УКАЗАНИЯ
относно прилагането на чл. 75, ал. 1 от Наредба № 71 от 22.07.2021 г. за изискванията към системата на управление на застрахователите и презастрахователите на Комисията за финансов надзор във връзка със спазването на Насоките за възлагане на дейности на доставчици на облачни услуги, издадени от Европейския орган по застраховане и професионално пенсионно осигуряване (EIOPA-BoS-20-002)

На основание чл. 13, ал. 1, т. 4 от Закона за Комисията за финансов надзор (ЗКФН) във връзка с чл. 12, ал. 1, т. 1 от ЗКФН, чл. 9, ал. 4, чл. 77, ал. 5, чл. 110 и чл. 111 от Кодекса за застраховането (КЗ) и чл. 75, ал. 2 от Наредба № 71 от 22.07.2021 г. за изискванията към системата на управление на застрахователите и презастрахователите на Комисията за финансов надзор, обн., ДВ, бр. 64 от 2021 г., (Наредба № 71) и при съобразяване с Насоките за възлагане на дейности на доставчици на облачни услуги (EIOPA-BoS-20-002), издадени от Европейския орган за застраховане и професионално пенсионно осигуряване, Комисията за финансов надзор издава настоящите указания относно прилагането на чл. 75, ал. 1 от Наредба № 71 във връзка със спазването на Насоките за възлагане на дейности на доставчици на облачни услуги, издадени от Европейския орган по застраховане и професионално пенсионно осигуряване (EIOPA-BoS-20-002).

I. Облачни услуги и прехвърляне на функции или дейности на доставчици на облачни услуги

1. Застрахователят, съответно презастрахователят, преценява дали дадено споразумение с доставчик на облачни услуги представлява прехвърляне на дейност по смисъла на чл. 110 от КЗ, като съобразява дали:

1.1. оперативната функция или дейност, или части от тях, които се възлагат на доставчик на облачни услуги, се извършват постоянно или периодично;

1.2. оперативната функция или дейност, или части от тях обикновено попадат в обхвата на оперативните функции или дейности, които застрахователят, съответно презастрахователят, осъществява или би могъл да осъществява в хода на обичайната си стопанска дейност, независимо дали ги е осъществявал по-рано.

2. Когато споразумението по т. 1 с доставчика на облачни услуги обхваща повече функции или дейности, при преценката по т. 1 застрахователят, съответно презастрахователят, го съобразява в неговата цялост.

3. Тези указания се прилагат и в случаите, когато застрахователят, съответно презастрахователят, прехвърля оперативните си функции на доставчик на услуги, който не е доставчик на облачни услуги, но разчита в значителна степен на инфраструктурата за облачни услуги, за да осъществява своята дейност.

II. Общи принципи на управление при прехвърляне на облачни услуги

4. Компетентният орган на застрахователя, съответно на презастрахователя, гарантира, че всяко решение за прехвърляне на критични или важни оперативни функции или дейности на доставчици на облачни услуги се основава на задълбочена оценка на риска, включваща всички относими рискове, произтичащи от споразумението, като рискове, свързани с 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. По отношение на застрахователите с право на достъп до единния пазар на Европейския съюз и на презастрахователите изпълнението на задълженията по изречение първо не засяга спазването на изискванията по чл. 274, параграф 3 от Делегиран регламент (ЕС) № 2015/35 на Комисията 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 12/1 от 17 януари 2015 г.) (Делегиран регламент (ЕС) 2015/35).

5. Когато възлага критични или важни оперативни функции или дейности на доставчици на облачни услуги и поради сключваните договори за прехвърляне на облачни услуги настъпват промени в рисковия му профил, застрахователят, съответно презастрахователят, ги отразява в собствената оценка на риска и платежоспособността (СОРП).

6. Използването на облачни услуги трябва да бъде в съответствие със стратегиите и с вътрешните политики и процеси на застрахователя, съответно презастрахователя, които при необходимост се актуализират.

