УКАЗАНИЯ
относно прилагането на чл. 102, 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 сигурност и управление на информационните и комуникационните технологии, издадени от Европейския орган по застраховане и професионално пенсионно осигуряване (EIOPA- BoS-20/600)

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. 76, ал. 2, чл. 77, ал. 5, чл. 114, ал. 4 от Кодекса за застраховането (КЗ) и чл. 102, 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 сигурност и управление на информационните и комуникационните технологии (EIOPA- BoS-20/600), издадени от Европейския орган за застраховане и професионално пенсионно осигуряване, Комисията за финансов надзор издава настоящите указания относно прилагането на чл. 102, ал. 1 от Наредба № 71 във връзка със спазването на Насоките за сигурност и управление на информационните и комуникационните технологии, издадени от Европейския орган по застраховане и професионално пенсионно осигуряване (EIOPA- BoS-20/600):

I. Пропорционалност

1. Застрахователят, съответно презастрахователят, прилага правилата по тези указания по начин, който съответства на естеството, обема и сложността на рисковете, присъщи на дейността му, и в съответствие с изпълнението на задълженията, предвидени в нормативните актове, регламентиращи изисквания към сигурността и управлението на информационните и комуникационните технологии (ИКТ).

II. Информационни и комуникационни технологии в рамките на системата на управление

2. Компетентният орган на застрахователя, съответно на презастрахователя, гарантира, че системата на управление на застрахователя, съответно на презастрахователя, и по-конкретно системата за управление на риска и системата за вътрешния контрол, адекватно управляват рисковете в областта на ИКТ и сигурността.

3. Компетентният орган на застрахователя, съответно на презастрахователя, гарантира, че числеността и уменията на служителите на застрахователя, съответно на презастрахователя, са достатъчни, за да осигурят постоянно потребностите му в областта на ИКТ и процесите по управление на риска в областта на ИКТ и сигурността, както и да гарантират изпълнението на стратегията в областта на ИКТ. Служителите редовно получават подходящо обучение относно рисковете в областта на ИКТ и сигурността, включително по информационна сигурност.

4. Компетентният орган на застрахователя, съответно на презастрахователя, гарантира, че ангажираните ресурси са подходящи за изпълнение на изискванията по т. 2 и 3.

III. Стратегия за ИКТ

5. Компетентният орган на застрахователя, съответно на презастрахователя, отговаря за определянето и одобряването на обща стратегия за ИКТ на застрахователя, съответно на презастрахователя, в писмена форма, като съгласувано допълнение към общата програма за дейността, а също така отговаря и за нейното оповестяване и изпълнение.

6. Стратегията за ИКТ определя най-малко:

6.1. развитието на ИКТ на застрахователя, съответно на презастрахователя, които подпомагат и изпълняват ефективно програмата за дейността, в това число, развитието на организационната структура, на бизнес моделите, на системата за ИКТ и на ключовите зависимости спрямо доставчици на услуги;

6.2. развитието на архитектурата на ИКТ, включително на зависимостите от доставчици на услуги;

6.3. ясни цели на информационната сигурност, съсредоточени върху системите и услугите, персонала и процесите в областта на ИКТ.

7. Застрахователят, съответно презастрахователят, гарантира, че стратегията за ИКТ се приема, прилага и съобщава своевременно на всички служители и доставчици на услуги, които имат отношение към нейното прилагане.

8. Застрахователят, съответно презастрахователят, създава процес за наблюдение и измерване на ефективността на прилагането на стратегията за ИКТ, който редовно преразглежда и при необходимост актуализира.

IV. Рискове в областта на ИКТ и сигурността в рамките на системата за управление на риска

9. Компетентният орган на застрахователя, съответно на презастрахователя, отговаря за създаването на ефективна система за управлението на риска в областта на ИКТ и сигурността като част от общата система за управление на риска на застрахователя, съответно на презастрахователя, като определя лимити за поемане на риск по отношение на тези рискове в съответствие с рисковата стратегия на застрахователя, съответно на презастрахователя, и изисква редовна вътрешна отчетност относно резултатите от процеса по управление на риска.

10. Като част от общата система за управление на рисковете, по отношение на риска в областта на ИКТ и сигурността застрахователят, съответно презастрахователят:

10.1. създава и редовно актуализира схема на бизнес процесите и дейностите, на бизнес функциите, правомощията, информационните активи и активите на ИКТ, за да установи тяхната важност и техните взаимозависимости спрямо риска в областта на ИКТ и сигурността;

10.2. установява и измерва всички относими рискове в областта на ИКТ и сигурността, на които е изложен и класифицира установените бизнес процеси и дейности, бизнес функции, правомощия, информационните активи и активите на ИКТ от гледна точка на тяхната критичност, както и оценява изискванията за защита най-малко по отношение поверителност, цялост и наличност на тези бизнес процеси и дейности, бизнес функции и правомощия и активи, като установява и титулярите на активи, които са отговорни за тяхно класифициране;

10.3. гарантира, че методите, използвани за определяне на критичността и на изискуемото равнище на защита, в частност - по отношение на целите за защита на целостта, наличността и поверителността, осигуряват изисквания към защитата, които са последователни и всеобхватни;

