

Насоки

за възлагане на дейности на външни доставчици на компютърни услуги „в облак“

Съдържание

1	Обхват	3
2	Нормативни документи, съкращения и определения	4
2.1	Препратки към законодателни актове	4
2.2	Съкращения	5
2.3	Определения	5
3	Цел	7
4	Задължения за спазване на насоките и изисквания за докладване	8
4.1	Статус на насоките	8
4.2	Изисквания за докладване	8
5	Насоки за възлагане на дейности на доставчици на услуги в облак	8
	Насока 1. Управление, надзор и документация	8
	Насока 2. Анализ преди възлагане на дейности на външен доставчик и комплексна проверка	11
	Насока 3. Основни договорни елементи	13
	Насока 4. Информационна сигурност	14
	Насока 5. Стратегии за оттегляне	16
	Насока 6. Права на достъп и одит	17
	Насока 7. Възлагане на дейности на подизпълнители	19
	Насока 8. Писмено уведомяване на компетентните органи	20
	Насока 9. Надзор на споразумения за възлагане на услуги в облак на външни доставчици	21

1 Обхват

Кой?

1. Настоящите насоки се прилагат за компетентните органи и за i) депозитарите на алтернативни инвестиционни фондове (АИФ), посочени в член 21, параграф 3, буква в) и в член 21, параграф 3, трета алинея от ДЛУАИФ, когато те не са финансови субекти, за които се прилага DORA, и ii) депозитарите на ПКИПЦК, посочени в член 23, параграф 2, буква в) от Директивата за ПКИПЦК, когато те не са финансови субекти, за които се прилага DORA.¹

Какво?

2. Настоящите насоки се прилагат по отношение на следните разпоредби:
 - а) По отношение на депозитарите на АИФ: член 21 от ДЛУАИФ; член 98 от Делегиран регламент (ЕС) 2013/231 на Комисията;
 - б) По отношение на депозитарите на ПКИПЦК: членове 22 и 22а, член 23, параграф 2 от Директивата за ПКИПЦК; член 32 от Директива 2010/43/ЕС на Комисията; Член 2, параграф 2, буква й), член 3, параграф 1, член 13, параграф 2, членове 15, 16 и 22 от Делегиран регламент (ЕС) 2016/438 на Комисията.

Кога?

3. Настоящите насоки се прилагат от датата на публикуването им на уебсайта на ЕОЦКП на всички официални езици на ЕС и за всички споразумения за възлагане на услуги в облак на външни изпълнители, сключени, подновени или изменени на тази дата или след нея.
4. С оглед на прилагането на DORA предишните насоки на ЕОЦКП относно възлагането на дейности на доставчици на услуги в облак престават да се прилагат за финансовите субекти, за които се прилага DORA, посочени в член 2 от същия регламент. За депозитарите на АИФ и за депозитарите на ПКИПЦК, посочени в параграф 1 по-горе, предишните насоки на ЕОЦКП относно възлагането на дейности на доставчици на услуги в облак ще продължат да се прилагат до датата на публикуване на настоящите насоки на уебсайта на ЕОЦКП на всички официални езици на ЕС.

¹ По отношение на договореностите за използване на облачни услуги, финансовите субекти, определени в член 2, параграфи 1 и 2 от Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета относно цифровата оперативна устойчивост за финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (регламент DORA), са обект на специфичните правила, установени в регламента DORA и съответните делегирани и изпълнителни регламенти на Комисията.

2 Нормативни документи, съкращения и определения

2.1 Препратки към законодателни актове

Регламент за ESMA	Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за ценни книжа и пазари), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/77/ЕО на Комисията ²
Директива за ЛУАИФ	Директива 2011/61/ЕС на Европейския парламент и на Съвета от 8 юни 2011 г. относно лицата, управляващи алтернативни инвестиционни фондове и за изменение на директиви 2003/41/ЕО и 2009/65/ЕО и на регламенти (ЕО) № 1060/2009 и (ЕС) № 1095/2010 ³
Делегиран регламент (ЕС) 2013/231 на Комисията	Делегиран регламент (ЕС) 2013/231 на Комисията от 19 декември 2012 г. за допълване на Директива 2011/61/ЕС на Европейския парламент и на Съвета по отношение на освобождаванията, общите условия във връзка с дейността, депозитарите, ливъриджа, прозрачността и надзора ⁴
Директивата за ПКИПЦК	Директива № 2009/65/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно координирането на законовите, подзаконовите и административните разпоредби относно предприятията за колективно инвестиране в прехвърлими ценни книжа (ПКИПЦК) ⁵
Директива 2010/43/ЕС на Комисията	Директива 2010/43/ЕС на Комисията от 1 юли 2010 г. за прилагане на Директива 2009/65/ЕО на Европейския парламент и на Съвета по отношение на организационните изисквания, конфликтите на интереси, правилата за поведение, управлението на риска и съдържанието на споразумението между депозитар и управляващо дружество ⁶ .

² ОВ L 331, 15.12.2010 г., стр. 84.

³ ОВ L 174, 12.1.2011 г., стр. 36.

⁴ ОВ L 83, 23.2.2013 г., стр. 1.

⁵ ОВ L 302, 17.11.2009 г., стр. 32.

