EBA/REC/2017/03

28/03/2018

Препоръки

за възлагане на външни изпълнители на дейности в облак

1. Спазване на препоръките и задължения за докладване

Статут на препоръките

1. Настоящият документ съдържа препоръки, издадени съгласно член 16 от Регламент (ЕС) № 1093/2010[1]. Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010 компетентните органи и финансовите институции полагат всички усилия за спазване на препоръките.

2. В препоръките е представено становището на ЕБО относно подходящите надзорни практики в Европейската система за финансов надзор или за това как следва да се прилага правото на Съюза в дадена област. Компетентните органи, определени в член 4, параграф 2 от Регламент (ЕС) № 1093/2010, за които се отнасят тези препоръки, следва да ги спазват, като ги включат в практиките си по подходящ начин (напр. чрез изменение на правната рамка или надзорните процеси), включително в случаите, когато препоръките са насочени основно към институциите.

Изисквания за докладване

3. Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, най-късно до 28.05.2018 компетентните органи трябва да уведомят ЕБО дали спазват или възнамеряват да спазват тези препоръки, или в противен случай да изложат причините за неспазването им. При липса на уведомление в този срок ЕБО ще счита, че компетентните органи не спазват препоръките. Уведомленията следва да се изпратят чрез подаване на формуляра, който можете да се намери на уебсайта на ЕБО, на адрес compliance@eba.europa.eu, като се посочи референтен номер „EBA/REC/2017/03“. Уведомленията следва да се подават от лица, оправомощени да докладват за наличието на съответствие от името на техните компетентни органи. Всяка промяна в статута на спазването трябва също да се докладва на ЕБО.

Уведомленията се публикуват на уебсайта на ЕБО в съответствие с член 16, параграф 3.

[1] Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 12).

2. Предмет, обхват и определения

Предмет и обхват на прилагане

1. Настоящите препоръки допълнително определят условията за възлагане на дейности на външни изпълнители, както е посочено в Насоките на КЕБНО за възлагане на дейности на външни изпълнители от 14 декември 2006 г., и се прилагат за възлагането на дейности на външни изпълнители от институции, както са определени в член 4, параграф 1, точка 3 от Регламент (ЕС) № 575/2013, на доставчици на услуги в облак.

Адресати

2. Настоящите препоръки са предназначени за компетентните органи, както са определени в член 4, параграф 2, подточка (i) от Регламент (ЕС) № 1093/2010, и за институциите, както са определени в член 4, параграф 1, точка 3 от Регламент (ЕС) № 575/2013.[2]

Определения

3. Освен ако не е посочено друго, термините, използвани и определени в Директива 2013/36/ЕС[3] за капиталовите изисквания и в насоките на КЕБНО, имат същото значение в препоръките. В допълнение, за целите на настоящите препоръки се прилагат следните определения:

Услуги в облак	Услуги, предоставяни чрез обработка на данни в облак, а именно – модел за реализиране на повсеместен, удобен мрежов достъп по заявка до споделен набор от изчислителни ресурси с възможност за конфигуриране (напр. мрежи, сървъри, хранилища, приложения и услуги), които бързо могат да бъдат обезпечавани и реализирани с минимални усилия за управление или взаимодействие с доставчика на услуги.
Публичен облак	Инфраструктура за услуги в облак, която може свободно да се използва от широката общественост.
Частен облак	Инфраструктура за услуги в облак, която може да се използва само от една институция.

[2] Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 година относно пруденциалните изисквания за кредитните институции и инвестиционните посредници и за изменение на Регламент (ЕС) № 648/2012.

[3] Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 година относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО.

Общностен облак	Инфраструктура за услуги в облак, която може да се използва само от конкретна общност от институции, включително няколко институции, принадлежащи към една група.
Хибриден облак	Инфраструктура за услуги в облак, която е съставена от две или повече обособени инфраструктури за услуги в облак.

3. Въвеждане

Дата на прилагане

4. Настоящите препоръки влизат в сила от 1 юли 2018 г.

