2024/1774

25.6.2024 г.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2024/1774 НА КОМИСИЯТА

от 13 март 2024 година

за допълнение на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета във връзка с регулаторните технически стандарти за определяне на инструментите, методите, процесите и политиките за управление на риска в областта на ИКТ и опростената рамка за управление на риска в областта на ИКТ

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид 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) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 ([1]), и по-специално член 15, четвърта алинея и член 16, параграф 3, четвърта алинея от него,

като има предвид, че:

(1) Регламент (ЕС) 2022/2554 обхваща голямо разнообразие от финансови субекти, които се различават по размер, структура, вътрешна организация, както и по естеството и сложността на своите дейности, и поради това разполагат с по-голям или по-малък брой елементи на сложност или рискове. За да се гарантира, че това разнообразие е надлежно взето предвид, всички изисквания по отношение на политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, както и по отношение на опростената рамка за управление на риска в областта на ИКТ следва да бъдат пропорционални на посочения размер, структура, вътрешна организация, естество и сложност на тези финансови субекти и на съответните рискове.

(2) Поради същата причина финансовите субекти, попадащи в обхвата на Регламент (ЕС) 2022/2554, следва да разполагат с определена гъвкавост по отношение на начина, по който спазват изискванията във връзка с политиките, процедурите, протоколите и инструментите за сигурност на ИКТ и във връзка с всяка опростена рамка за управление на риска в областта на ИКТ. Ето защо финансовите субекти следва да имат възможност да използват всяка документация, с която вече разполагат, за да спазят всички изисквания относно документацията, които произтичат от посочените изисквания. От това следва, че разработването, документирането и прилагането на специфични политики за сигурност на ИКТ следва да се изискват само за определени съществени елементи, като се вземат предвид, наред с другото, водещите практики и стандарти в сектора. Освен това, за да се вземат предвид конкретни аспекти на техническото изпълнение, е необходимо да се разработят, документират и прилагат процедури за сигурност на ИКТ с цел да се обхванат специфични аспекти на техническото изпълнение, включително управление на капацитета и ефективността, уязвими места и управление на коригирането, сигурност на данните и системата и регистриране.

(3) С цел да се осигури правилното прилагане във времето на политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, посочени в дял II, глава I от настоящия регламент, е важно финансовите субекти да разпределят и поддържат правилно всички роли и отговорности, свързани със сигурността на ИКТ, и да определят последствията от неспазване на политиките или процедурите за сигурност на ИКТ.

(4) За да се ограничи рискът от конфликти на интереси финансовите субекти следва да гарантират разделянето на функциите при разпределянето на ролите и отговорностите в областта на ИКТ.

(5) С цел да се осигури гъвкавост и да се опрости рамката за контрол на финансовите субекти от финансовите субекти не следва да се изисква да разработват специфични разпоредби относно последиците от неспазване на политиките, процедурите и протоколите за сигурност на ИКТ, посочени в дял II, глава I от настоящия регламент, когато такива разпоредби вече са включени в друга политика или процедура.

([1]) ОВ L 333, 27.12.2022 г., стр. 1, ELI: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

(6) В една динамична среда, в която рисковете в областта на ИКТ се променят непрекъснато, е важно финансовите субекти да разработват свои набори от политики за сигурност на ИКТ въз основа на водещите практики и, когато е приложимо, на стандартите, определени в член 2, параграф 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета ([2]). Това следва да даде възможност на посочените в дял II от настоящия регламент финансови субекти да продължат да бъдат информирани и да са подготвени за променящата се среда.