⁶ ОВ L 176, 10.7.2010 г., стр. 42.

ДОРА	Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) No 1060/2009, (ЕС) No 648/2012, (ЕС) No 600/2014, (ЕС) No 909/2014 и (ЕС) 2016/1011 ⁷
ОРЗД	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) ⁸

2.2 Съкращения

<i>CSP</i>	Доставчик на услуги в облак
<i>ESMA</i>	Европейски орган за ценни книжа и пазари
<i>ЕС</i>	Европейски съюз

2.3 Определения

<i>функция</i>	означава всички процеси, услуги или дейности;
<i>Критична или важна функция</i>	означава всяка функция, чийто дефект или неизправност в нейното изпълнение биха увредили съществено: а) спазването от страна на посредника на задълженията му съгласно приложимото законодателство; б) финансовите резултати на посредника; или в) надеждността или непрекъснатостта на основните услуги и дейности на посредника;

⁷ ОВ L 333, 27.12.2022 г., стр. 1—79.

⁸ ОВ L 119, 4.5.2016 г., стр. 1—88

<i>услуги „в облак“</i>	означава услуги, предоставяни чрез изчисления в облак;
<i>изчислителни облаци или изчислителни облаци⁹</i>	означава парадигма за осигуряване на мрежов достъп до мащабируем и еластичен набор от физически или виртуални ресурси, които могат да бъдат споделяни (например сървъри, операционни системи, мрежи, софтуер, приложения и оборудване за съхранение), с предоставяне на самообслужване и администриране при поискване;
<i>доставчик на облачни услуги</i>	означава трета страна, предоставяща услуги в облак съгласно споразумение за възлагане на услуги в облак на външни изпълнители;
<i>споразумение за аутсорсинг на облачни услуги</i>	означава договореност под каквато и да е форма, включително договорености за делегиране, между: (i) дружество и ДУУ, чрез които този ДУУ изпълнява функция, която в противен случай би била поета от самото дружество; или (ii) дружество и трета страна, която не е ДУУ, но която разчита в значителна степен на ДУУ, за да изпълнява функция, която в противен случай би била предприета от самото дружество. В този случай позоваването на „ДУО“ в настоящите насоки следва да се разбира като позоваване на такава трета страна.
<i>вторично възлагане на дейности на външни изпълнители</i>	означава ситуация, при която ДУУ допълнително прехвърля възложената на външен изпълнител функция (или част от тази функция) на друг доставчик на услуги съгласно договореност за възлагане на дейности на външен изпълнител;

⁹ Изчислителните облаци често се съкращават като „облак“. Терминът „облак“ се използва в останалата част от документа за по-лесна справка.

модел за внедряване в облак означава начинът, по който облакът може да бъде организиран въз основа на контрола и споделянето на физически или виртуални ресурси. Моделите за внедряване в облак включват общностни, 10 хибридни, 11 частни 12 и публични 13 облаци;

посредници

- а) депозитарите, посочени в член 21, параграф 3, буква в) и в член 21, параграф 3, трета алинея от ДЛУАИФ („депозитарите на алтернативни инвестиционни фондове (АИФ)“);
- б) депозитарите, посочени в член 23, параграф 2, буква в) от Директивата за ПКПЦК („депозитарите на ПКПЦК“).

3 Цел

5. Настоящите насоки се основават на член 16, параграф 1 от Регламента за създаване на Европейски орган за ценни книжа и пазари (ESMA). Целта на настоящите насоки е да бъдат установени последователни, ефикасни и ефективни надзорни практики в рамките на Европейската система за финансов надзор и да се гарантира общо, уеднаквено и последователно прилагане на изискванията, посочени в Раздел 1.1 под заглавието „Какво?“, когато се възлагат дейности на CSP от посредници. По-специално целта на насоките е да помогнат на посредниците и на компетентните органи да установяват, разглеждат и наблюдават рисковете и предизвикателствата, свързани със споразуменията за възлагане на дейности в облак на външни доставчици, от вземането на решение за възлагане на дейности на външни доставчици, избора на доставчик на услуги в облак, наблюдението на дейностите, възложени на външни доставчици, до осигуряването на стратегии за оттегляне.

¹⁰ модел за внедряване в облак, при който услугите в облак се поддържат изключително и се споделят от конкретна група клиенти на услуги в облак, които имат общи изисквания и отношения помежду си, и при който ресурсите се контролират от поне един член на тази група;

¹¹ Модел за внедряване в облак, който използва най-малко два различни модела за внедряване в облак

¹² Модел за внедряване на облачни услуги, при който облачните услуги се използват изключително от един клиент на облачна услуга и ресурсите се контролират от този клиент на облачна услуга

¹³ Модел за внедряване на облачни услуги, при който облачните услуги са потенциално достъпни за всеки клиент на облачни услуги и ресурсите се контролират от доставчика на облачни услуги

4 Задължения за спазване на насоките и изисквания за докладване

4.1 Статус на насоките

6. Съгласно член 16, параграф 3 от Регламента за ESMA компетентните органи и посредниците полагат всички усилия за спазване на настоящите насоки.
7. Компетентните органи, за които се отнасят настоящите насоки, следва да ги спазват, като ги включат в националните си правни и/или надзорни практики, както е целесъобразно, включително когато определени насоки са насочени предимно към посредници. В такива случаи компетентните органи следва да гарантират чрез своя надзор, че посредниците спазват насоките.