4. Препоръки за възлагане на дейности на доставчици на услуги в облак

4.1 Оценка на съществеността

1. Преди да възлагат дейности на външни изпълнители, институциите трябва да определят кои дейности следва да се считат за съществени. Институциите трябва да извършат оценка на съществеността на дейностите въз основа на насока 1(е) от насоките на КЕБНО и – конкретно за възлагането на дейности на доставчици на услуги в облак – да имат предвид всички от следните аспекти:

    а) критичното значение и присъщия рисков профил на дейностите, които ще се възлагат, т.е. дали това са дейности от критично значение за непрекъснатостта/жизнеспособността на работния процес на институцията и задълженията ѝ към клиентите;

    б) прякото оперативно въздействие на прекъсването на дейността и свързаните правни и репутационни рискове;

    в) въздействието, което дадено прекъсване на дейността би имало върху очакваните приходи;

    г) потенциалното въздействие, което дадено нарушение на поверителността или целостта на данните би имало върху институцията и клиентите ѝ.

4.2 Задължение за надлежно уведомяване на надзорните органи

2. Институциите, които възлагат дейности на външни изпълнители, трябва надлежно да уведомяват компетентните органи при възлагане на съществени дейности на доставчици на услуги в облак. Институциите трябва да извършват това въз основа на параграф 4.3 от насоките на КЕБНО и при всички случаи да предоставят на компетентните органи следната информация:

    а) наименованието на доставчика на услуги в облак и наименованието на неговото предприятие майка (ако има такова);
    б) описание на дейностите и данните, които ще се възлагат;
    в) държавата или държавите, в които ще се предоставя услугата (вкл. местоположението на данните);
    г) началната дата на услугата;
    д) последната дата на подновяване на договора (когато е приложимо);

е) приложимото законодателство, уреждащо договора;
ж) датата на изтичане на услугата или датата на следващото подновяване на договора (когато е приложимо).

3. Освен информацията, предоставяна в съответствие с предходния параграф, компетентният орган може да поиска от възлагащата институция допълнителна информация за нейния анализ на риска относно съществените дейности, които ще се възлагат на външни изпълнители, като например:

а) дали доставчикът на услуги в облак има план за непрекъснатост на дейността, подходящ за услугите, предоставяни на възлагащата институция;
б) дали възлагащата институция има изходна стратегия в случай на прекратяване от която и да е страна или нарушаване на предоставянето на услугите от доставчика на услуги в облак;
в) дали възлагащата институция притежава уменията и ресурсите, необходими за подходящо наблюдение на възлаганите дейности.

4. Възлагащата институция трябва да поддържа актуален регистър на информацията за всички свои съществени и несъществени дейности, възлагани на доставчици на услуги в облак, на ниво институция и на групово ниво. При поискване възлагащата институция трябва да представи пред компетентния орган копие от споразумението за възлагане на дейности на външни изпълнители и съответната информация, записана в този регистър, независимо дали дейността, възложена на доставчик на услуги в облак, е оценена от институцията като съществена.

5. В регистъра, посочен в предходния параграф, трябва да се включва поне следната информация:

а) информацията, посочена в параграф 2, букви а)—ж), ако все още не е предоставена;
б) тип на възлагането (модел на услуги и внедряване в облака, т.е. публичен/частен/хибриден/общностен облак);
в) страни, получаващи услуги в облак съгласно споразумението за възлагане на дейности на външни изпълнители;
г) доказателство за одобрение на възлагането от страна на ръководния орган или делегираните му комитети, ако е приложимо;
д) наименования на подизпълнителите, ако а приложимо;
е) държава, в която е регистриран доставчикът на услуги в облак/главният подизпълнител;
ж) дали възлагането на дейности е оценено като съществено (да/не);
з) дата, на която институцията е извършила последната оценка на съществеността на възлаганите дейности;
и) дали доставчикът на услуги в облак/подизпълнителя(ите) поддържат бизнес операции с критично ограничено време (да/не);
й) оценка на заменяемостта на доставчика на услуги в облак (като лесна, трудна или невъзможна);
к) определяне на алтернативен доставчик на услуги, когато е възможно;

л) дата на последната оценка на риска, свързан с възлагането на дейностите или при използване на подизпълнител.

4.3 Правомощия за достъп и одит

За институциите

6. Въз основа на насока 8(2)(ж) от насоките на КЕБНО и за целите на възлагането на дейности в облак на външни изпълнители, възлагащите институции допълнително трябва да гарантират, че са сключили писмено споразумение с доставчика на услуги в облак, в което последният поема следните задължения:

    а) да предостави на институцията, на трета страна, определена за тази цел от институцията, и на регистрирания одитор на институцията пълен достъп до обектите, в които извършва дейността си (централи и оперативни центрове), включително пълния набор от устройства, системи, мрежи и данни, използвани за предоставяне на възлаганите услуги (правомощия за достъп);

    б) да предостави на институцията, на трета страна, определена за тази цел от институцията, и на регистрирания одитор на институцията неограничени правомощия за инспекции и проверка, свързани с възлаганите услуги (правомощия за одит).