III. Актуализиране на писмената политика за прехвърляне на функции или дейности на доставчици на облачни услуги

7. Когато възнамерява да прехвърля дейности на доставчик на облачни услуги застрахователят, съответно презастрахователят, актуализира писмената си политика за прехвърляне на функции или дейности на доставчици на услуги по чл. 77, ал. 1, т. 3, буква „д“ от КЗ, по чл. 73 от Наредба № 71 и другите относими вътрешни политики, като отразява най-малко следното относно спецификите на възлагането на облачни услуги, а именно:

7.1. ролите и отговорностите на компетентния орган на застрахователя, съответно на презастрахователя, и на другите функции, които са ангажирани и по-конкретно на функциите, отговорни за ИКТ, за информационната сигурност, за съответствието, за управлението на риска и за вътрешния одит;

7.2. процесите и отчетните процедури, необходими за одобряване, изпълнение, наблюдение, управление и подновяване на споразуменията за възлагане на критични или важни оперативни функции, или дейности на доставчици на облачни услуги;

7.3. контрола върху облачните услуги съобразен с естеството, обема и сложността на рисковете, характерни за предоставяните услуги, включително:

а) оценка на риска във връзка със споразуменията за възлагане на функции и дейности на доставчици на облачни услуги и комплексна проверка на доставчиците на облачни услуги, включително честотата на оценката на риска;

б) наблюдение и управленски контрол;

в) стандарти и проверки за сигурност;

7.4. изискване за прилагане на договорните условия по Раздел Х по отношение на прехвърлянето на критични или важни оперативни функции или дейности на доставчици на облачни услуги;

7.5. изискванията относно документирането и писменото уведомяване на Комисията за финансов надзор (Комисията) във връзка с прехвърлянето на критични или важни оперативни функции или дейности на доставчици на облачни услуги;

7.6. изискване за предвиждане на документирана и в достатъчна степен изпитана стратегия за изход по отношение на всяко споразумение за прехвърляне на функции и

дейности на доставчици на облачни услуги, което обхваща критични или важни оперативни функции, или дейности, която:

а) е пропорционална на естеството, мащаба и сложността на рисковете, присъщи на предоставяните услуги;

б) може да включва набор от процеси за прекратяване на прехвърлянето на дейността, включващи преустановяване, реинтеграция в рамките на застрахователя или презастрахователя или прехвърляне към друг доставчик на услугите, включени в споразумението за прехвърляне на функции и дейности на доставчик на облачни услуги.

IV. Писмено уведомление

8. Застрахователят, съответно презастрахователят, представя проекта на договора за прехвърляне на функция или дейност по чл. 74 от Наредба № 71 в Комисията при всяко прехвърляне на критична или важна функция, или дейност на доставчик на облачни услуги. При промяна на класификацията на функция или дейност от страна на застрахователя, съответно на презастрахователя, която към момента на прехвърлянето ѝ не е била определена като важна или критична но в последствие е станала такава, договорът за прехвърляне се представя в Комисията.

9. Заедно с проекта на договор, съответно договора за прехвърлянето на функцията или дейността по т. 8 застрахователят, съответно презастрахователят, представя най-малко следната информация:

9.1. кратко описание на подлежащата на прехвърляне функция или дейност;

9.2. началната и крайната дата на действие на договора, както и сроковете за предизвестие за страните в случай на предсрочно прекратяване;

9.3. приложимото право към споразумението за прехвърляне на облачни услуги на доставчици на облачни услуги;

9.4. идентификационна информация относно доставчика на облачни услуги, която съдържа най-малко:

а) ЕИК/БУЛСТАТ, с който той е вписан в търговския регистър, а за доставчик от друга държава – идентификационен код и информация за вписването му в съответния регистър на държавата по произход;

б) идентификатор на юридическото лице (LEI код), ако има такъв;

в) седалище, адрес на управление и други относими данни за контакт, както и наименованието на предприятието майка, ако има такова;

г) информация за това дали доставчикът на облачни услуги е част от групата, от която е част застрахователят, съответно презастрахователят;

9.5. облачните услуги и моделите на функциониране на облачната среда (публични, частни, хибридни, общностни), както и специфичното естество на данните, които трябва да се съхраняват, както и местоположението, където ще се съхраняват такива данни;

9.6. кратко обобщение на причините, поради които прехвърлената функция или дейност се счита за критична или важна;

9.7. датата на последната оценка на критичността или важността на прехвърлената функция или дейност.

V. Изисквания относно документирането

10. Застрахователят, съответно презастрахователят, документира своите споразумения за прехвърляне на облачни услуги на доставчици на облачни услуги и поддържа актуална информация за тях като част от системата на управление и управлението на риска.

11. Застрахователят, съответно презастрахователят, води регистър на прекратените споразумения за прехвърляне на облачни услуги на доставчици на облачни услуги, който се съхранява за период от не по-малко от 5 години след датата на прекратяването на договора.