10.4. гарантира, че измерването на рисковете в областта на ИКТ и сигурността се извършва на базата на определени критерии за риска в областта на ИКТ и сигурността, като се вземат предвид критичността на неговите бизнес процеси и дейности, бизнес функции и правомощия, информационните активи и активите на ИКТ, степента на известните уязвимости и предварителни инциденти, които са засегнали застрахователя, съответно презастрахователя;

10.5. гарантира, че оценката на рисковете в областта на ИКТ и сигурността се извършва и документира редовно, а също така и преди всяка съществена промяна на инфраструктурата, процесите или процедурите, засягащи бизнес процесите и дейностите, бизнес функциите, правомощията, информационните активи и активите на ИКТ;

10.6. определя и прилага, на базата на оценка на риска, мерки за управление на идентифицираните рискове в областта на ИКТ и сигурността и защитава информационните активи в съответствие с тяхната класификация, включително като предвижда мерки за управление на оставащите остатъчни рискове.

11. Резултатите от процеса по управление на рисковете в областта на ИКТ и сигурността се одобряват от компетентния орган на застрахователя, съответно на презастрахователя, и се включват в процеса по управление на оперативния риск, като част от общото управление на риска на застрахователя, съответно на презастрахователя.

V. Проверка

12. Системите и процесите на застрахователя, съответно на презастрахователя, за управлението на риска и сигурността в областта на ИКТ подлежат на периодична проверка в съответствие с плана за проверки на застрахователя, съответно на презастрахователя от проверители с достатъчни знания, умения и опит по отношение на рисковете в областта на ИКТ и сигурността, за да осигурят независима увереност относно тяхната ефективност пред компетентния орган на застрахователя, съответно презастрахователя. Честотата и насочеността на такива проверки се съобразява със съответните рискове в областта на ИКТ и сигурността.

VI. Политика и мерки за информационна сигурност

13. Застрахователят, съответно презастрахователят, приема писмена политика за информационна сигурност, одобрена от неговия компетентен орган, която определя ръководните принципи и правила за защита на поверителността, целостта и наличността на информацията на застрахователя, съответно на презастрахователя, за да се осигури прилагането на стратегията за ИКТ.

14. Политиката включва описание на основните правомощия и отговорности за управление на информационната сигурност и установява изискванията по отношение на служителите, процесите и технологията във връзка с информационната сигурност, отчитайки, че служителите на всички равнища имат отговорности за гарантиране на информационната сигурност на застрахователя, съответно на презастрахователя.

15. Застрахователят, съответно презастрахователят, запознава всичките си служители с политиката и те са длъжни да я спазват и прилагат. Когато е приложимо, политиката се съобщава на и се прилага от доставчиците на услуги.

16. На базата на политиката застрахователят, съответно презастрахователят, разработва и прилага процедури и мерки за информационна сигурност, по-специално за намаляване на рисковете в областта на ИКТ и сигурността, на които са изложени. Процедурите и мерките за информационна сигурност включват всеки процес, описан в тези указания.

VII. Функция по информационна сигурност

17. Застрахователят, съответно презастрахователят, създава в рамките на системата на управление и при спазване на принципа за пропорционалност, функция по информационна сигурност и определя лице, което да я осъществява.

18. Застрахователят, съответно презастрахователят, гарантира независимостта и обективността на функцията за информационна сигурност, като я разграничава по подходящ начин от процесите по разработване на ИКТ и тяхното използване.

19. Функцията по т. 17 е подчинена на компетентния орган на застрахователя, съответно на презастрахователя.

20. Функцията по т. 17:

20.1. подпомага компетентния орган при определяне и поддържане на политиката за информационна сигурност и контрола при нейното прилагане;

20.2. докладва и съветва компетентния орган редовно и при поискване за състоянието на информационната сигурност и нейното развитие;

20.3. наблюдава и преглежда прилагането на мерките за информационна сигурност;

20.4. гарантира, че изискванията за информационна сигурност се спазват при използване на доставчици на услуги;

20.5. гарантира, че всички служители и доставчици на услуги, които достъпват информация и системи, са запознати с политиката за информационна сигурност, посредством обучение или инструктаж;

20.6. координира разследването на оперативни инциденти или инциденти по сигурността и докладва съответните случаи на компетентния орган.

VIII. Управление на идентичността и достъпа

21. Застрахователят, съответно презастрахователят, определя, документира и прилага процедури за логически контрол на достъпа или за логическа сигурност (управление на идентичността и достъпа) в съответствие с изискванията за защита по раздел IV. Застрахователят, съответно презастрахователят, привежда в изпълнение, наблюдава и периодично преразглежда процедурите по изречение първо, като включва в тях контроли за наблюдение на аномалии.