7. Ефективното упражняване на правомощията за достъп и одит не трябва да се възпрепятства или ограничава от договорни споразумения. Ако извършването на одит или използването на определени техники за одит може да създаде риск за средата на друг клиент, следва да се договорят алтернативни начини за предоставяне на подобно ниво на гарантиране, изисквано от институцията.

8. Възлагащата институция следва да упражнява правомощията си за одит и достъп по рисково базиран начин. Когато възлагащата институция не използва собствени ресурси за одит, тя трябва да обмисли използването на поне един от следните инструменти:

    а) съвместни одити, организирани заедно с други клиенти на същия доставчик на услуги в облак и провеждани от тези клиенти или от трета страна, определена от тях, за по-ефективно използване на ресурсите за одит и намаляване на организационната тежест както върху клиентите, така и върху доставчика на услуги в облак;

    б) сертификати на трети страни и доклади на трети страни или вътрешен одит, предоставени от доставчика на услуги в облак, при условие че:

        i. възлагащата институция се увери, че обхватът на сертификата или одиторския доклад покрива системите (т.е. процеси, приложения, инфраструктура, центрове за данни и др.) и механизмите за контрол, определени от възлагащата институция като ключови;

ii. възлагащата институция периодично извършва задълбочена оценка на съдържанието на сертификатите или одиторските доклади и по-специално – се уверява, че ключовите механизми за контрол все още се покриват в бъдещи версии на одиторските доклади и проверява дали сертификатът или одиторският доклад продължава да е актуален;

iii. възлагащата институция е удовлетворена от правоспособността на страната, която издава сертификати или провежда одит (напр. по отношение на ротацията на одиторските дружества, квалификациите, компетентността, повторните проверки/потвърждения на данните в основната одитна документация);

iv. сертификатите са издадени и одитите са проведени в съответствие с широко признати стандарти и включват проверка на оперативната ефективност на установените ключови механизми за контрол;

v. съгласно договора възлагащата институция има право да изиска разширяване на обхвата на сертификатите или одиторските доклади към съответните системи и/или механизми за контрол; броят и честотата на такива искания за промяна на обхвата трябва да са обосновани и оправдани с оглед управлението на риска.

9. Предвид че решенията за услуги в облак имат високо ниво на техническа сложност, възлагащата институция трябва да се увери, че персоналът, който провежда одита/проверката – независимо дали от страна на вътрешния одитор на институцията или група от одитори, действащи от името на институцията, или одитори, определени от доставчика на услуги в облак – или съответно персоналът, който преглежда сертификатите от трета страна или одиторските доклади на доставчика на услуги в облак, притежава подходящи умения и знания за провеждане на ефективни и практически значими одити/проверки и/или оценки на решения, предоставяни чрез облак.

За компетентните органи

10. Въз основа на насока 8(2)(з) от насоките на КЕБНО и за целите на възлагането на дейности в облак възлагащите институции трябва да гарантират, че са сключили писмено споразумение с доставчика на услуги в облак, в което последният поема следните задължения:

а) да предостави на компетентния орган, осъществяващ надзор над възлагащата институция (или трета страна, определена за тази цел от органа), пълен достъп до обектите, в които доставчикът на услуги в облак извършва дейността си (централи и оперативни центрове), включително пълния набор от устройства, системи, мрежи и данни, използвани за предоставяне на услугите към възлагащата институция (правомощия за достъп);

б) да предостави на компетентния орган, осъществяващ надзор над възлагащата институция (или трета страна, определена за тази цел от органа), неограничени права за инспекции и проверки, свързани с възлаганите услуги (право на проверка).

11. Възлагащата институция трябва да се увери, че договорните споразумения не пречат на компетентния орган да осъществява надзорните си функции и цели.

12. Информацията, която компетентният орган получава при упражняване на правомощията за достъп и проверка, се подчинява на изискванията за професионална тайна и поверителност, посочени в член 53 и следващи от Директива 2013/36/ЕС (ДКИ IV). Компетентните органи трябва да се въздържат от участие в каквито и да е договорни споразумения или декларации, които биха им попречили да съблюдават разпоредбите на правото на Съюза относно поверителността, професионална тайна и обмена на информация.

13. Въз основа на резултатите от проверката си компетентният орган при необходимост се заема с всички установени несъответствия, като налага мерки директно върху възлагащата институция.