4.2 Изисквания за докладване

8. До два месеца след датата на публикуване на насоките на интернет страницата на ESMA на всички официални езици на ЕС компетентните органи, за които се отнасят настоящите насоки, уведомяват ESMA за това дали i) спазват, ii) не спазват, но възнамеряват да спазват, или iii) не спазват и не възнамеряват да спазват насоките.
9. В случай че не спазват насоките, до два месеца след датата на публикуване на насоките на интернет страницата на ESMA на всички официални езици на ЕС компетентните органи уведомяват също така ESMA за мотивите си да не спазват насоките. На интернет страницата на ESMA е публикуван образец за уведомленията. Попълненият образец се изпраща до ESMA.
10. От посредниците не се изисква да докладват дали спазват настоящите насоки.

5 Насоки за възлагане на дейности на доставчици на услуги в облак

Насока 1. Управление, надзор и документация

11. Посредникът следва да има определена и актуална стратегия за възлагане на услуги в облак на външни доставчици, която да е съгласувана със съответните стратегии на посредника и вътрешните политики и процеси, включително по отношение на информационните и комуникационните технологии, информационната сигурност и управлението на оперативния риск.

12. Посредникът трябва:

- а) ясно да определи отговорностите за документацията, управлението и контрола на споразуменията за възлагане на дейности на външни доставчици в своята организация;
- б) да разпредели достатъчно ресурси, за да осигури спазване на тези насоки и всички правни изисквания, приложими по отношение на неговите споразумения за възлагане на услуги в облак на външни доставчици;
- в) да създаде функция за надзор на възлагането на дейности в облак на външни доставчици или да определи членове на ръководния персонал, които пряко да се отчитат пред ръководния орган и да отговарят за управлението и надзора на рисковете, свързани със споразуменията за възлагане на услуги в облак на външни доставчици. При спазването на тази насока посредниците следва да вземат предвид естеството, мащаба и сложността на своята дейност, включително с оглед на риска за финансовата система и рисковете, присъщи на функциите, възлагани на външни доставчици, и да се уверят, че техният ръководен орган има съответните технически умения да разбира рисковете във връзка със споразуменията за възлагане на услуги в облак на външни доставчици. Малките посредници с по-малко сложна структура следва най-малкото да осигурят ясно разделение на задачите и отговорностите за управлението и надзора на споразуменията за възлагане на услуги в облак на външни доставчици.

13. Посредникът следва да наблюдава изпълнението на дейностите, мерките за сигурност и спазването на договорените нива на услугите от своите CSP. Това наблюдение следва да се основава на риска, с основна насоченост към възложените на външни доставчици критични или важни функции.

14. Посредникът следва периодично да преоценява дали неговите споразумения за възлагане на услуги в облак на външни доставчици се отнасят за критична или важна функция, и дали рискът, естеството или мащабът на функцията, възложена на външен доставчик, се е променила съществено.

15. Посредникът следва да поддържа актуален регистър с информация за всички свои споразумения за възлагане на услуги в облак на външни доставчици, като разграничи възлагането на критични или важни функции на външни доставчици от останалите споразумения за възлагане на дейности на външни доставчици. Когато възлагането на критични или важни функции на външни доставчици се разграничава от останалите споразумения за възлагане на дейности на външни доставчици, трябва да се представи кратко резюме на причините защо възложената на външен доставчик функция се счита или не се счита за критична или важна. Като се има предвид националното законодателство, посредникът следва също така да води дневник за прекратените споразумения за възлагане на услуги в облак на външни доставчици за определен период от време.

16. За споразуменията за възлагане на услуги в облак на външни доставчици, отнасящи се за критични или важни функции, регистърът следва да включва поне следната информация за всяко споразумение за възлагане на услуги в облак на външни доставчици:

- а) референтен номер;
- б) началната дата и, ако е целесъобразно, следващата дата на подновяване на договора, крайната дата и/или сроковете за предизвестие за доставчика на услуги в облак и за посредника;
- в) кратко описание на възложената на външен доставчик функция, включително данните, предоставени на външен доставчик, и дали те включват лични данни (напр. чрез посочване на „да“ или „не“ в отделно поле за данни);
- г) категория, определена от посредника, която отразява естеството на възложената на външен доставчик функция (напр. информационни технологии, функция по управление), която следва да помогне за установяването на различните типове споразумения за възлагане на услуги в облак на външни доставчици;
- д) дали възложената на външен доставчик функция подпомага дейности, които са критични по отношение на времето;
- е) името и търговското наименование (ако има такова) на CSP, държава на регистрация, корпоративен регистрационен номер, идентификатор на юридическо лице (ако е приложимо), адрес на управление, съответни данни за контакт и наименованието на неговото дружество майка (ако има такова);
- ж) приложимото право на споразумението за възлагане на услуги в облак на външни доставчици и, изборът на юрисдикция, ако е направен такъв;
- з) вида облачни услуги и модели на разполагане и специфичния характер на съхраняваните данни и местата (по-конкретно региони или държави), където могат да се съхраняват такива данни;
- и) датата на последната оценка на критичността или важността на възложената на външен доставчик функция и датата на следващата планирана оценка;
- к) датата на последната оценка/одит на риска на CSP, заедно с кратко резюме на основните резултати, и датата на следващата планирана оценка/одит на риска;
- л) лицето или органа за вземане на решения при посредника, одобрили споразумението за възлагане на услуги в облак на външни доставчици;
- м) когато е приложимо, имената на всеки подизпълнител, на когото е възложена критична или важна функция (или съществени части от нея), включително държавите на регистрация подизпълнителите, където ще се извършва услугата, и местата (региони или държави), където ще се съхраняват данни;
- н) прогнозната стойност на годишния бюджет на споразумението за възлагане на услуги в облак на външни доставчици.