12. При прехвърляне на критични или важни оперативни функции или дейности, застрахователят, съответно презастрахователят, документира:

12.1. информацията по т. 9;

12.2. в случай на групи – застрахователните и презастрахователните дружества и други дружества, попадащи в обхвата на консолидация за надзорни цели, които използват облачните услуги;

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

12.4. органа, одобрил проекта на споразумението за възлагане на облачни услуги на доставчик на облачни услуги;

12.5. датите на последните и следващите одити, ако има такива;

12.6. подробна информация за всички подизпълнители, на които са превъзложени за изпълнение съществени части от критичната или важна оперативна функция, или дейност, включително държавите и регионите, в които са регистрирани подизпълнителите, в които ще се извършва услугата и в които ще се съхраняват данните;

12.7. резултат от извършената оценка за заменяемост на доставчика на облачни услуги;

12.8. дали прехвърлянето на критичната или важна функция или дейност на доставчик на облачни услуги позволява извършването на спешни бизнес операции;

12.9. прогнозираните годишни бюджетни разходи;

12.10. дали застрахователят, съответно презастрахователят, има стратегия за изход по т. 7.6.

13. Когато застрахователят, съответно презастрахователят, прехвърля на доставчици на облачни услуги оперативни функции или дейности, които не са критични или важни, той определя информацията, която се документира, като извършва преценка на естеството, мащаба и сложността на рисковете, присъщи на услугите, предоставяни от доставчика на облачни услуги.

14. Застрахователят, съответно презастрахователят, предоставя на Комисията при поискване цялата необходима за упражняването на надзорната дейност информация, включително копие на споразумението за прехвърляне на дейности на доставчици на облачни услуги.

VI. Анализ преди прехвърлянето на функции или дейности на доставчици на облачни услуги

15. Преди да сключи споразумение за прехвърляне на функция или дейност с доставчик на облачни услуги, застрахователят, съответно презастрахователят:

15.1. извършва преценка по Раздел VII относно това, дали споразумението се отнася за критична или важна функция или дейност;

15.2. извършва идентификация и оценка по Раздел VIII на всички относими рискове, свързани със споразумението;

15.3. извършва подходяща комплексна проверка по Раздел IX на потенциалния доставчик;

15.4. установява и оценява дали потенциалният доставчик е предприел необходимите мерки за избягване на конфликт на интереси, които биха могли да застрашат изпълнението на прехвърлените функции или дейности.

VII. Оценка на критични или важни функции или дейности

16. Преди да сключи споразумение с доставчик на облачни услуги, застрахователят, съответно презастрахователят, извършва преценка дали споразумението се отнася за критична или важна функция, или дейност, както и дали има потенциала да стане критична или важна функция, или дейност в бъдеще.

17. В случай че естеството, мащабът и сложността на рисковете, присъщи на споразумението, се променят съществено, застрахователят, съответно презастрахователят, извършва повторна оценка на критичността или важността на оперативната функция или дейност.

18. При извършването на оценка, освен резултатите от оценката на риска, застрахователят, съответно презастрахователят, взема предвид най-малко следните фактори:

18.1. потенциалното въздействие на всяко съществено прекъсване на възложената на доставчик оперативна функция или дейност, или на невъзможността на доставчика на облачни услуги да предоставя услугите съгласно договорените условия върху:

а) непрекъснатото спазване на регулаторните задължения на застрахователя, съответно на презастрахователя;

б) краткосрочната и дългосрочната финансова и платежоспособна устойчивост и жизнеспособност на застрахователя, съответно на презастрахователя;

в) непрекъснатостта на стопанските дейности и оперативната устойчивост на застрахователя, съответно на презастрахователя;

г) оперативния риск на застрахователя, съответно на презастрахователя, включително рискове във връзка с пазарното поведение, риска, свързан с ИКТ и правния риск;

д) репутационния риск;

18.2. потенциалното въздействие на споразумението за прехвърляне на функция или дейност на доставчик на облачни услуги върху способността на застрахователя, съответно на презастрахователя, да:

а) идентифицира, наблюдава и управлява всички относими рискове;

б) спазва всички нормативни изисквания;

в) да провежда подходящи одити във връзка с прехвърлената на доставчици на облачни услуги оперативна функция или дейност;

18.3. общата експозиция на застрахователя, съответно презастрахователя, или групата, към един и същ доставчик на облачни услуги и потенциалното кумулативно въздействие на споразуменията за прехвърляне на дейности на доставчици на облачни услуги в една и съща сфера на дейност;

18.4. размера и сложността на сферите на дейност на застрахователя, съответно на презастрахователя, засегнати от споразумението за прехвърляне на функция или дейност на доставчик на облачни услуги;

18.5. възможността да се прехвърли предвижданото споразумение за прехвърляне на функция или дейност на доставчик на облачни услуги на друг доставчик на облачни услуги или да се реинтегрират услугите в рамките на застрахователя, съответно на презастрахователя („заменяемост“);

18.6. защита на данните, включително личните данни, данните, представляващи търговска тайна или чувствителна информация, и потенциалното въздействие върху застрахователя, съответно презастрахователя, притежателите на полици или други заинтересовани лица на нарушенията на поверителността или на липсата на гаранции за наличието и целостта на данните въз основа на 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 119/1 от 4 май 2016 г.).