22. Процедурите по т. 21 включват най-малко следните елементи:

22.1. принципи за достъп до информация:

а) застрахователят, съответно презастрахователят, управлява правата на достъп, включително отдалечения достъп до информационните активи, и системите, които ги поддържат, на принципа „необходимост да се знае“;

б) потребителите получават минимални права на достъп, които са строго необходими за осъществяване на техните задължения (принцип на „минимална привилегия“), т.е. за предотвратяване на необоснован достъп до данни;

в) правата на достъп до данни трябва да се разграничат, така че да не може да се използват за заобикаляне на контролите (принцип за разграничаване на правомощията);

22.2. отчетност на потребителя: застрахователят, съответно презастрахователят, ограничава, колкото се може повече, употребата на общи или споделени потребителски профили и гарантира, че потребителите могат да бъдат установени и проследени до отговорното физическо лице или до конкретната позволена задача за действията им, извършени в системите за ИКТ по всяко време;

22.3. привилегировани права на достъп: застрахователят, съответно презастрахователят, прилага засилени контроли по отношение на привилегирования

достъп до системите, като строго ограничава и тясно контролира профилите с по-висок достъп до системите;

22.4. отдалечен достъп: за да се осигури сигурна комуникация и да се намали рискът, отдалечен достъп до критичните системи за ИКТ се предоставя само на базата на принципа „необходимост да се знае“ и като се прилагат засилени технологични решения за установяване на самоличността;

22.5. регистриране на действията на потребителите:

а) дейностите на потребителите се регистрират и наблюдават по начин, който е пропорционален на риска, като се обхващат най-малко потребителите с привилегирован достъп;

б) регистрите на достъпа се обезпечават, за да се предотврати непозволена поправка или заличаване на записи и се съхраняват за срокове съобразно критичността на идентифицираните бизнес функции, процеси и информационни активи в съответствие със сроковете, предвидени в закона или в правото на Европейския съюз;

в) информацията от регистрите се използва за установяване и разследване на неправомерни дейности, забелязани при предоставянето на услугите;

22.6. управление на достъпа: правата на достъп се предоставят, отнемат или променят своевременно съобразно предварително установени процедури за одобрение, като се включва съответният титуляр на информационен актив, като когато достъпът повече не е необходим, правата на достъп се отнемат незабавно;

22.7. оценка на достъпа: правата на достъп се преразглеждат периодично, за да се гарантира, че потребителите не разполагат с извънредни привилегии и че правата на достъп се отнемат или премахват, когато повече не са необходими;

22.8. даването, промяната, отнемането на права на достъп се документира по начин, който позволява проследяване и анализ;

22.9. методи за установяване на самоличност:

а) застрахователят, съответно презастрахователят, прилага методи за установяване на самоличността, които са достатъчно надеждни, за да гарантира адекватно и ефективно, че политиките и процедурите за контрол на достъпа се спазват;

б) методите за установяване на самоличността са съобразени с критичността на системите за ИКТ, информацията или процеса, който подлежи на достъпване, като това най-малко включва прилагане на силни пароли или на засилени методи за установяване на самоличност, включително двуфакторна идентификация, в зависимост от съответния риск.

23. По смисъла на т. 22 понятието „потребител“ включва и техническите потребители.

24. Застрахователят, съответно презастрахователят, ограничава посредством устройства електронния достъп до данни и системи за ИКТ до минимума, изискуем за предоставяне на съответната услуга.

IX. Физическа сигурност

25. Застрахователят, съответно презастрахователят, определя, документира и прилага мерки за физическа сигурност, включително мерки срещу изключване на електричество, пожар, наводнение и непозволен физически достъп, за да защити помещенията, центровете за съхранение на данни и чувствителните зони от непозволен достъп и от природни заплахи.

26. Физически достъп до системите за ИКТ се допуска само за оправомощени служители, които са подходящо обучени и подлежат на наблюдение. Застрахователят, съответно презастрахователят, периодично преразглежда предоставения физически

достъп, за да гарантира, че права на достъп, които вече не са необходими, се отнемат своевременно.

27. Мерките за защита срещу природни заплахи са съобразени с важността на сградите и с критичността на дейностите или на системите за ИКТ, разположени в тези сгради.

X. Сигурност на операциите в ИКТ

28. Застрахователят, съответно презастрахователят, прилага процедури, за да гарантира поверителност, цялост и наличност на системите в областта на ИКТ и на услугите в областта на ИКТ, за да намали въздействието на проблемите в областта на сигурността върху доставянето на услугите в областта на ИКТ.

29. Процедурите по т. 28 обхващат по подходящ начин следните мерки:

29.1. идентифициране на потенциални уязвимости, които следва да се оценят и на които следва да се противодейства, като се гарантира, че системите в областта на ИКТ са актуални, включително програмното осигуряване, предоставено от застрахователя, съответно от презастрахователя на вътрешните и външните потребители, посредством разполагане на доработки за сигурност, включително актуализация на дефиниции на антивирусни програми или чрез прилагане на компенсаторни контроли;

29.2. прилагане на сигурни базови линии за конфигурация за всички компоненти, като операционни системи, бази данни, рутери и превключватели;

29.3. прилагане на сегментация на мрежата, на системи за защита от изтичане на данни и криптиране на мрежовия трафик в съответствие с класификацията на информационните активи;

29.4. прилагане на защита по отношение на крайните точки, включително сървъри, работни станции и мобилни устройства, като застрахователят, съответно презастрахователят, оценява, дали крайните точки покриват стандартите за сигурност определени от тях, преди да им се даде достъп до корпоративната мрежа;

29.5. осигуряване на механизми за проверка на целостта за установяване на целостта на системите за ИКТ;

29.6. криптиране на неактивни данни и на данни в пренос в съответствие с класификацията на информационните активи.