17. За споразумения за възлагане на услуги в облак на външни доставчици относно функции, които не са критични или важни, посредникът следва да определи

информацията, която да се включи в регистъра според естеството, мащаба и сложността на рисковете, присъщи на възложената функция.

Насока 2. Анализ преди възлагане на дейности на външен доставчик и комплексна проверка

18. Преди сключването на споразумение за възлагане на услуги в облак на външни доставчици всеки посредник следва:

- а) да направи оценка дали споразумението за възлагане на услуги в облак на външни доставчици се отнася за критична или важна функция;
- б) да установи и оцени всички съответни рискове на споразумението за възлагане на услуги в облак на външни доставчици;
- в) да извърши подходяща комплексна проверка на бъдещия CSP;
- г) да установи и оцени всеки конфликт на интереси, който може да възникне при възлагането на дейности на външни доставчици.

19. Анализът преди възлагането на дейности на външен доставчик и комплексната проверка на съответните CSP следва да са пропорционални на естеството, мащаба и сложността на функцията, която посредникът възнамерява да възложи на външен доставчик, и на рисковете, присъщи на тази функция. Това следва да включва най-малко оценка на потенциалното въздействие на споразумението за възлагане на услуги в облак на външни доставчици върху оперативните, правните рискове, риска от неспазване на нормативните изисквания и от накърняване на репутацията.

20. Ако споразумението за възлагане на услуги в облак на външни доставчици се отнася за критични или важни функции, посредникът следва също така:

- а) да оцени всички съответни рискове, които могат да възникнат във връзка със споразумението за възлагане на услуги в облак на външни доставчици, включително рискове по отношение на информационните и комуникационните технологии, информационната сигурност, непрекъснатостта на дейността, законосъобразността, рисковете от накърняване на репутацията, оперативните рискове и възможните ограничения на надзора за посредника, възникващи от:
 - i. избраните облачни услуги и предложените модели на разполагане;
 - ii. процесите на миграция и/или изпълнение;
 - iii. чувствителността на функцията и свързаните данни, които се обмисля да бъдат възложени, и мерките за сигурност, които следва да се вземат;
 - iv. оперативната съвместимост на системите и приложенията на посредника и CSP, а именно техният капацитет да обменят информация и да използват взаимно обменяната информация;

- v. преносимостта на данните на посредника, а именно капацитета за лесно прехвърляне на данните на посредника от един CSP на друг или обратно към посредника;
 - vi. политическата стабилност, сигурността и правната система (включително въведените разпоредби за правоприлагане, законодателните разпоредби за неплатежоспособност, които ще се прилагат в случай на несъстоятелност на CSP, действащото законодателство за защита на данните и дали са изпълнени условията за прехвърляне на лични данни на трета страна съгласно ОРЗД) на държавите (във или извън ЕС), където ще се осъществяват възложените на външни доставчици функции и където ще се съхраняват предоставените данни; при възлагане на подизпълнители могат да възникнат допълнителни рискове, ако подизпълнителят се намира в трета държава или в различна държава от CSP, а в случай на верига от подизпълнители — всеки допълнителен риск, който може да възникне, включително поради липсата на пряк договор между посредника и подизпълнителя, изпълняващ възложена на външен доставчик функция;
 - vii. възможната концентрация при посредника (включително, според случая, на ниво група) поради много споразумения за възлагане на услуги в облак, възложени на един CSP, както и възможна концентрация във финансовия сектор на ЕС поради това, че много посредници използват един и същ CSP или малка група от CSP. При оценка на риска от концентрация посредникът следва да вземе предвид всички свои споразумения за възлагане на услуги в облак на външни доставчици (и, според случая, споразуменията за възлагане на услуги в облак на външни доставчици на ниво група), сключени с този CSP;
- б) да отчита очакваните ползи и разходи, свързани със споразуменията за възлагане на услуги в облак на външни доставчици, включително да оценява тежестта на всички съществени рискове, които могат да бъдат намалени или по-добре управлявани спрямо всички съществени рискове, които могат да възникнат във връзка със споразумение за възлагане на услуги в облак на външни доставчици.
21. При възлагане на външни доставчици на критични или важни функции, комплексната проверка следва да включва оценка на пригодността на CSP. Когато оценява пригодността на CSP, посредникът следва да се увери, че CSP има бизнес репутация, умения, ресурси (напр. човешки, ИТ, финансови), организационна структура и, ако е приложимо, необходимия(ите) регулаторен(и) лиценз(и) или регистрация(и) за извършване на критична или важна функция по надежден и професионален начин, така че да изпълни своите задължения в рамките на срока на споразумението за възлагане на услуги в облак на външни