VIII. Оценка на риска във връзка с прехвърлянето дейности и функции на доставчици на облачни услуги

19. Застрахователят, съответно презастрахователят, като използва подход, който съответства на естеството, обема и сложността на рисковете, присъщи на дейностите подлежащи на прехвърляне на доставчик на облачни услуги, извършва оценка на потенциалното въздействие на прехвърлянето върху оперативните и репутационните рискове.

20. При прехвърляне на критични или важни оперативни функции или дейности на доставчик на облачни услуги, застрахователят, съответно презастрахователят:

20.1. отчита очакваните ползи и разходи, свързани с предвижданото споразумение за прехвърляне на функция или дейност на доставчик на облачни услуги, включително като съпоставя всички значителни рискове, които могат да бъдат намалени или по-добре управлявани със значителните рискове, които могат да възникнат в резултат на споразумението за прехвърляне;

20.2. оценява, когато е необходимо, рисковете, включително правните рискове, рисковете, свързани с ИКТ, рисковете, свързани със спазването на изискванията, и репутационните рискове, както и ограниченията по отношение на контрола, произтичащи от:

а) избраната облачна услуга и моделите на функциониране на облачната среда – публични, частни, хибридни или общностни;

б) миграцията и/или изпълнението;

в) дейностите и свързаните с тях данни и системи, които се предвижда да се възложат или вече са прехвърлени на доставчик на облачни услуги, както и тяхната чувствителност и необходимите мерки за сигурност;

г) политическата стабилност и положението със сигурността на държавите, в които прехвърлените на доставчик облачни услуги се предоставят или могат да се предоставят и в които данните се съхраняват или е вероятно да се съхраняват, като при оценката следва да се вземат предвид:

аа) относимото действащо законодателство, включително законодателството за защита на данните;

бб) ефективността на механизмите относно прилагането на закона;

вв) нормативните разпоредби в областта на несъстоятелността, които се прилагат в случай на неплатежоспособност на доставчик на облачни услуги и всички ограничения, които биха възникнали във връзка със спешното възстановяване на данните на застрахователя, съответно презастрахователя;

д) превъзлагането 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 застрахователя, съответно на презастрахователя, да наблюдава своите критични или важни оперативни функции или дейности и способността на надзорните органи да упражняват ефективен надзор върху тях;

е) цялостния концентрационен риск на застрахователя, съответно на презастрахователя, спрямо един и същ доставчик на облачни услуги, включително прехвърляне на доставчик на облачни услуги, който не е лесно заменяем или множество споразумения за прехвърляне с един и същ доставчик на облачни услуги.

21. Оценката на риска се извършва преди да се пристъпи към прехвърлянето на дейността или функцията на доставчик на облачни услуги.

22. В случай че настъпят значителни промени в предоставяните услуги или в положението на доставчика, застрахователят, съответно презастрахователят, незабавно преразглежда оценката на риска или извършва нова оценка.

23. Застрахователят, съответно презастрахователят, извършва повторна оценка и при изменение на предмета на споразумението за прехвърляне на облачни услуги на доставчик на услуги.

IX. Комплексна проверка на доставчик на облачни услуги

24. Застрахователят, съответно презастрахователят, в процеса на подбор и оценка на доставчик на облачни услуги и преди сключване на споразумение с него, извършва комплексна проверка на доставчика на облачни услуги, за да гарантира, че той е подходящ съгласно критериите, определени в писмената политика за прехвърляне на дейности на доставчици на услуги. Проверка на доставчика на облачни услуги следва да се извърши и преди прехвърлянето на всяка оперативна функция или дейност.

25. В случай че се сключва последващо споразумение с доставчик на облачни услуги, който е бил вече оценяван, застрахователят, съответно презастрахователят, като прилага подход, базиран на риска, решава дали е необходима повторна комплексна проверка.

26. Комплексната проверка незабавно се преразглежда или се извършва повторно, когато застрахователят, съответно презастрахователят, узнае за значителни слабости или значителни промени в предоставяните услуги или в положението на доставчика на облачни услуги.

27. Когато се прехвърлят критични или важни оперативни функции или дейности на доставчик на облачни услуги, застрахователят, съответно презастрахователят, извършва комплексна проверка, в която включва оценката на пригодността на доставчика, в това число знания и умения, инфраструктура, икономическо състояние, корпоративно и надзорно положение.