XI. Наблюдение на сигурността

30. Застрахователят, съответно презастрахователят, създава и прилага процедури и процеси за постоянно наблюдение на дейностите, които въздействат на информационната му сигурност.

31. Наблюдението по т. 30 обхваща най-малко:

31.1. вътрешни и външни фактори, включително административните функции на дейността и на ИКТ;

31.2. транзакции на доставчици на услуги, на други субекти и на вътрешни потребители;

31.3. потенциални вътрешни и външни заплахи.

32. Застрахователят, съответно презастрахователят, въз основа на наблюдението по т. 31 прилага подходящи и ефективни методи за установяване, отчитане и реакция на аномални дейности и заплахи, като физическо или логическо проникване, нарушаване на поверителността, целостта и наличността на информационните активи, зловреден код и публично известни уязвимости на софтуера и техниката.

33. Отчетността от наблюдението на сигурността се използва от застрахователя, съответно от презастрахователя, за анализ на естеството на оперативните инциденти и

на инцидентите по сигурността, за установяване на тенденции и за обезпечаване на вътрешни разследвания, както и за обосноваване вземането на подходящи решения.

XII. Прегледи, оценки и изпитване на информационната сигурност

34. Застрахователят, съответно презастрахователят, извършва поредица от разнообразни прегледи, оценки и изпитвания, за да гарантира ефективното установяване на уязвимости в своите системи и услуги в областта на ИКТ, включително анализ на пропуски в съпоставка със стандарти за информационна сигурност, прегледи за спазване на изискванията, вътрешни и външни проверки на информационните системи и прегледи на физическата сигурност.

35. Застрахователят, съответно презастрахователят, разработва и прилага схема за изпитвания на информационната сигурност, която проверява надеждността и ефективността на мерките за информационна сигурност и гарантира, че тази схема взема предвид заплахите и уязвимостите, установени чрез наблюдение и чрез процеса на оценка на риска в областта на ИКТ и сигурността.

36. Изпитванията се извършват по безопасен и сигурен начин и от независими експерти с достатъчно знания, умения и опит в изпитването на мерки за информационна сигурност.

37. Застрахователят, съответно презастрахователят, извършва изпитвания редовно. Обхватът, честотата и методът на изпитване, включително изследване на проникването, както и изследване на проникване, предизвикано от заплаха, се съобразяват с равнището на установения риск. Изпитването на критични системи за ИКТ и сканиране за уязвимости се извършва ежегодно.

38. Застрахователят, съответно презастрахователят, гарантира, че изпитвания на мерките за сигурност се извършват в случай на промени в инфраструктурата, процесите и процедурите, както и ако се извършват промени в резултат на значителни оперативни инциденти или инциденти по сигурността или в резултат на пускане в експлоатация на нови или значително променени критични програмни продукти. Застрахователят, съответно презастрахователят, наблюдава и оценява резултатите от изпитванията на сигурността и актуализира мерките си за сигурност в съответствие с тях в срочен порядък, когато се отнася за критични системи за ИКТ.

XIII. Обучение и инструктиране по информационна сигурност

39. Застрахователят, съответно презастрахователят, разработва програми за обучение по информационна сигурност по отношение на всички служители включително членовете на управителния и на контролния му орган, за да гарантира, че всички са обучени да изпълняват своите задължения и правомощия, като се намаляват човешките грешки, кражбите, измамите, злоупотребите и загубите, както и други неправомерни или необосновани действия с цел гарантиране на информационната сигурност. Застрахователят, съответно презастрахователят, гарантира, че програмите за обучение осигуряват редовно обучение по отношение на всички служители.

40. Застрахователят, съответно презастрахователят, разработва и прилага периодични програми за инструктажи по информационна сигурност за обучаване на служителите, включително членовете на управителния и на контролния му орган, как да се отнасят с рисковете, свързани с информационната сигурност.

XIV. Управление на дейностите в областта на ИКТ

41. Застрахователят, съответно презастрахователят, управлява дейностите си в областта на ИКТ на базата на стратегията за ИКТ. Вътрешните документи на

застрахователя, съответно на презастрахователя, определят как той оперира, наблюдава и контролира системите в областта на ИКТ и услугите в областта на ИКТ, включително документирането на критичните процеси, процедури и дейности в областта на ИКТ.

42. Застрахователят, съответно презастрахователят, прилага процедури за регистриране и наблюдение по отношение на критичните дейности в областта на ИКТ, за да създаде условия за установяване, анализ и отстраняване на грешки.

43. Застрахователят, съответно презастрахователят, поддържа инвентаризационен опис на активите на ИКТ, който е достатъчно подробен, за да осигури бърза идентификация на всеки един актив, неговото разположение, класификация от гледна точка на сигурността и собственост.