(7) За да гарантират оперативната устойчивост на цифровите си технологии, посочените в дял II от настоящия регламент финансовите субекти следва да разработят и да прилагат като част от своите политики, процедури, протоколи и инструменти за сигурност на ИКТ, политика за управление на активи на ИКТ, процедури за управление на капацитета и ефективността, както и политики и процедури за основаните на ИКТ операции. Тези политики и процедури са необходими, за да се гарантира наблюдението на статуса на активите на ИКТ през целия им жизнен цикъл, така че тези активи да бъдат ефективно използвани и поддържани (управление на активи на ИКТ). Тези политики и процедури следва също така да гарантират оптимизирането на работата на системите на ИКТ и че ефективността на системите и капацитета на ИКТ отговаря на установените цели за стопанска сигурност и сигурност на информацията (управление на капацитета и ефективността). И накрая, тези политики и процедури следва да гарантират ефективното и безпроблемно ежедневно управление и работа на системите на ИКТ (основани на ИКТ операции), като по този начин се свежда до минимум рискът от загуба на поверителност, цялостност и наличност на данни. Ето защо тези политики и процедури са необходими, за да се гарантира сигурността на мрежите, да се предоставят подходящи защитни механизми срещу проникване и срещу злоупотреба с данни и да се запазят наличността, автентичността, цялостността и поверителността на данните.

(8) За да се гарантира правилното управление на риска за наследените системи на ИКТ, финансовите субекти следва да записват и наблюдават крайните дати на услугите за поддръжка в областта на ИКТ, предоставяни от трети страни. Поради потенциалното въздействие, което е възможно да окаже загубата на поверителност, цялостност и наличност на данните, при записването и наблюдението на крайните дати финансовите субекти следва да поставят акцент върху онези активи или системи на ИКТ, които са от критично значение за стопанската дейност.

(9) Криптографските механизми за контрол могат да гарантират наличността, автентичността, цялостността и поверителността на данните. Поради това посочените в дял II от настоящия регламент финансови субекти следва да установят и прилагат такива механизми за контрол въз основа на подход, при който се отчита рискът. За тази цел финансовите субекти следва да криптират съответните данни при тяхното съхранение, предаване или, когато е необходимо, използване, въз основа на резултатите от двупосочен процес, а именно класификация на данните и цялостна оценка на риска в областта на ИКТ. Предвид сложността на криптиране на използваните данни, посочените в дял II от настоящия регламент финансови субекти следва да криптират използваните данни само когато това би било подходящо с оглед на резултатите от оценката на риска в областта на ИКТ. Когато обаче криптирането на използваните данни не е осъществимо или е твърде сложно, посочените в дял II от настоящия регламент финансови субекти следва да могат да защитят поверителността, цялостността и наличността на съответните данни чрез други мерки за сигурност на ИКТ. Предвид бързото технологично развитие в областта на криптографските техники, посочените в дял II от настоящия регламент финансови субекти следва да са в течение на съответните развития в областта на криптоанализа и да вземат предвид водещите практики и стандарти. Поради това, за да се справят с динамичната обстановка по отношение на криптографските заплахи, включително заплахите от напредващото развитие на квантовите изчислителни технологии, посочените в дял II от настоящия регламент финансови субекти следва да прилагат гъвкав подход, основан на намаляване на риска и на наблюдение.

(10) Сигурността на основаните на ИКТ операции и оперативните политики, процедури, протоколи и инструменти са от съществено значение за гарантиране на поверителността, цялостността и наличността на данните. Един основен аспект е стриктното отделяне на продукционните среди на ИКТ от средите, в които се разработват и тестват системите на ИКТ, или от други непродукционни среди. Това отделяне следва да служи като важна мярка за сигурност на ИКТ срещу непреднамерен и непозволен достъп до данните в продукционната среда, промени в тях и заличаването им, в резултат на което може да се стигне до големи смущения в стопанската дейност на финансовите субекти, посочени в дял II от настоящия регламент. Предвид настоящите практики за разработване на системи на ИКТ на финансовите субекти следва обаче да се даде възможност при изключителни обстоятелства да провеждат тестове в продукционни среди, при условие че обосноват такова тестване и получат необходимото одобрение.

([2]) Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ L 316, 14.11.2012 г., стр. 12, ELI: https://eur-lex.europa.eu/eli/reg/2012/1025/oj?locale=bg).