X. Договорни условия

28. Договорът между застрахователя, съответно презастрахователя, и доставчика на облачни услуги се сключва в писмена форма и в него ясно се регламентират съответните права и задължения на страните.

29. В случай че с договора се прехвърля изпълнението на критични или важни функции или дейности на доставчик на облачни услуги, освен предвиденото в чл. 111, ал. 3 от КЗ и по чл. 274, параграф 4 от Делегиран регламент (ЕС) 2015/35, в договора задължително се съдържа:

29.1. кратко описание на прехвърлената функция, която ще бъде осъществена;

29.2. началната и крайната дата на действие на договора, както и сроковете за предизвестие за страните в случай на предсрочно прекратяване;

29.3. определяне на приложимото право и на компетентен съд за решаване на споровете, възникнали във връзка със споразумението;

29.4. финансовите задължения на страните, произтичащи от споразумението;

29.5. допуска ли се превъзлагане на прехвърлената критична или важна функция или дейност на подизпълнител, и в случай че се допуска – при какви условия;

29.6. местоположенията, където съответните данни ще се съхраняват и обработват, както и условията, които трябва да бъдат изпълнени, включително изискване

за уведомяване на застрахователя, съответно на презастрахователя, ако доставчикът на облачни услуги предлага промяна на местоположението;

29.7. клаузи относно достъпността, наличността, целостта, поверителността, неприкосновеността и безопасността на съответните данни, като се вземат предвид спецификациите по Раздел XII;

29.8. правото на застрахователя, съответно на презастрахователя, да наблюдава редовно дейността на доставчика на облачни услуги;

29.9. договорените нива на обслужване, които следва да включват точни количествени и качествени показатели за изпълнение на прехвърлената функция, за да се даде възможност за своевременни коригиращи действия, ако договорените нива на обслужване не са изпълнени;

29.10. задълженията за отчетност от страна на доставчика на облачни услуги, включително, ако е целесъобразно – задължение за представяне на периодични отчети, свързани с функцията по сигурността и ключовите функции на застрахователя, съответно на презастрахователя;

29.11. дали доставчикът на облачни услуги се задължава да сключи застраховка срещу определени рискове и необходимото равнище на покритие по тази застраховка;

29.12. изискванията за въвеждане и тестване на планове за действия при извънредни ситуации;

29.13. изискване доставчикът на облачни услуги да предостави на застрахователя, съответно презастрахователя, на Комисията, на заместник-председателя, ръководещ управление „застрахователен надзор“ и на всяко друго лице, определено от тях, следното:

а) пълен достъп до всички търговски помещения, включително пълния обхват на съответните устройства, системи, мрежи, информация и данни, които се използват за предоставяне на възложената на доставчика на облачни услуги функция или дейност, включително свързаната с нея финансова информация, до персонала и външните одитори на доставчика на облачни услуги („права на достъп“);

б) неограничени права за проверка и одит, свързани със споразумението за възлагане на дейности или функции на доставчик на облачни услуги („права на проверка“), за да се даде възможност да извършват наблюдение на споразумението за възлагане на дейности на доставчик на услуги, и да се гарантира спазването на всички приложими регулаторни и договорни изисквания;

29.14. клаузи, с които се гарантира, че данните, собственост на застрахователя, съответно на презастрахователя, могат да бъдат незабавно възстановени от него в случай на несъстоятелност, преструктуриране или прекратяване на доставчика на облачни услуги.

XI. Права на достъп и проверка

30. Споразумението за прехвърляне на функции или дейности на доставчик на облачни услуги не може да ограничава ефективното упражняване на правата на достъп и правата на проверка на застрахователя, съответно презастрахователя, както и възможностите за контрол на облачните услуги с цел изпълнение на възложените му задължения.

31. Застрахователят, съответно презастрахователят, упражнява правата си на достъп и на проверка, определя честотата на проверките, както и областите и услугите, които да бъдат проверявани, въз основа на подход, основан на риска в съответствие с глава втора, раздел VIII от Наредба № 71.

32. Честотата и обхвата при упражняването на право на достъп или право на проверка се преценяват въз основа на това, дали прехвърлянето на дейности на доставчик

на облачни услуги е свързано с критична или важна функция или дейност, естеството и степента на риска и въздействието му върху застрахователя, съответно презастрахователя.

33. В случай че упражняването на правото на достъп или право на проверка или използването на определени техники за проверка от застрахователя, съответно презастрахователя, създава риск за средата на доставчика на облачни услуги или за друг клиент на доставчика на облачни услуги, страните се споразумяват за алтернативни начини за осигуряване на сходно равнище на увереност и обслужване на застрахователя, съответно на презастрахователя.