4.4 В частност за правомощията за достъп

14. Споразумението, посочено в параграфи 6 и 10, включва следните разпоредби:

а) страните, възнамеряващи да упражняват правомощията си за достъп (институция, компетентен орган, одитор или трета страна, действаща от името на институцията или компетентния орган), в разумен срок преди планираното посещение на място изпращат уведомление до съответния обект на дейност, освен ако изпращането на предизвестие не е възможно поради спешен случай или кризисна ситуация;

б) доставчикът на услуги в облак е длъжен изцяло да съдейства на съответните компетентни органи, както и на институцията и одитора ѝ, във връзка с посещението на място.

4.5 Сигурност на данните и системите

15. Както е посочено в насока 8(2)(д) от насоките на КЕБНО, договорът за възлагане на дейности на външни изпълнители обвързва доставчика на тези услуги да защитава поверителността на информацията, предавана от финансовата институция. В съответствие с насока 6(6)(д) от насоките на КЕБНО институциите предприемат необходимите мерки за осигуряване на непрекъснато предоставяне на услугите от външните изпълнители на услуги. В съответствие с насоки 8(2)(б) и 9 от насоките на КЕБНО, съответните нужди на възлагащите институции по отношение на качеството и изпълнението трябва да бъдат формализирани с договори за възлагане на дейност на външни изпълнители и споразумения за услуги. Тези аспекти от сигурността също трябва да бъдат периодично наблюдавани (насока 7).

16. За целите на предходния параграф институцията трябва да извършва – преди възлагането на дейности на външни изпълнители и с цел оповестяване на съответното решение – поне следното:

    а) определя и класифицира дейностите, процесите, съответните данни и системи за запазване на чувствителна информация и необходимите защити;

    б) провежда задълбочен, рисково базиран избор на дейностите, процесите, съответните данни и системи, за които се обмисля да бъдат прехвърлени към решение за обработка на данни в облак;

    в) определя и избира подходящо ниво за защита на поверителността на данните, непрекъснатост на възлаганите дейности, пълнота и проследяване на данните и системите в контекста на планираното възлагане на дейности в облак. Институциите трябва също да обмислят конкретни мерки, необходими за данните в движение, данните в паметта и данните в хранилище, като например употребата на криптиращи технологии в комбинация с подходяща основна архитектура за управление.

17. Впоследствие институциите трябва да се уверят, че са сключили писмено споразумение с доставчика на услуги в облак, в което – наред с други неща – са описани задълженията на доставчика съгласно параграф 16, буква в).

18. Институциите трябва периодично да наблюдават изпълнението на дейностите и мерките за сигурност съгласно насока 7 от насоките на КЕБНО, включително инциденти, и когато е подходящо, да проверяват дали възлагането на дейности на външни изпълнители отговаря на предходните параграфи. При необходимост трябва своевременно да предприемат коригиращи мерки.

4.6 Местоположение и обработка на данните

19. Както е посочено в насока 4(4) от насоките на КЕБНО, институциите трябва да обръщат особено внимание при сключване и управление на споразумения за възлагане на дейности на външни изпълнители, предприети извън ЕИП, поради възможните рискове за защита на данните и за ефективен надзор от страна на надзорния орган.

20. Възлагащата институция трябва да прилага рисково базиран подход при избора на местоположение на данните и обработката им, когато възлага дейности в облак. Оценката трябва да отчита потенциалните рискови въздействия, включително правните рискове и проблеми с нормативното съответствие, както и ограниченията в контрола, свързани с държавите, в които се предоставят или е вероятно да бъдат предоставяни възложените на външни изпълнители услуги и в които се съхраняват или е вероятно да бъдат съхранявани данните. Оценката трябва да включва съображения по отношение на общата политическа стабилност и във връзка със сигурността, приложимите закони в тези юрисдикции (вкл. закони за защита на данните) и осигуряваното правоприлагане в тези юрисдикции, включително разпоредбите на законите за несъстоятелност, които биха се приложили при фалит на доставчика на услуги в облак. Възлагащата институция трябва да се увери, че тези рискове остават в приемливи граници, съизмерими със съществеността на възлаганата дейност.