(11) Характеризиращата се с бързи промени среда в областта на ИКТ, уязвимите места на ИКТ и киберзаплахите налагат проактивен и всеобхватен подход за установяване, оценяване и отстраняване на уязвимите места на ИКТ. Без подобен подход финансовите субекти, техните клиенти, ползвателите или контрагентите може да бъдат изложени на сериозни рискове, които биха изложили на опасност оперативната устойчивост на техните цифрови технологии, сигурността на техните мрежи и наличността, автентичността, цялостността или поверителността на данните, които трябва да бъдат защитени с политиките и процедурите за сигурност на ИКТ. Поради това посочените в дял II от настоящия регламент финансови субекти следва да идентифицират и коригират уязвимите места в своята среда на ИКТ, а както финансовите субекти, така и третите страни, техни доставчици на услуги в областта на ИКТ, следва да се придържат към последователна, прозрачна и отговорна рамка за управление на уязвимите места. По същата причина финансовите субекти следва да наблюдават уязвимите места на ИКТ, като използват надеждни ресурси и автоматизирани инструменти, с които проверяват дали третите страни доставчици на услуги в областта на ИКТ осигуряват бързи действия по отношение на уязвимите места в предоставяните услуги в областта на ИКТ.

(12) Управлението на коригирането следва да бъде важна част от тези политики и процедури за сигурност на ИКТ, с които чрез тестване и внедряване в контролирана среда трябва да се намери решение за установените уязвими места и да се предотвратят смущения при инсталирането на корекции.

(13) С цел да се осигури своевременно и прозрачно съобщаване на потенциални заплахи за сигурността, които биха могли да повлияят на финансовия субект и свързаните с него заинтересовани страни, финансовите субекти следва да установят процедури за отговорно уведомяване на клиентите, на контрагентите и на обществеността за уязвими места на ИКТ. При определянето на тези процедури, финансовите субекти следва да вземат предвид фактори, включително сериозността на уязвимите места, потенциалното въздействие на такава уязвими места върху заинтересованите страни и готовността за коригиране или предприемане на мерки за намаляване на риска.

(14) За да се даде възможност да се предоставят права на достъп на ползвателите, посочените в дял II от настоящия регламент финансови субекти следва да въведат строги мерки за установяване на уникалната идентификация на лицата и системите, които ще имат достъп до информацията на финансовия субект. Неизпълнението на това би изложило финансовите субекти на потенциален непозволен достъп, нарушения на сигурността на данните и дейности с цел измама, с което ще се компрометира поверителността, цялостността и наличността на чувствителни финансови данни. Макар че използването на общи или съвместни профили следва да бъде разрешено по изключение при определени от финансовите субекти обстоятелства, финансовите субекти следва да гарантират, че се поддържа отчетността за действията, предприети чрез тези профили. Без този защитен механизъм потенциалните злонамерени ползватели ще бъдат в състояние да попречат на прилагането на мерки за разследване и корективни мерки, което ще направи финансовите субекти уязвими за неоткрити злонамерени действия или санкции за неспазване.

(15) За да се управлява бързото развитие на средите на ИКТ, посочените в дял II от настоящия регламент финансови субекти следва да прилагат стабилни политики и процедури за управление на проекти в областта на ИКТ, за да поддържат наличността, автентичността, цялостността и поверителността на данните. С тези политики и процедури за управление на проекти в областта на ИКТ следва да се идентифицират елементите, които са необходими за успешното управление на проекти в областта на ИКТ, включително промени в системите на ИКТ на финансови субект и тяхното придобиване, поддържане и развитие, независимо от избраната от финансовия субект методика за управление на проекти в областта на ИКТ. В контекста на тези политики и процедури финансовите субекти следва да приемат практики и методи за тестване, които отговарят на техните нужди, като същевременно се придържат към подход, при който се отчита рискът, и гарантират, че се поддържа сигурна, надеждна и устойчива среда на ИКТ. С цел да се гарантира сигурното изпълнение на проект в областта на ИКТ, финансовите субекти следва да гарантират, че служители от конкретни стопански сектори или роли, които са под влиянието или въздействието на този проект в областта на ИКТ, могат да предоставят необходимата информация и опит. За да се гарантира ефективен надзор, докладите за проектите в областта на ИКТ, по-специално за проекти, които засягат критични или важни функции, и за свързаните с тях рискове, следва да се представят на ръководния орган. Финансовите субекти следва да съобразят честотата и информацията за систематичните и текущите прегледи и доклади със значението и размера на съответните проекти в областта на ИКТ.