доставчици. Допълнителните фактори, които трябва да се вземат под внимание, когато се извършва комплексна проверка на CSP, включват, но не се ограничават до:

- а) управлението на информационната сигурност, и по-специално защитата на личните, поверителни или други чувствителни данни;
- б) поддръжка на услугата, включително плановете и контактите за поддръжка и процесите на управление на инциденти;
- в) плановете за непрекъснатост на дейността и за възстановяване при катастрофично събитие;

22. Когато е целесъобразно и за да се подпомогне извършваната комплексна проверка, посредникът може също така да използва сертификати, базирани на международни стандарти и доклади от външен или вътрешен одит.

23. Ако на посредника му станат известни съществени недостатъци и/или съществени промени на предоставяните услуги или на състоянието на CSP, анализът преди възлагане на дейностите и комплексната проверка на CSP следва надлежно да се прегледат и да се извършат повторно, ако е необходимо.

24. Ако посредник сключи ново споразумение или поднови съществуващо споразумение с CSP, на когото вече е извършена оценка, той следва да определи чрез основан на риска подход, дали е необходима нова комплексна проверка.

Насока 3. Основни договорни елементи

25. Съответните права и задължения на посредника и неговия CSP следва ясно да се посочат в писмено споразумение.

26. В писменото споразумение следва изрично да се предвижда възможност да бъде прекратено от посредника, ако това е необходимо.

27. Когато се възлагат критични или важни функции на външни доставчици, писменото споразумение следва да включва най-малко:

- а) ясно описание на възложената на външен доставчик функция;
- б) началната и крайната дата, ако е приложимо, на споразумението и сроковете за предизвестие за CSP и за посредника;
- в) приложимото право на споразумението и избора на юрисдикция, ако е направен такъв;
- г) финансовите задължения на посредника и CSP;
- д) дали се разрешава възлагане на дейност на подизпълнител и при какви условия, като се има предвид Насока 7;
- е) местоположението(ята) (т.е. региони или държави), където се изпълнява възложената функция и където съответните данни ще се съхраняват и

- обработват, както и условията, които трябва да бъдат изпълнени, включително изискване за уведомяване на посредника, ако CSP предлага промяна на местоположението(ята);
- ж) разпоредби относно информационната сигурност и защитата на личните данни, като се има предвид Насока 4;
 - з) правото за посредника регулярно да наблюдава изпълнението на CSP по споразумението за възлагане на услуги в облак на външни доставчици, като се има предвид Насока 6;
 - и) договорените нива на услугите, които следва да включват количествени и качествени показатели за изпълнение, за да се даде възможност за своевременно наблюдение, така че да могат своевременно да бъдат предприети подходящи коригиращи действия, ако договорените нива на услугите не се изпълняват;
 - к) задълженията за докладване на CSP към посредника, включително, ако е целесъобразно, задълженията за представяне на доклади, свързани с функцията за сигурност и ключовите функции на посредника, например доклади, изготвени чрез функцията за вътрешен одит на CSP;
 - л) разпоредби относно управлението на инциденти от CSP, включително задължението на CSP своевременно да докладва на посредника инциденти, които са засегнали функционирането на договорената услуга на посредника;
 - м) дали CSP следва да сключи задължителна застраховка срещу определени рискове и, ако е приложимо, необходимото ниво на застрахователното покритие;
 - н) изискванията за CSP да въведе и тества планове за непрекъснатост на стопанската дейност и възстановяване при катастрофично събитие;
 - о) изискването CSP да предоставя на посредника, неговите компетентни органи и всяко друго лице, назначено от посредника или компетентните органи, право на достъп („права на достъп“) и на проверка („права на одит“) на съответната информация, помещения, системи и устройства на CSP в необходимата степен за наблюдение на работата на CSP по споразумението за възлагане на услуги в облак на външни доставчици и спазването на приложимите регулаторни и договорни изисквания, като се има предвид Насока 6;
 - п) разпоредби с които се гарантира, че може да се осъществява достъп до данните, които CSP обработва или съхранява от името на посредника, както и те да бъдат възстановени и върнати на посредника при необходимост, като се има предвид Насока 5.

Насока 4. Информационна сигурност

28. Посредникът следва да определи изискванията за информационната сигурност в своите вътрешни политики и процедури и в рамките на писменото

споразумение за възлагане на дейности на външни доставчици и да наблюдава спазването на тези изисквания постоянно, включително да осигурява защита за поверителни, лични или други чувствителни данни. Тези изисквания следва да бъдат пропорционални на естеството, мащаба и сложността на функцията, която посредникът възнамерява да възложи на CSP, и рисковете, присъщи на тази функция.