34. Без да се засяга отговорността на застрахователя, съответно на презастрахователя, по отношение на извършваната дейност от избрания доставчик на облачни услуги и неговите клиенти, за целите на проверката на дейността на доставчика на услуги застрахователят, съответно презастрахователят, може да използва следните методи:

34.1. заверки и доклади от вътрешни одити или от трети страни, предоставени от доставчика на облачни услуги;

34.2. съвместни проверки, извършени заедно с други клиенти на същия доставчик на облачни услуги или проверки, извършени от трети лица, назначени съвместно с други клиенти на същия доставчик на облачни услуги.

35. В случай на прехвърляне на критични или важни оперативни функции, или дейности на доставчици на облачни услуги, застрахователят, съответно презастрахователят, може да използва метода по т. 34.1. само ако:

35.1. гарантира, че обхватът на заверката или одиторския доклад включва системите и контролните механизми, установени от застрахователя, съответно презастрахователя, и оценява спазването на съответните нормативни изисквания;

35.2. извършва редовно задълбочена оценка на съдържанието на новите заверки или одитни доклади и проверява тяхната актуалност;

35.3. гарантира, че ключовите системи и контролни механизми ще бъдат обхванати в бъдещите версии на заверките или одиторския доклад;

35.4. е удовлетворен от пригодността на сертифициращата или одитиращата страна;

35.5. се увери, че заверките се издават, а одитите се извършват въз основа на подходящи стандарти и включват проверка на оперативната ефективност на въведените основни контролни механизми;

35.6. има право да изиска разширяване на обхвата на заверките или одитните доклади, за да включат в него други системи и контролни механизми;

35.7. запазва договорното си право да извършва индивидуални проверки на място по своя преценка по отношение на възлагане на критични или важни оперативни функции или дейности на доставчици на облачни услуги, в случай че възникне такава специфична нужда.

36. Във връзка с прехвърлянето на критични или важни оперативни функции, застрахователят, съответно презастрахователят, извършва преценка дали заверките и докладите по т. 34.1. са подходящи и достатъчни, за да може да отговарят на неговите регулаторни задължения.

37. При извършване на планирана проверка на място застрахователят, съответно презастрахователят, изпраща предизвестие в срок не по-рано от 14 дни преди датата на проверката, в което са посочени мястото и целта на проверката и персоналът, който ще участва. Изречение първо не се прилага при извънредни и кризисни ситуации.

38. Застрахователят, съответно презастрахователят, гарантира, че персоналът, който извършва проверката, съответно персоналът, който преглежда заверките или

докладите от одита на доставчика на облачни услуги, притежава подходящи умения и знания за провеждане на съответните одити и/или оценки.

XII. Сигурност на данните и системите

39. Застрахователят, съответно презастрахователят, гарантира, че доставчиците на облачни услуги спазват европейското и националното законодателство, както и подходящи стандарти за сигурност на ИКТ.

40. При прехвърляне на критични или важни оперативни функции или дейности на доставчици на облачни услуги, застрахователят, съответно презастрахователят, определя специфични изисквания за информационна сигурност в договора за прехвърляне на дейности на доставчици на облачни услуги и наблюдава редовно спазването на тези изисквания.

41. За постигане на целите по т. 40, когато прехвърля критични или важни функции или дейности на доставчици на облачни услуги, застрахователят, съответно презастрахователят, като прилага основан на риска подход, следва да:

41.1. постигне споразумение за ясни задължения и отговорности между себе си и доставчика на облачните услуги по отношение на оперативните функции или дейности, които са предмет на прехвърляне на доставчика на облачни услуги и които следва да са ясно разделени;

41.2. определи и избере подходящо равнище на защита на поверителността на данните, непрекъснатост на прехвърляните дейности, цялост и проследяемост на данните и системите в контекста на планираното възлагане на облачни услуги на доставчици;

41.3. предвиди конкретни мерки, когато е необходимо, по отношение на данните в движение, данните в паметта и данните в хранилище, включително употребата на криптиращи технологии в комбинация с подходящо управление на ключовете;

41.4. предвиди механизмите на интегриране на облачните услуги със системите на застрахователя, съответно презастрахователя;

41.5. гарантира в договора по т. 28, че разполагаемостта на мрежовия трафик и очакваният капацитет отговорят на изискванията за непрекъснатост, когато това е приложимо;

41.6. определя подходящи изисквания за непрекъснатост, осигуряващи адекватни нива на всяко равнище на технологичната верига;