(16) Необходимо е да се гарантира, че софтуерните пакети, които посочените в дял II от настоящия регламент финансови субекти придобиват и разработват, са ефективно и сигурно интегрирани в съществуващата среда на ИКТ в съответствие с установените цели за стопанска сигурност и сигурност на информацията. Поради това финансовите субекти следва да извършат цялостна оценка на такива софтуерни пакети. За тази цел и за да се установят уязвимите места и потенциални пропуски в сигурността както в рамките на софтуерните пакети, така и в по-широките системи на ИКТ, финансовите субекти следва да извършват тестове за сигурност на ИКТ. За да се оцени цялостността на софтуера и да се гарантира, че използването на този софтуер не създава рискове за сигурността на ИКТ, финансовите субекти следва също така да направят преглед на първичните кодове на придобития софтуер, включително, когато е възможно, на лицензиран софтуер, предоставен от трети страни доставчици на услуги в областта на ИКТ, като използват както статични, така и динамични методи за тестване.

(17) Независимо от своя мащаб промените носят присъщи рискове и могат да породят значителни рискове от загуба на поверителност, цялостност и наличност на данни и по този начин могат да доведат до сериозни смущения в стопанската дейност. С цел да се осигури защитен механизъм за финансовите субекти срещу потенциални уязвими места и слабости на ИКТ, които биха могли да ги изложат на значителни рискове, е необходим строг процес на проверка, за да се потвърди, че всички промени отговарят на необходимите изисквания за сигурност на ИКТ. Поради това посочените в дял II от настоящия регламент финансови субекти следва да въведат като съществен елемент от техните политики и процедури за сигурност на ИКТ надеждни политики и процедури за управление на промените в ИКТ. За да се поддържат обективността и ефективността на процеса на управление на промените в ИКТ, да се предотвратят конфликти на интереси и да се гарантира, че промените в ИКТ се оценяват обективно, е необходимо да се отделят функциите, които отговарят за одобряването на тези промени, от функциите, които налагат и прилагат тези промени. С цел постигането на ефективни преходи, контролирано прилагане на промените в ИКТ и минимални смущения във функционирането на системите на ИКТ, финансовите субекти следва ясно да разпределят роли и отговорности, с които да се гарантира, че промените в ИКТ са планирани, адекватно тествани и че качеството е гарантирано. За да се гарантира продължаването на ефективното функциониране на системите на ИКТ и да се предостави защитен механизъм за финансовите субекти, те следва също така да разработят и прилагат аварийни процедури. Финансовите субекти следва ясно да установят тези аварийни процедури и да разпределят отговорности, за да осигурят бърза и ефективна реакция в случай на неуспешни промени в ИКТ.

(18) С цел откриване, управление и докладване на инциденти с ИКТ посочените в дял II от настоящия регламент финансови субекти следва да въведат политика за инциденти с ИКТ, обхващаща компонентите на процеса на управление на инциденти с ИКТ. За тази цел финансовите субекти следва да установят всички съответни контакти в рамките на организацията и извън нея, които могат да способстват за правилната координация и изпълнение на различните етапи в рамките на този процес. За да се оптимизират откриването и реакцията на инциденти с ИКТ и да се установят тенденциите сред тези инциденти, които са ценен източник на информация, позволяваща на финансовите субекти да идентифицират и отстранят първопричините и проблемите по ефективен начин, финансовите субекти следва по-специално да анализират подробно инцидентите с ИКТ, които считат за най-значими, наред с другото, поради редовното им повторение.