44. Застрахователят, съответно презастрахователят, наблюдава и управлява жизнения цикъл на активите на ИКТ, за да гарантира, че те продължават да покриват изискванията за извършване на дейността и за управление на риска. Застрахователят, съответно презастрахователят, следи активите на ИКТ да се поддържат от техните доставчици или от разработчиците в рамките на предприятието и че всички доработки и актуализации се прилагат на базата на документиран процес. Рисковете, произтичащи от остарели или неподдържани активи на ИКТ, се оценяват и се прилагат мерки за тяхното намаляване. Застрахователят, съответно презастрахователят преработва и се освобождава от изведените от експлоатация активи на ИКТ по безопасен начин.

45. Застрахователят, съответно презастрахователят, прилага планиране на изпълнението, капацитета и процесите по наблюдение, за да установи, предотврати и отрази важни проблеми на функционирането на системите на ИКТ и недостатъци на капацитета на ИКТ своевременно.

46. Застрахователят, съответно презастрахователят, определя и прилага архивиране на данни и на системи на ИКТ и процедури за възстановяване, за да гарантира, че те могат да бъдат възобновени. Обхватът и честотата на архивирането се определя във връзка с изискванията за възобновяване на дейността и във връзка с критичността на данните и на системите на ИКТ, оценени в съответствие с извършената оценка на риска. Застрахователят, съответно презастрахователят, редовно извършва изпитвания на процедурите по архивиране и възобновяване.

47. Застрахователят, съответно презастрахователят, гарантира, че архивите на данните и на системите на ИКТ се съхраняват в едно или повече места, различни от основното място, които са сигурни и достатъчно отдалечени от основното място, за да се изключи излагането на едни и същи рискове.

XV. Управление на инциденти и проблеми в областта на ИКТ

48. Застрахователят, съответно презастрахователят, разработва и прилага в дейността си процес за управление на инциденти и проблеми, за да наблюдава и регистрира оперативни инциденти или инциденти по сигурността и да си осигури възможност да продължи или да възстанови критичните си работни функции или процеси, когато настъпят прекъсвания.

49. Застрахователят, съответно презастрахователят, определя подходящи критерии и прагове за класифициране на дадено събитие като оперативен инцидент или инцидент по сигурността, а също така и показатели за ранно предупреждение, които да служат като сигнал, за да се осигури ранно разкриване на тези инциденти.

50. За да се сведе до минимум въздействието на неблагоприятни събития и да се способства своевременното възстановяване, застрахователят, съответно презастрахователят, създава подходящи процеси и организационни структури, гарантиращи последователно и интегрирано наблюдение, преодоляване и последващи действия по повод на оперативни инциденти или инциденти по сигурността, с цел

установяване на причините, тяхното анализиране и предприемане на действия и мерки за корекция, които да предотвратят повторното настъпване на инцидента.

51. Застрахователят, съответно презастрахователят, осигурява процес за управление на инциденти и проблеми, който урежда най-малко:

51.1. процедурите за установяване, проследяване, регистриране, категоризиране и класифициране на инцидентите според приоритет, определен от застрахователя, съответно презастрахователя, и базиран на критичността на дейността и на договорите за услуги;

51.2. правомощията и отговорностите по отношение на различни сценарии за инциденти, включително грешки, неправилно функциониране, кибератаки;

51.3. процедура за управление на проблеми, по която застрахователят, съответно презастрахователят, установява, анализира и отстранява причините, стоящи в основата на един или повече инциденти, включително като се правят изводи и се актуализират мерките за сигурност;

51.4. ефективни планове за вътрешен обмен на информация, включително алармиране за инцидента и процедури за отнасяне на въпроса до по-високите управленски равнища, които обхващат и жалби от страна на ползватели на застрахователни услуги, разкриващи проблеми със сигурността, за да се гарантира, че:

а) инцидентите с възможно значително неблагоприятно въздействие върху критични системи в областта на ИКТ и услуги в областта на ИКТ се докладват пред съответните лица на ръководни длъжности;

б) компетентният орган е уведомен извънредно в случай на значителни инциденти и е получил информация най-малко относно въздействието, противодействието и допълнителните контроли, които трябва да се предвидят поради инцидента;

51.5. процедури за реакция в случай на инцидент, които да намалят въздействието, произтичащо от инциденти, и да гарантират, че услугата е функционална и надеждна в срочен порядък;

51.6. специфични външни комуникационни планове по отношение на критични функции и процеси на дейността с цел да:

а) се сътрудничи със съответните заинтересовани лица за ефективна реакция и възстановяване след инцидента;

б) предоставяне на навременна информация, включително отчет за инцидента пред външни лица, като:

аа) ползватели на застрахователни услуги, други пазарни участници, когато в резултат на инцидента се засягат техни права и интереси, произтичащи от отношенията им със застрахователя или презастрахователя;

бб) Комисията, във всеки случай по буква „аа“, както и когато инцидентът води до невъзможност за изпълнение в срок на задължения по силата на КЗ или на актовете по неговото прилагане, включително по силата на пряко приложимите актове на правото на Европейския съюз;

вв) други държавни органи, когато това е предвидено в специален закон.

XVI. Управление на проекти в областта на ИКТ

52. Застрахователят, съответно презастрахователят, разработва методология за проекти в областта на ИКТ с адекватен процес за управление и адекватно ръководство за внедряване на проектите, за да се способства ефективно прилагането на стратегията за ИКТ посредством проекти в областта на ИКТ.