29. За тази цел при възлагане на външни доставчици на критични или важни функции и без да се засягат приложимите изисквания по ОРЗД, като прилага основан на риска подход, посредникът трябва най-малко:

- а) *организация за информационна сигурност*: да се увери, че има ясно разпределение на ролите и отговорностите за информационната сигурност между посредника и CSP, включително по отношение на откриването на заплахи, управлението на инциденти и управлението на поправки, и да се увери, че CSP ефективно може да изпълнява своите роли и отговорности;
- б) *управление на идентификационни данни и достъпа*: да се увери, че са въведени надеждни механизми за автентификация (напр. многофакторна автентификация) и контрол на достъпа с цел предотвратяването на неразрешен достъп до данните на посредника и поддържащите ресурси в облака;
- в) *криптиране на управление на ключове*: да се увери, че при необходимост се използват съответните технологии за криптиране по отношение на предавани данни, запазени данни, съхранявани данни и резервни копия на данни, в комбинация с подходящи решения за управление на ключове за ограничаване на риска от неразрешен достъп до ключовете за криптиране; по-специално посредникът следва да има предвид технологии и процеси на най-високо технологично ниво, когато прави своя избор за решението за управление на ключове;
- г) *оперативна и мрежова сигурност*: да разгледа подходящи нива на достъпност на мрежата, разделяне на мрежите (напр. изолиране на ползвателя в общата среда на облака, оперативно разделяне по отношение на мрежовото приложение, логика на приложението, операционна система, мрежа, Система за управление на база данни (DBMS) и нива на съхранение), както и среда за обработване (напр. тестване, потребителски приемни изпитания, разработване, производство);
- д) *приложни програмни интерфейси (API)*: да се обмислят механизми за интеграция на облачните услуги със системите на посредника, за да се осигури сигурност на API (напр., установяване и поддържане на политики и процедури за информационна сигурност за API в много системни интерфейси, юрисдикции и бизнес функции за предотвратяване на неразрешено разкриване, изменение или унищожаване на данни);
- е) *непрекъснатост на дейността и възстановяване при катастрофично събитие*: да се увери, че са въведени ефективни контролни механизми на

непрекъснатостта на дейността и възстановяването при катастрофично събитие (напр. чрез определяне на минимални изисквания за капацитет, избор на възможности за хостинг, които са географски разпръснати, и възможност за превключване от една на друга или заявяване и преглед на документация, която показва транспортния маршрут на данните на посредника между системите на CSP, както и разглеждане на възможността за дублиране на машинни изображения в независимо място за съхранение, което е достатъчно изолирано от мрежата или се извежда офлайн);

- ж) *местоположение на данни*: да възприеме основан на риска подход за мястото/местата за съхранение на данни и обработване на данни (а именно региони или държави);
- з) *спазване на насоките и наблюдение*: да проверява дали CSP съблюдава международно признатите стандарти за информационна сигурност и дали са въведени подходящи контролни механизми за информационна сигурност (напр. като поиска от CSP да представи доказателства, че провежда съответните прегледи на информационната сигурност и като извършва редовни оценки и тестове на споразуменията за информационна сигурност на CSP).

Насока 5. Стратегии за оттегляне

30. В случай на възлагане на външни доставчици на критични или важни функции посредникът следва да се увери, че може да прекрати споразумението за възлагане на услуги в облак на външни доставчици без ненужно прекъсване на неговата дейност и обслужването на неговите клиенти и без това да наруши спазването на неговите задължения съгласно приложимото законодателство, както и поверителността, целостта и достъпността на неговите данни. За тази цел посредникът следва:

- а) да разработи планове за оттегляне, които са изчерпателни, документиран и тествани в достатъчна степен. Тези планове следва да се актуализират при необходимост, включително в случай на промени във възложената на външен доставчик функция;
- б) да установява алтернативни решения и да разработва планове за преход за премахване на възложена на външен доставчик функция и данни от CSP и, според случая, от подизпълнител, както и да ги прехвърли на алтернативен CSP, посочен от посредника, или директно обратно на посредника. 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 преходната фаза;
- в) да се увери, че писменото споразумение за възлагане на дейности в облак на външни доставчици включва задължение за CSP да съдейства за

надлежното прехвърляне на възложената функция и свързаната обработка на данни от CSP и всеки подизпълнител на друг CSP, посочен от посредника, или директно на посредника, ако посредникът задейства стратегията за оттегляне. Задължението за подпомагане на надлежното прехвърляне на възложената функция и свързаното обработване на данни следва да включва, ако е подходящо, сигурното изтриване на данните от системите на CSP и на всеки подизпълнител.

31. При разработването на планове и решенията за оттегляне, както е посочено в букви а) и б) по-горе („стратегия за оттегляне“), посредникът следва да вземе предвид следното:

- а) да определи целите на стратегията за оттегляне;
- б) да определи събитията, при които може да се задейства стратегията за оттегляне. Те следва да включват най-малко прекратяването на споразумението за възлагане на услуги в облак на външни доставчици по инициатива на посредника или CSP и срив или друго сериозно прекратяване на дейността на CSP;
- в) да извърши анализ на въздействието върху дейността, който е съизмерим с възложената функция, за да се установи какви човешки и други ресурси ще бъдат необходими за изпълнение на стратегията за оттегляне;
- г) да възлага роли и отговорности за управление на стратегията за оттегляне;
- д) да тества пригодността на стратегията за оттегляне, като използва основан на риска подход (напр. чрез извършване на анализ на потенциалните разходи, въздействие, ресурси и времеви последици от прехвърлянето на възложена на външен доставчик услуга на алтернативен доставчик);
- е) да определи критериите за успешен преход.