(19) За да се гарантира ранно и ефективно откриване на необичайни дейности, посочените в дял II от настоящия регламент финансови субекти следва да събират, наблюдават и анализират различните източници на информация и следва да разпределят свързаните роли и отговорности. Що се отнася до вътрешните източници на информация, регистрационните файлове представляват изключително важен източник, но финансовите субекти не следва да разчитат единствено на тях. Вместо това финансовите субекти следва да вземат предвид по-подробна информация, която да включва докладваното от други вътрешни функции, тъй като тези функции често са ценен източник на подходяща информация. По същата причина финансовите субекти следва да анализират и наблюдават събраната от външни източници информация, включително информация, предоставена от трети страни доставчици в областта на ИКТ относно инциденти, засягащи техните системи и мрежи, и други източници на информация, които финансовите субекти считат за подходящи. Доколкото такава информация представлява лични данни, се прилага законодателството на Съюза относно защитата на данните. Личните данни следва да бъдат ограничени до това, което е необходимо за откриване на инцидент.

(20) За да се улесни откриването на инциденти с ИКТ, финансовите субекти следва да съхраняват доказателства за тези инциденти. С цел да се гарантира, от една страна, че такива доказателства се съхраняват достатъчно дълго и за да се избегне, от друга страна, прекомерна регулаторна тежест, финансовите субекти следва да определят срока на съхранение, като вземат предвид, наред с другото, критичната значимост на данните и изискванията за съхранение, произтичащи от правото на Съюза.

(21) За да се гарантира навременното откриване на инциденти с ИКТ, посочените в дял II от настоящия регламент финансови субекти следва да считат, че установените критерии за задействане на процесите за откриване на инциденти с ИКТ и за реакция не са изчерпателни. Освен това, въпреки че финансовите субекти трябва да вземат предвид всеки от тези критерии, не следва да се счита за необходимо обстоятелствата, описани в критериите, да настъпват едновременно, а значението на засегнатите услуги в областта на ИКТ следва да се отчита по подходящ начин, за да се задействат процесите за откриване и за реагиране на инциденти с ИКТ.

(22) При разработването на политиката за непрекъснатост на дейността на ИКТ, посочените в дял II от настоящия регламент финансови субекти следва да вземат предвид основните компоненти на управлението на риска в областта на ИКТ, включително стратегията за управление на инциденти с ИКТ и комуникационната стратегия, процеса за управление на промените в ИКТ и рисковете, свързани трети страни доставчици на услуги в областта на ИКТ.

(23) Необходимо е да се определи набор от сценарии, които посочените в дял II от настоящия регламент финансови субекти следва да вземат предвид както за изпълнението на плановете за реакция и възстановяване на ИКТ, така и за тестването на плановете за непрекъснатост на дейността на ИКТ. Тези сценарии следва да служат като отправна точка за финансовите субекти, за да анализират както значението и правдоподобността на всеки сценарий, така и необходимостта от разработване на алтернативни сценарии. Финансовите субекти следва да поставят акцент върху тези сценарии, при които инвестирането в мерки за устойчивост може да се окаже по-ефикасно и ефективно. Чрез тестване на преминаването от първична инфраструктура на ИКТ към възпроизвеждащия я капацитет, резервни копия и възпроизвеждащи системи, финансовите институции следва да преценят дали този капацитет, резервно копие и тези съоръжения работят ефективно за достатъчен период от време и да гарантират, че нормалното функциониране на първичната инфраструктура на ИКТ се възстановява в съответствие със заложените цели за възстановяване на информацията.

(24) Необходимо е да се определят изисквания за оперативен риск и по-специално изисквания за проекти в областта на ИКТ и управление на промените в ИКТ и за управление на непрекъснатостта на дейността на ИКТ, които се основават на вече прилаганите за централните контрагенти, централните депозитари на ценни книжа и местата за търговия респективно съгласно Регламент (ЕС) № 648/2012 ([3]), Регламент (ЕС) № 600/2014 ([4]) и Регламент (ЕС) № 909/2014 ([5]) на Европейския парламент и на Съвета.

(25) Съгласно член 6, параграф 5 от Регламент (ЕС) 2022/2554 от финансовите субекти се изисква да преразгледат своята рамка за управление на риска в областта на ИКТ и да представят на компетентния си орган доклад за този преглед. За да се даде възможност на компетентните органи лесно да обработват информацията в тези доклади и да се гарантира адекватно предаване на тази информация, финансовите субекти следва да подават тези доклади в електронен формат с възможност за търсене.