53. Застрахователят, съответно презастрахователят, наблюдава по подходящ начин и взема мерки за намаляване на рисковете, произтичащи от портфейла проекти в областта на ИКТ, като взема предвид и рисковете, които могат да произтекат от

взаимозависимости между различни проекти и от зависимости на множество проекти от едни и същи ресурси и експертни умения.

XVII. Придобиване и разработване на системи в областта на ИКТ

54. Застрахователят, съответно презастрахователят, разработва и прилага процес, регулиращ разработването и поддържането на системите в областта на ИКТ, за да осигури, че поверителността, целостта и наличността на данните, подлежащи на обработка, са всеобхватно гарантирани и че определените изисквания за защита са спазени. Процесът се проектира, като се използва подход, основан на риска.

55. Застрахователят, съответно презастрахователят, осигурява, че преди придобиването на системи, съответно преди започване на действия по тяхното разработване се определят ясно функционалните и нефункционалните изисквания, в това число изискванията за информационна сигурност, както и техническите цели.

56. Застрахователят, съответно презастрахователят, осигурява, че са взети мерки за предотвратяване на неумишлена промяна или на целенасочена манипулация на системите в областта на ИКТ в процеса на разработка.

57. Застрахователят, съответно презастрахователят, разполага с методология за изпитване и одобряване на системи в областта на ИКТ, на услуги в областта на ИКТ и на мерки за информационна сигурност.

58. Застрахователят, съответно презастрахователят, по подходящ начин изпитва системи в областта на ИКТ, услуги в областта на ИКТ и мерки за информационна сигурност, за да установи потенциални слабости, нарушения и инциденти в областта на сигурността.

59. Застрахователят, съответно презастрахователят, осигурява разграничение на производствената среда от разработването, изпитването и другите непроизводствени среди.

60. Застрахователят, съответно презастрахователят, прилага мерки за защита на целостта на изходния код (source code), когато разполага с такъв, за системите в областта на ИКТ. Застрахователят, съответно презастрахователят, документира разработването, прилагането, функционирането и/или конфигурирането на системите в областта на ИКТ по всеобхватен начин, за да се намали ненужната зависимост от експерти в съответната област.

61. Процесите за придобиване и разработване на системи в областта на ИКТ на застрахователя, съответно на презастрахователя, се прилагат и по отношение на системи в областта на ИКТ, разработвани или управлявани от крайни потребители на бизнес функцията извън организацията на ИКТ, като се прилага подход, основан на риска. Застрахователят, съответно презастрахователят, поддържа регистър на приложенията по изречение първо, които осигуряват критични функции и процеси на дейността.

XVIII. Управление на промяна в ИКТ

62. Застрахователят, съответно презастрахователят, разработва и прилага процес за промяна в ИКТ, за да осигури, че всички промени на системите в областта на ИКТ се описват, оценяват, изпитват, одобряват, разрешават и прилагат по контролиран начин. Промените в спешни или извънредни ситуации подлежат на проследяване и се съобщават след извършването им на съответния титуляр на актив за последващ анализ.

63. Застрахователят, съответно презастрахователят, определя дали промените в съществуващата оперативна среда въздействат върху съществуващите мерки за сигурност или изискват приемането на допълнителни мерки за намаляване на свързаните

с тях рискове. Тези промени трябва да бъдат в съответствие с процеса за управление на промените на застрахователя, съответно на презастрахователя.

XIX. Управление на непрекъснатостта на дейността

64. Компетентният орган на застрахователя, съответно на презастрахователя, разработва и одобрява политика за непрекъснатостта на ИКТ и взема мерки за запознаването с политиката и нейното изпълнение в рамките на предприятието.

65. Политиката за непрекъснатостта на ИКТ по т. 64 се прилага спрямо съответните служители на застрахователя, съответно на презастрахователя, и спрямо доставчиците им на услуги.

XX. Анализ на въздействието върху дейността

66. Като част от надеждното управление на непрекъснатостта на дейността застрахователят, съответно презастрахователят, извършва количествен и качествен анализ на въздействието върху дейността, за да оцени доколко застрахователят, съответно презастрахователят, е изложен на риска от тежки прекъсвания на дейността и тяхното потенциално въздействие, като използва вътрешни и/или външни данни, и като прави анализ на сценарии.

67. При анализа на въздействието върху дейността се взема предвид критичността на установените и класифицирани процеси и дейности, функции на дейността, правомощия и информационни активи, и активи на ИКТ и техните взаимозависимости в съответствие с Раздел IV.

68. Застрахователят, съответно презастрахователят, осигурява, че неговите системи в областта на ИКТ и услуги в областта на ИКТ са проектирани и съобразени в съответствие с неговия анализ, включително като се съкратят някои критични компоненти, за да се предотвратят прекъсвания, причинени от събития, засягащи тези компоненти и др.

XXI. Планиране на непрекъснатостта на дейността

69. В общата си политика за непрекъснатост на дейността по чл. 258, параграф 3 от Делегиран регламент (ЕС) 2015/35 на Комисията от 10 октомври 2014 година 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.) застрахователят, съответно презастрахователят, обсъжда съществените рискове, които могат да засегнат неблагоприятно системите в областта на ИКТ и услугите в областта на ИКТ. Планът осигурява постигането на целите за защита и, ако е необходимо, за възстановяване на поверителността, целостта и наличността на процесите и дейностите, на функциите на дейността, правомощията и информационните активи и активите на ИКТ. Застрахователят, съответно презастрахователят, сътрудничи със съответните вътрешни и външни заинтересовани лица при разработването на този план.

