споразуменията за възлагане на облачни услуги на външни доставчици, сключени от дружествата:

a. рискове, свързани с ИКТ;

b. други операционни рискове (вкл. правен риск и риск, свързан със спазването на изискванията, риск, свързан с възлагане на дейности на външни изпълнители и управление от трета страна);

c. риск, свързан с репутацията;

d. риск от концентрация, включително на равнище държава/секторно равнище.

59. В рамките на своята оценка надзорните органи следва да включват следните аспекти с оглед на основан на риска подход:

a. целесъобразност и ефективност на управлението и оперативните процеси на предприятието във връзка с одобряването, изпълнението, наблюдението, управлението и подновяването на споразуменията за възлагане на облачни услуги на външни доставчици;

b. дали предприятието разполага с достатъчно ресурси, притежаващи адекватни умения и знания, за да се наблюдават услугите, възложени на външни доставчици на облачни услуги;

c. дали предприятието идентифицира и управлява всички рискове, посочени в настоящите насоки.

60. Що се отнася до групи, органът за надзор върху групите следва да гарантира, че въздействията на възлагането на критични или важни оперативни функции или дейности на външен доставчик на облачни услуги са отразени в оценката на риска за групата, извършена от органа за надзор върху групите, като се вземат предвид изискванията, посочени в точки 58—59 и индивидуалните характеристики на управлението и оперативните характеристики на групата.

61. Ако възлагането на критични или важни оперативни функции или дейности на външен доставчик на облачни услуги включва повече от едно предприятие в различни държави членки и се управлява централно от дружеството майка или от дъщерно предприятие от групата (напр. предприятие или дружество за услуги от групата, напр. доставчикът на ИКТ от групата), органът за надзор върху групите и/или съответните надзорни органи на дружествата, участващи във

възлагането на облачни услуги на външни доставчици, следва да обсъдят, когато е целесъобразно, в рамките на колегиума на надзорните органи, въздействията на възлагането на дейности на външен доставчик на облачни услуги върху рисковия профил на групата.

62. Когато има опасения, водещи до заключението, че дадено предприятие вече не разполага с надеждни правила за управление или не спазва регулаторните изисквания, надзорните органи следва да предприемат подходящи действия, които може да включват, например изискване от предприятието да подобри правилата за управление като ограничи обхвата на възложените на външни изпълнители функции, или налагане на изход от едно или повече споразумения за възлагане на дейности на външни изпълнители. По-специално, като се има предвид необходимостта от гарантиране на непрекъснатост на дейността на предприятието, може да се наложи отмяна на договори, ако надзорът и прилагането на регулаторните изисквания не могат да се осигурят чрез други мерки.

Правила за нормативно съответствие и за докладване

63. Този документ съдържа насоки, издадени съгласно член 16 от Регламент (ЕС) № 1094/2010. Съгласно член 16, параграф 3 от този регламент компетентните органи и финансовите институции трябва да положат всички усилия за спазване на насоките и препоръките.

64. Компетентните органи, които спазват или възнамеряват да спазват настоящите насоки, следва да ги включат по подходящ начин в своята регулаторна или надзорна рамка.

65. Компетентните органи трябва да потвърдят пред EIOPA дали спазват или възнамеряват да спазват настоящите насоки, като посочат причините за неспазване, в срок от два месеца от датата на публикуването на преводните версии.

66. При липса на отговор в този срок се счита, че компетентните органи не спазват изискването за докладване и това се докладва.

Заключителна разпоредба относно преразглежданията

67. Настоящите препоръки подлежат на преразглеждане от страна на EIOPA.