32. Посредникът следва да включи показатели за събития, при които се задейства стратегията за оттегляне, в текущо извършваните от него наблюдения и надзор на услугите, извършвани от CSP по споразумение за възлагане на услуги в облак на външни доставчици.

Насока 6. Права на достъп и одит

33. Посредникът следва да гарантира, че писменото споразумение за възлагане на дейности в облак на външни доставчици не ограничава ефективното упражняване от посредника и компетентния орган на правата за достъп и одит, както и възможностите за надзор над CSP.

34. Посредникът следва за се увери, че при упражняването на правата на достъп и одит (напр. честотата на одита и областите и услугите, които следва да бъдат одитирани) се отчита дали възложените на външен доставчик дейности са свързани с критична или важна функция, както и естеството и степента на

рисковете и въздействието, произтичащо от споразумението за възлагане на услуги в облак на външни доставчици за посредника.

35. Ако упражняването на правата за достъп и одит, или използването на определени техники за одит създават риск за средата на CSP и/или друг клиент на CSP (напр. като влияят върху нивата на услугите, поверителността, целостта и достъпността на данните), CSP следва да представи ясна обосновка пред посредника защо това ще създаде риск, а CSP следва да договори с посредника алтернативни начини за постигане на сходен резултат (напр. включването на специфични контролни механизми, които да бъдат тествани в специален доклад/сертификат, изготвен от CSP).
36. Без да се засяга тяхната окончателна отговорност по отношение на споразуменията за възлагане на услуги в облак на външни доставчици, с цел по-ефективно използване на ресурсите за одит и намаляване на организационната тежест за доставчика на услуги в облак и неговите клиенти, посредниците могат да използват:
- а) сертификати от трети страни и доклади за вътрешен или външен одит, предоставени от CSP;
 - б) обединени одити, извършвани съвместно с други клиенти на същия CSP, или обединени одити, извършвани от одитор на трета страна, назначен от множество клиенти на един и същ CSP.
37. При възлагане на външен доставчик на критични или важни функции посредникът следва да оцени дали сертификатите на трета страна и докладите за външен или вътрешен одит, посочени в параграф 37, буква а), са подходящи и достатъчни за спазване на неговите задължения по приложимото законодателство, и следва да се стреми да не разчита само на тези сертификати и доклади в течение на времето.
38. При възлагане на външни доставчици на критични или важни функции посредникът следва да използва сертификатите от трети страни и докладите за вътрешен и външен одит, посочени в параграф 37, буква а), само ако:
- а) се е уверил, че обхватът на сертификатите или докладите за одит покрива ключовите системи на CSP (напр. процеси, приложения, инфраструктура, центрове за данни), ключовите контролни механизми, установени от посредника, и спазването на съответното приложимо законодателство;
 - б) извършва редовно задълбочена оценка на съдържанието на сертификатите или докладите за одит и проверява дали сертификатите, или докладите не са загубили своята актуалност;
 - в) гарантира, че ключовите системи и контролни механизми на CSP ще бъдат обхванати в бъдещите версии на сертификатите или одитните доклади;

- г) е удовлетворен от сертифициращата или одитираща страна (напр. по отношение на нейната квалификация, експертни познания, повторно изпълнение/проверка на данните в съответния одитен файл, както и на ротацията на сертифициращото или одитиращото дружество);
 - д) е удовлетворен, че сертификатите се издават, а одитите се извършват въз основа на подходящи стандарти и включват проверка на ефективността на въведените основни контролни механизми;
 - е) има договорното право да изисква разширяване на обхвата на сертификатите или одитните доклади, така че да включат други съответни системи и контролни механизми на CSP; броят и честотата на подобни искания за промяна на обхвата следва да бъдат разумни и законосъобразни с оглед на управлението на риска;
 - ж) запазва договорното право да извършва индивидуални одити на място по своя преценка по отношение на възложената на външен доставчик функция.
39. Посредникът следва да гарантира, че преди всяко посещение на място, включително от трета страна, назначена от посредника (напр., одитор), на CSP се изпраща предизвестие в разумен срок, освен ако по-ранно предизвестие не е възможно поради спешна или кризисна ситуация или би довело до ситуация, при която одитът няма да бъде ефективен. В това предизвестие следва да бъдат посочени мястото и целта на посещението и служебните лица, които ще участват в посещението.
40. Като се има предвид, че облачните услуги са с високо ниво на техническа сложност и поставят специфични предизвикателства, свързани с юрисдикцията, извършващите одит лица, които са вътрешни одитори на посредника, или одитори, действащи от негово име, следва да притежават подходящите умения и знания, за да оценят правилно съответните облачни услуги и да извършат ефективен и подходящ одит. Това се отнася и за служители на посредниците, които извършват преглед на сертификатите или одитните доклади, предоставени от CSP.