70. Застрахователят, съответно презастрахователят, създава плана за непрекъснатост на дейността, за да осигури, че може да реагира по подходящ начин на потенциални сценарии на прекъсване в рамките на целевото време за възстановяване и на целевата точка за възстановяване.

71. Застрахователят, съответно презастрахователят, предвижда в плана за непрекъснатост на дейността поредица от различни сценарии, включително крайни, но правдоподобни сценарии и сценарии на кибератаки и оценява потенциалното въздействие на такива сценарии. Въз основа на тези сценарии застрахователят, съответно

презастрахователят, описва как се осигурява непрекъснатостта на системите и услугите в областта на ИКТ и информационната му сигурност на застрахователя, съответно на презастрахователя.

XXII. Планове за реакция и за възстановяване

72. Въз основа на анализа на въздействието върху дейността и правдоподобни сценарии застрахователят, съответно презастрахователят, разработва планове за реакция и за възстановяване. Тези планове определят условията, при които се задействат, и действията, които трябва да се предприемат, за да се осигури целостта, наличието, непрекъснатостта и възстановяването най-малко на критичните системи и услуги в областта на ИКТ на застрахователя, съответно на презастрахователя, както и на данните. Плановете за реакция и възстановяване целят да постигнат целевото време и целевата точка за възстановяване на дейността на застрахователя, съответно на презастрахователя.

73. Застрахователят, съответно презастрахователят, разработва плановете за реакция и възстановяване в краткосрочни и дългосрочни варианти.

74. Плановете за реакция и възстановяване най-малко:

74.1. предвиждат възстановяването на важните услуги в областта на ИКТ, на функциите на дейността, на поддържащите процеси, на информационните активи и техните взаимозависимости с цел избягване на неблагоприятни въздействия върху функционирането на застрахователя, съответно на презастрахователя;

74.2. се документират и предоставят на оперативните и поддържащи звена, както и са достъпни в случай на извънредна ситуация, като включват ясно определяне на правомощията и отговорностите;

74.3. подлежат на непрекъсната актуализация в съответствие с опита от инциденти, изпитвания, новоустановени рискове и заплахи, промени в целевото време и целевата точка за възстановяване на дейността на застрахователя, съответно на презастрахователя, както и в съответствие с промяна на приоритетите.

75. Плановете също така предвиждат алтернативни възможности, когато възстановяването не може да бъде постигнато в кратък срок, поради висока цена, рискове, логистика или непредвидени обстоятелства.

76. Като част от плановете за реакция и възстановяване, застрахователят, съответно презастрахователят, предвижда и прилага мерки за осигуряване на непрекъснатост, за да се намали ефектът от неизпълнение от страна на доставчици на услуги, които са от ключово значение за непрекъснатостта на услугите в областта на ИКТ на застрахователя, съответно на презастрахователя в съответствие с изискванията 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).

XXIII. Изпитвания на плановете

77. Застрахователят, съответно презастрахователят, изпитва плана за непрекъснатост на дейността и осигурява, че работата на неговите процеси и дейности, на функциите на дейността, правомощия, информационни активи и активи на ИКТ и техните взаимозависимости, включително доставяните от доставчици на услуги, редовно подлежат на изпитване въз основа на рисковия профил на застрахователя, съответно на презастрахователя.

78. Застрахователят, съответно презастрахователят, актуализира плановете за непрекъснатост на дейността, на базата на резултатите от изпитванията, текущото проучване на рисковете и опита от предходни събития. Всякакви промени в целевото

време и целевата точка за възстановяване на дейността на застрахователя, съответно на презастрахователя или промени в работните процеси и дейности, във функциите на дейността, правомощията, информационните активи и активите на ИКТ също се включват при актуализацията на плановете.

79. Изпитванията на плановете за непрекъснатост на дейността показват тяхната възможност да поддържат жизнеспособността на дейността до възстановяване на критичните дейности на предварително определени нива, на качество на услугата или на издръжливост на външно въздействие.

80. Застрахователят, съответно презастрахователят, гарантира, че:

80.1. резултатите от изпитванията се документират;

80.2. слабостите, установени при изпитванията, се анализират;

80.3. се вземат съответните мерки за преодоляване на установените слабости;

80.4. се предоставя отчет за изпитванията и резултатите от тях пред компетентния орган.

XXIV. Комуникация при кризи

81. В случай на прекъсване или извънредна ситуация, както и по време на прилагане на планове за непрекъснатост на дейността, застрахователят, съответно презастрахователят, осигурява ефективни мерки за комуникация при кризи, така че всички относими вътрешни и външни заинтересовани лица, както и Комисията, други надзорни органи и доставчиците на услуги да получават информация по подходящ начин.