(26) Изискванията към финансовите субекти, за които се прилага посочената в член 16 от Регламент (ЕС) 2022/2554 опростената рамка за управление на риска в областта на ИКТ, следва да бъдат съсредоточени върху онези основни области и елементи, които с оглед на мащаба, риска, размера и сложността на тези финансови субекти са необходими като минимум за гарантиране на поверителността, цялостността, наличността и автентичността на данните и услугите на тези финансови субекти. В този контекст тези финансови субекти следва да разполагат с вътрешна рамка за управление и контрол с ясни отговорности с цел да се даде възможност за ефективна и стабилна рамка за управление на риска. Освен това, за да се намалят административната и оперативната тежест, тези финансови субекти следва да разработят и документират само една политика, която е политика за сигурност на информацията, с която се определят принципите и правилата на високо равнище, необходими за защита на поверителността, цялостността, наличността и автентичността на данните и на услугите на тези финансови субекти.

(27) Разпоредбите на настоящия регламент се отнасят до областта на рамката за управление на риска в областта на ИКТ, като се уточняват конкретни елементи, приложими към финансовите субекти в съответствие с член 15 от Регламент (ЕС) 2022/2554, и чрез разработване на опростена рамка за управление на риска в областта на ИКТ за финансовите субекти, посочени в член 16, параграф 1 от посочения регламент. За да се осигури съгласуваност между обикновената и опростената рамка за управление на риска в областта на ИКТ и като се има предвид, че тези разпоредби следва да станат приложими едновременно, е целесъобразно те да бъдат включени в един законодателен акт.

(28) Настоящият регламент се основава на проектите на регулаторни технически стандарти, представени на Комисията от Европейския банков орган, Европейския орган за застраховане и професионално пенсионно осигуряване и Европейския орган за ценни книжа и пазари (европейски надзорни органи — ЕНО) след консултации с Агенцията на Европейския съюз за киберсигурност (ENISA).

([3]) Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета от 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на транзакции (ОВ L 201, 27.7.2012 г., стр. 1, ELI: https://eur-lex.europa.eu/eli/reg/2012/648/oj?locale=bg).

([4]) Регламент (ЕС) № 600/2014 на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 173, 12.6.2014 г., стр. 84, ELI: https://eur-lex.europa.eu/eli/reg/2014/600/oj?locale=bg).

([5]) Регламент (ЕС) № 909/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. за подобряване на сетълмента на ценни книжа в Европейския съюз и за централните депозитари на ценни книжа, както и за изменение на директиви 98/26/ЕО и 2014/65/ЕС и Регламент (ЕС) № 236/2012 (ОВ L 257, 28.8.2014 г., стр. 1, ELI: https://eur-lex.europa.eu/eli/reg/2014/909/oj?locale=bg).

(29) Съвместният комитет на европейските надзорни органи, посочен в член 54 от Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета ([6]), в член 54 от Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета ([7]) и в член 54 от Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета ([8]), проведе открити обществени консултации по проектите на регулаторни технически стандарти, въз основа на които е изготвен настоящият регламент, анализира потенциалните разходи и ползи от предложените стандарти и поиска мнението на Групата на участниците от банковия сектор, създадена в съответствие с член 37 от Регламент (ЕС) № 1093/2010, Групата на участниците от сектора на застраховането и презастраховането, създадена в съответствие с член 37 от Регламент (ЕС) № 1094/2010, и Групата на участниците от сектора на ценните книжа и пазарите, създадена в съответствие с член 37 от Регламент (ЕС) № 1095/2010.