4.7 Верижно възлагане на дейности на външни изпълнители

21. Както е посочено в насока 10 от насоките на КЕБНО, институциите трябва да обръщат внимание на рисковете, свързани с възлагане на дейности на външни изпълнители, когато външният изпълнител на услуги използва подизпълнител за елементи на услугата с други доставчици. Възлагащата институция може да приеме верижно възлагане на дейности на външни изпълнители само ако подизпълнителят също се задължи да спазва напълно всички ангажименти, съществуващи между възлагащата институция и доставчика на възложени услуги. Освен това възлагащата институция трябва да предприеме подходящи стъпки за овладяване на рисковете поради пропуски или неизпълнение на дейности, прехвърлени на подизпълнител, които оказват значително влияние върху възможността на доставчика на възложени услуги да изпълнява отговорностите си съгласно споразумението за възлагане.

22. Споразумението за възлагане между възлагащата институция и доставчика на услуги в облак трябва да уточнява типа дейности, които са изключени от потенциално прехвърляне на подизпълнител, и да посочва, че доставчикът на услуги в облак запазва пълна отговорност за и контрол върху онези от услугите, които е прехвърлил към подизпълнители.

23. Споразумението за възлагане трябва също да включва задължение доставчикът на услуги в облак да уведомява възлагащата институция за всички планирани значителни промени на подизпълнителите или услугите, прехвърлени на подизпълнител, посочени в

първоначалното споразумение, които могат да повлияят върху възможността на доставчика на услуги да изпълнява отговорностите си съгласно споразумението за възлагане. Периодът за уведомление относно такива промени трябва да бъде предварително договорен, за да може възлагащата институция да извърши оценка на риска за ефектите от предложените промени, преди да влезе в сила действителната промяна на подизпълнителите или услугите, прехвърлени на подизпълнител.

24. В случай че доставчик на услуги в облак планира промени на подизпълнителите или услугите, прехвърлени на подизпълнител, които биха оказали неблагоприятен ефект върху оценката на риска за договорените услуги, възлагащата институция трябва да има право да прекрати договора.

25. Възлагащата институция трябва периодично да преглежда и наблюдава изпълнението на цялостната услуга, независимо дали се предоставя от доставчик на услуги в облак, или негови подизпълнители.

4.8 Планове за действие при извънредни ситуации и изходни стратегии

26. Както е посочено в насоки 6.1, 6(6)(д) и 8(2)(г) от насоките на КЕБНО, възлагащата институция трябва да планира и прилага мерки за поддържане на непрекъснато провеждане на дейностите си, в случай че предоставянето на услуги от доставчик на възложени услуги прекъсне или се влоши до неприемлива степен. Тези мерки трябва да включват планиране при извънредни ситуации и ясно определени изходни стратегии. Освен това договорът за възлагане трябва да включва клауза за управление на прекратяването, която позволява дейностите, възложени на доставчика на услуги, да бъдат прехвърлени към друг доставчик или обратно поети от възлагащата институция.

27. Възлагащата институция трябва също да се увери, че при необходимост може да прекратява споразумения за възлагане на дейности в облак без съществено нарушаване на предоставянето на услуги или неблагоприятни ефекти върху съответствието ѝ с регулаторния режим, както и без влошаване на непрекъснатостта и качеството на предоставяните от нея услуги към клиентите. За да постигне това, възлагащата институция трябва да:

    а) разработва и прилага изходни планове, които са изчерпателни, документирани и достатъчно добре изпробвани съобразно необходимостта;

    б) определя алтернативни решения и разработва преходни планове, които ѝ позволяват да премахва и възлага съществуващи дейности и данни от доставчика на услуги в облак към тези решения по контролиран и достатъчно добре изпробван начин, отчитайки проблемите с местоположението на данните и поддържането на непрекъснатост на работния процес в преходната фаза;

в) гарантира, че споразумението за възлагане включва задължение на доставчика на услуги в облак да оказва необходимата помощ на възлагащата институция при прехвърлянето на възлаганите дейности на друг доставчик или към прякото управление на възлагащата институция в случай на прекратяване на споразумението за възлагане.

28. При разработване на изходни стратегии възлагащата институция трябва да има предвид следното:

а) разработване на ключови рискови индикатори за установяване на неприемливо ниво на услугата;

б) провеждане на анализ на въздействието върху работния процес, съизмерим с прехвърлените дейности, за установяване на необходимото време, човешки и материални ресурси за прилагане на изходния план;

в) възлагане на роли и отговорности за управление на изходните планове и преходните дейности;

г) определяне на критерии за успешен преход.

29. Възлагащата институция трябва да включи индикатори, които могат да задействат изходния план при условия на непрекъснато наблюдение и контрол на услугите, предоставяни от доставчика на услуги в облак.