41.7. разполага със солиден и добре документиран процес на управление на инциденти, включващ съответните отговорности;

41.8. приеме предпазлив подход по отношение на местата за съхранение и обработка на данни и мерки за сигурност на информацията;

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

XIII. Превъзлагане на критични или важни функции или дейности

42. В случай че превъзлагането на подизпълнител е разрешено с договора между застрахователя, съответно презастрахователя, и доставчика на облачни услуги, договорът следва да съдържа:

42.1. всички видове дейности, които не могат да се превъзлагат на подизпълнители;

42.2. условията, които трябва да бъдат изпълнени в случай на превъзлагане на подизпълнител, като тези задължения включват правата на проверка и достъп и сигурността на данните и системите;

42.3. посочване, че доставчикът на облачни услуги запазва пълна отговорност и задължение за контрол за превъзложените услуги;

42.4. задължение доставчикът на облачни услуги да уведомява застрахователя, съответно презастрахователя, за всички планирани значителни промени на подизпълнителите или услугите, превъзложени за подизпълнение, които могат да повлияят върху способността на доставчика на услуги да изпълнява задълженията си съгласно договора за прехвърляне на функции или дейности на доставчици на облачни услуги;

42.5. уговорки, че когато доставчикът на облачни услуги планира промени на подизпълнителите или на услугите, превъзложени на подизпълнител, които биха оказали неблагоприятно въздействие върху оценката на риска на договорените услуги, застрахователят, съответно презастрахователят, има право да възрази срещу тези промени и/или едностранно да прекрати договора.

XIV. Наблюдение и контрол върху споразумения за прехвърляне на функции или дейности на доставчици на облачни услуги

43. Застрахователят, съответно презастрахователят, извършва редовно наблюдение върху изпълнението на дейностите, мерките за сигурност и придържането към договорените условия от доставчика на облачни услуги въз основа на подход, основан на риска.

44. За осъществяване на редовно наблюдение, застрахователят, съответно презастрахователят, създава механизми за наблюдение и контрол, които могат да отчитат, където е приложимо, и наличието на превъзлагане на подизпълнители на критични или важни оперативни функции или дейности, или части от тях.

45. Компетентният орган на застрахователя, съответно на презастрахователя, периодично изисква и получава актуална информация относно рисковете, установени при прехвърляне на критични или важни оперативни функции, или дейности на доставчици на облачни услуги.

46. Застрахователят, съответно презастрахователят, осигурява персонал с подходящи знания и умения за осъществяването на адекватно наблюдение и контрол върху изпълнението на договорите за прехвърляне на критични или важни оперативни функции или дейности на доставчици на облачни услуги.

XV. Права на прекратяване и стратегии за изход

47. В случаите, когато се прехвърлят критични или важни оперативни функции, или дейности на доставчици на облачни услуги, в договора за прехвърляне се предвижда ясна и точно определена стратегия за изход, гарантираща, че застрахователят, съответно презастрахователят, може да прекрати споразумението, ако това е необходимо, без с това да се наруши непрекъснатостта и качеството на предоставяните от него услуги. За да постигне това, застрахователят, съответно презастрахователят:

47.1. разработва планове за изход, които са всеобхватни, основани на услуги, документирани и изпитани в достатъчна степен;

47.2. идентифицира алтернативни решения и разработва подходящи и осъществими планове за преход, за да има възможност да изземе съществуващите дейности и данни от доставчика на облачни услуги и да ги прехвърли на алтернативни доставчици на облачни услуги или обратно в застрахователя, съответно в презастрахователя;

47.3. гарантира, че доставчикът на облачни услуги му оказва адекватна подкрепа при прехвърлянето на възложените на подизпълнител данни, системи или приложения

на друг доставчик на облачни услуги или пряко към застрахователя, съответно към презастрахователят;

47.4. се споразумява за заличаване на данните от доставчика на облачни услуги веднага след прехвърлянето им обратно към застрахователя, съответно на презастрахователя, независимо от това къде са били съхранявани данните.

48. При разработването на стратегии за изход, застрахователят, съответно презастрахователят:

48.1. определя целите на стратегията за изход;

48.2. определя обстоятелствата, при които започва прилагането на стратегията за изход;

48.3. извършва анализ на въздействието на стратегията за изход върху работния процес, съответстващ на обема и значимостта на дейностите, прехвърлени на доставчици на облачни услуги, за установяване на необходимото време, човешки и други ресурси за прилагане на плана за изход;

48.4. възлага задължения и отговорности за управление на плановете за изход и дейностите по преход по т. 47.1. и 47.2;

48.5. определя критерии за успешен преход.