XXV. Възлагане на доставчици на услуги в областта на ИКТ и системи в областта на ИКТ

82. Когато услуга в областта на ИКТ и системи в областта на ИКТ се възлагат на доставчик на услуги, застрахователят, съответно презастрахователят, осигурява спазването на изискванията на настоящите указания за съответната услуга в областта на ИКТ или система в областта на ИКТ в допълнение към изискванията 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) .

83. В случай на възлагане на критични или важни функции, застрахователят, съответно презастрахователят, гарантира, че договорните задължения на доставчика на услуги включват най-малко следното:

83.1. подходящи и пропорционални цели и мерки за информационна сигурност, включително изисквания като минимални изисквания за информационна сигурност, спецификация на жизнения цикъл на данните на застрахователя, съответно на презастрахователя, права за достъп и проверка, изисквания за разположение на центровете за данни, изисквания за криптиране на данните, за мрежова сигурност и за процеси за наблюдение на сигурността;

83.2. споразумения за равнище и качество на услугата, за да се гарантира непрекъснатост на услугите в областта на ИКТ и системите в областта на ИКТ, както и целеви стойности на изпълнението при нормални условия и в условията на планове за извънредни ситуации - в случай на прекъсване на услугата;

83.3. процедури за работа в случай на оперативен инцидент или инцидент по сигурността, включително за подаване на информация към по-високо управленско равнище и за отчетност.

84. Застрахователят, съответно презастрахователят, наблюдава и изисква гаранции относно равнището на спазване на поставените от него цели, мерки и целеви показатели на изпълнението от страна на доставчиците на услуги.

XXVI. Дефиниции

85. По смисъла на тези указания:

85.1. „Актив на информационна или комуникационна технология (актив на ИКТ)“ е актив, представляващ софтуер или хардуер, намиращ се в бизнес средата“.

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

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

85.4. „Изследване на проникване, предизвикано от заплаха“ е контролиран опит за застрашаване на киберустойчивостта на един субект чрез симулиране на тактики, техники и процедури на реални причинители на заплаха. Той се базира на целенасочено застрашаване и се съсредоточава върху служителите, процесите и технологиите на субекта с минимално предварително разкриване на информация и въздействие върху дейността.

85.5. „Информационен актив“ е материален или нематериален набор от информация, който си заслужава да бъде защитаван.

85.6. „Информационна сигурност“ е запазването на поверителността, целостта и наличността на информацията и/или на информационните системи. Допълнителни характеристики на информационната сигурност са запазване на автентичността, отговорността, липсата на отхвърляне и надеждността.

85.7. „Кибер атака“ е всякакъв вид хакерство, водещо до нападение/ злонамерен опит за разрушаване, разкриване, промяна, обезвреждане, кражба или получаване на непозволен достъп до или непозволено използване на информационен актив, което има за цел информационни или комуникационни системи.

85.8. „Кибер сигурност“ е запазване на поверителността, целостта и наличността на информация и/или на информационни системи посредством киберсредства.

85.9. „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.

85.10. „Наличност“ е характеристиката на достъпност и използваемост на информацията при поискване (навременност) от страна на оправомощен субект.

85.11. „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 (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.

85.12. „Оперативен инцидент или инцидент по сигурността“ е единично събитие или серия от свързани непланирани събития, които имат или вероятно ще имат неблагоприятно въздействие върху целостта, наличността и поверителността на системите и услугите в областта на ИКТ.

85.13. „Поверителност“ е характеристиката, че информацията не се предоставя, нито се предоставя на неоправомощени лица, субекти, процеси или системи.

85.14. „Проекти в областта на ИКТ“ са всеки проект или част от такъв проект, където системи и услуги в областта на ИКТ се променят, преместват или прилагат.

85.15. „Риск в областта на ИКТ и сигурността“ е подкомпонент на оперативния риск; риск от загуба поради нарушаване на поверителността, незапазване на целостта на системи и данни, неадекватност или неналичност на системи и данни или невъзможност да се промени ИКТ в рамките на разумно време и разходи, когато средата или изискванията за дейността се променят (т.е. липса на пъргавина). Това включва киберрисковете, а също така рискове за сигурността на информацията в резултат на неадекватни или несработващи вътрешни процеси или външни събития, включително кибератаки или неадекватна физическа сигурност.

85.16. „Системи в областта на ИКТ“ са набор от устройства, услуги, активи на информационни технологии, активи на ИКТ или други компоненти за боравене с информация, които включват и оперативната среда.

85.17. „Титуляр на актив на ИКТ“ – лице, което има отговорност и власт по отношение на актив на ИКТ.

85.18. „Услуги в областта на ИКТ“ са услугите предоставяне посредством системите и доставчиците на услуги в областта на ИКТ на един или повече вътрешни или външни потребители.

85.19. „Уязвимост“ е слабост, податливост или недостатък на актив или контрола, които могат да бъдат използвани от една или повече заплахи.

85.20. „Целевото време за възстановяване“ е максималното време, в рамките на което система или процес трябва да бъдат възстановени след настъпване на инцидент.

85.21. „Целевата точка за възстановяване“ е максималният период, в рамките на който могат да бъдат загубени данни в случай на инцидент на предварително определено равнище на услугата.

85.22. „Цялост“ е характеристиката на точност и пълнота на информацията.

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

Председател: Бойко Атанасов