Насока 7. Възлагане на дейности на подизпълнители

41. Ако се разрешава възлагане на подизпълнител на критични или важни функции (или на съществена част от тях), в споразумението за възлагане на услуги в облак на външни доставчици между посредника и CSP следва:
- а) да бъдат посочени всяка част или аспект на възложената на външен доставчик функция, които се изключват от възможното възлагане на подизпълнител;
 - б) да се определят условията, които трябва да бъдат спазени при възлагане на подизпълнител;

- в) да се посочи, че CSP остава отговорен и е задължен да наблюдава тези услуги, които възлага на подизпълнители, за да гарантира непрекъснатото спазване на всички договорни задължения между CSP и посредника;
- г) да се включи задължение за CSP да уведомява посредника за всяко планирано възлагане на подизпълнител или за съществени промени, по-специално когато това може да засегне способността на CSP да изпълнява своите задължения по споразумението за възлагане на услуги в облак на външни доставчици с посредника. Сроктът на уведомлението, посочен в писменото споразумение, следва да предоставя на посредника достатъчно време, за да извърши поне оценка на риска на предложеното възлагане на подизпълнител или на съществените промени и да възрази срещу тях, или изрично да ги одобри, както се посочва в буква д) по-долу;
- д) да гарантира, че посредникът има право да възрази срещу планираното възлагане на подизпълнител или срещу съществените промени, или че е необходимо изрично одобрение, преди предложеното възлагане на подизпълнител или съществените промени да влязат в сила;
- е) да гарантира, че посредникът има договорното право да прекрати споразумението за възлагане на услуги в облак на външни доставчици с CSP, ако има възражения срещу предложеното възлагане на дейности на подизпълнител или съществени промени, и в случай на неправомерно възлагане на подизпълнител (напр. когато CSP пристъпи към възлагане на подизпълнител, без да уведоми посредника или сериозно наруши условията за възлагане на подизпълнител, посочени в договора за възлагане на дейности на външен доставчик).

42. Посредникът следва да се увери, че CSP осъществява подходящ надзор над подизпълнителя.

Насока 8. Писмено уведомяване на компетентните органи

43. Посредникът следва своевременно да уведомява в писмен вид своя компетентен орган за отнасящи се за критична или важна функция планирани споразумения за възлагане на услуги в облак на външни доставчици. Посредникът следва също така да уведомява своевременно и в писмен вид своя компетентен орган за тези споразумения за възлагане на услуги в облак на външни доставчици, които се отнасят до функция, която не е класифицирана като важна или критична, а впоследствие става критична или важна.
44. В писменото уведомление от посредника следва да се съдържа, като се взема предвид принципът на пропорционалност, най-малко следната информация:
- а) началната дата на споразумението за възлагане на дейности в облак на външен доставчик и, когато е приложимо, следващата дата на подновяване

- на договора, крайната дата и/или сроковете за предизвестие за доставчика на услуги в облак и за посредника;
- б) кратко описание на възложената на външен доставчик функция;
 - в) кратко обобщение на причините, поради които възложената на външен доставчик функция се счита за критична или важна;
 - г) името и търговското наименование (ако има такова) на CSP, държава на регистрация, корпоративен регистрационен номер, идентификатор на юридическо лице (ако е приложимо), адрес на управление, съответните данни за контакт и наименованието на неговото дружество майка (ако има такова);
 - д) приложимото право на споразумението за възлагане на услуги в облак на външни доставчици и, ако е посочен, изборът на юрисдикция;
 - е) моделите на разполагане в облак и специфичният характер на съхраняваните данни и местата (т.е. региони или държави), където могат да се съхраняват такива данни;
 - ж) датата на последната оценка на критичността или важността на възложената на външен доставчик функция;
 - з) датата на последната оценка или одит на риска на CSP, заедно с кратко резюме на основните резултати, и датата на следващата планирана оценка или одит на риска;
 - и) лицето или органът за вземане на решения при посредника, което е одобрило споразумението за възлагане на услуги в облак на външни доставчици;
 - к) ако е приложимо, имената на всеки подизпълнител, на когото се възлагат съществени части от критична или важна функция, включително държавата или региона, където са регистрирани подизпълнителите, където се извършва възложената услуга и където ще се съхраняват данните.

Насока 9. Надзор на споразумения за възлагане на услуги в облак на външни доставчици

- 45. Компетентните органи следва да оценяват рисковете, произтичащи от споразуменията за възлагане на услуги в облак на външни доставчици на посредниците, като част от своя процес на надзор. По-специално тази оценка следва да се фокусира върху споразуменията, които се отнасят до възлагането на критични или важни функции на външен доставчик.
- 46. Компетентните органи следва да се уверят, че могат да осъществяват ефективен надзор, по-специално когато посредниците възлагат на външни доставчици критични или важни функции, които се изпълняват извън ЕС.
- 47. Като прилагат основан на риска подход, компетентните органи следва да преценят дали посредниците:

- а) разполагат със съответното управление, ресурси и оперативни процеси за подходящо и ефективно сключване, осъществяване и надзор на споразумения за възлагане на услуги в облак на външни доставчици;
- б) установяват и управляват всички съответни рискове, свързани с възлагане на услуги в облак на външни доставчици.

48. Когато се установят рискове от концентрация, компетентните органи следва да наблюдават развитието на тези рискове и да извършат оценка както на тяхното потенциално въздействие върху други посредници под техен надзор, така и върху стабилността на финансовия пазар.