XVI. Надзор върху споразумения за възлагане на дейности и функции на доставчици на облачни услуги

49. Комисията, при осъществяване на надзорната си дейност, извършва анализ на въздействията, произтичащи от договорите за прехвърляне на критични или важни функции, или дейности на доставчици на облачни услуги, както и от цялостната дейност на застрахователите и презастрахователите по прехвърляне на функции и дейности на доставчици на облачни услуги.

50. При осъществяване на надзора върху договорите за прехвърляне на функции или дейности на доставчици на облачни услуги, Комисията анализира следните рискове:

50.1. рискове, свързани с ИКТ;

50.2. други оперативни рискове, в това число правен риск и риск от неспазване на изискванията, риск от прехвърляне на дейности и риск от управление на трети лица;

50.3. репутационен риск;

50.4. риск от концентрация, включително на равнище сектор или страна.

51. При оценката Комисията изследва следните аспекти, като прилага подход, основан на риска:

51.1. целесъобразност и ефективност на управлението и оперативните процеси на застрахователя, съответно на презастрахователя във връзка с одобряването, изпълнението, наблюдението, управлението и подновяването на договорите за прехвърляне на функции или дейности на доставчици на облачни услуги;

51.2. дали застрахователят, съответно презастрахователят, разполага с достатъчно персонал, притежаващ адекватни умения и знания, за да се наблюдава услугите, прехвърлени на доставчици на облачни услуги;

51.3. дали застрахователят, съответно презастрахователят, идентифицира и управлява всички рискове, посочени в настоящия раздел.

52. Когато е орган за надзор на група, Комисията изисква прехвърлянето на критични или важни оперативни функции, или дейности да се отразява в управлението на риска на равнище група и прилага т. 49 - 51, като взема предвид индивидуалните оперативни характеристики и управление на групата.

53. Комисията поставя въпроса за прехвърлянето на критични или важни функции или дейности на доставчици на облачни услуги в дневния ред на заседания на надзорния

колегиум, когато повече от един застраховател или презастраховател, които са част от една и съща група извършват такова прехвърляне.

54. Когато бъде констатирано, че процесът на управление на възложените дейности на застрахователя, съответно на презастрахователя, не е достатъчно надежден или че той не спазва други нормативни изисквания, Комисията, съответно заместник-председателят, ръководещ управление „Застрахователен надзор“, предприема предвидените в закона мерки, в това число:

54.1. изисква от застрахователя, съответно от презастрахователя, да подобри правилата за управление;

54.2. изисква от застрахователя, съответно от презастрахователя, да ограничи обхвата на възложените на доставчици на облачни услуги функции, или;

54.3. разпорежда прекратяване на един или повече договори за прехвърляне на дейности.

55. Комисията прилага мярката по т. 54.2., когато спазването на нормативните изисквания не може да се постигне с други средства.

XVII. Дефиниции

56. По смисъла на тези указания:

56.1. „Доставчик на услуги“ е трето лице, което извършва процес, услуга или дейност, или части от тях по силата на споразумение за възлагане на дейности.

56.2. „Доставчик на облачни услуги“ е доставчик на услуги, който е отговорен за доставянето на облачни услуги по силата на споразумение за възлагане на дейности.

56.3. „Ключови функции“ са функциите по чл. 78, ал. 1, т. 1 - 4 от КЗ, както и функциите по чл. 78, ал. 1, т. 5 от КЗ, които застрахователят, съответно презастрахователят, изрично е определил като такива поради специфичната им важност за неговата дейност и организация.

56.4. „Облачни услуги“ са 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 (като мрежи, сървъри, хранилища, приложения и услуги и др.), които бързо могат да бъдат обезпечавани и реализирани с минимални усилия за управление или взаимодействие с доставчика на облачни услуги.

56.5. „Оперативна функция“ е всяка функция, свързана с търговската дейност на застрахователя, съответно на презастрахователя, която е различна от ключовите функции.

56.6. „Общностно облачно пространство“ е инфраструктура за облачни услуги, която може да се използва само от конкретна общност от дружества, включително няколко дружества, принадлежащи към една група.

56.7. „Публично облачно пространство“ е инфраструктура за облачни услуги, която може открито да се използва от широката общественост.

56.8. „Хибридно облачно пространство“ е инфраструктура за облачни услуги, която е съставена от две или повече обособени инфраструктури за облачни услуги.

56.9. „Частно облачно пространство“ е инфраструктура за облачни услуги, която може да се използва само от един застраховател, съответно от един презастраховател.

Настоящите указания са приети с решение по протокол № 66 от 09.09.2021 г. на Комисията за финансов надзор.

Председател: Бойко Атанасов