(30) Доколкото обработването на лични данни е необходимо за спазване на задълженията, предвидени в настоящия акт, Регламент (ЕС) 2016/679 ([9]) и Регламент (ЕС) 2018/1725 ([10]) на Европейския парламент и на Съвета следва да се прилагат изцяло. Например при събиране на лични данни с цел да се гарантира подходящото откриване на инциденти в областта на киберсигурността следва да се прилага принципът за свеждане на данните до минимум. При съставянето на проекта на текст на настоящия акт бяха проведени консултации и с Европейски надзорен орган по защита на данните,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

ДЯЛ I

ОБЩИ ПРИНЦИПИ

Член 1

Цялостен рисков профил и сложност

При разработването и прилагането на посочените в дял II политики, процедури, протоколи и инструменти за сигурност на ИКТ и на посочената в дял III опростена рамка за управление на риска в областта на ИКТ се вземат предвид размерът и цялостният рисков профил на финансовия субект, както и естеството, мащабът и елементите на повишаване или намаляване на сложността на неговите услуги, дейности и операции, включително елементи, свързани с:

а) криптиране и криптография;

б) сигурност на основаните на ИКТ операции;

в) сигурност на мрежата;

([6]) 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, ELI: https://eur-lex.europa.eu/eli/reg/2010/1093/oj).

([7]) Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за застраховане и професионално пенсионно осигуряване), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/79/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 48, ELI: https://eur-lex.europa.eu/eli/reg/2010/1094/oj?locale=bg).

([8]) 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 (ОВ L 331, 15.12.2010 г., стр. 84, ELI: https://eur-lex.europa.eu/eli/reg/2010/1095/oj?locale=bg).

([9]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 година относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

г) управление на проекти в областта на ИКТ и на промените в ИКТ;

д) потенциалното въздействие на риска в областта на ИКТ върху поверителността, цялостността и наличността на данните и на смущенията в непрекъснатостта и наличността на дейностите на финансовия субект.

ДЯЛ II

ДОПЪЛНИТЕЛНО ХАРМОНИЗИРАНЕ НА ИНСТРУМЕНТИТЕ, МЕТОДИТЕ, ПРОЦЕСИТЕ И ПОЛИТИКИТЕ ЗА УПРАВЛЕНИЕ НА РИСКА В ОБЛАСТТА НА ИКТ В СЪОТВЕТСТВИЕ С ЧЛЕН 15 ОТ РЕГЛАМЕНТ (ЕС) 2022/2554

ГЛАВА I

Политики, процедури, протоколи и инструменти за сигурност на ИКТ

Раздел 1

Член 2

Общи елементи на политиките, процедурите, протоколите и инструментите за сигурност на ИКТ

1. Финансовите субекти гарантират, че техните политики за сигурност на ИКТ, сигурност на информацията и свързаните с тях процедури, протоколи и инструменти, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, са включени в рамката им за управление на риска в областта на ИКТ. Финансовите субекти установяват определените в настоящата глава политики, процедури, протоколи и инструменти за сигурност на ИКТ, които:

а) гарантират сигурността на мрежите;

б) съдържат защитни механизми срещу проникване и срещу злоупотреба с данни;

в) запазват, включително чрез използването на техники за криптиране, наличността, автентичността, цялостността и поверителността на данните;

г) осигуряват точното и бързо предаване на данните без съществени смущения и неоправдано забавяне.

2. Финансовите субекти гарантират, че посочените в параграф 1 политики за сигурност на ИКТ:

а) са приведени в съответствие с целите за сигурност на информацията на финансовия субект, включени в стратегията за оперативна устойчивост на цифровите технологии, посочена в член 6, параграф 8 от Регламент (ЕС) 2022/2554;

б) указват датата на официалното одобрение от страна на ръководния орган на политиките за сигурност на ИКТ;

в) съдържат показатели и мерки за:

i) наблюдение на прилагането на политиките, процедурите, протоколите и инструментите за сигурност на ИКТ;

ii) документиране на изключенията от посоченото прилагане;

iii) гарантиране на осигуряването на оперативната устойчивост на цифровите технологии на финансовия субект в случай на посочените в точка ii) изключения;

г) конкретизират отговорностите на служителите на всички равнища, за да се гарантира сигурността на ИКТ на финансовия субект;

д) посочват последиците от неспазване от страна на служителите на финансовия субект на политиките за сигурност на ИКТ, когато свързани с това разпоредби не са предвидени в други политики на финансовия субект;

е) включват списък на документацията, която трябва да се поддържа;

ж) доуточняват правилата за разделяне на функциите в контекста на модела на трите защитни слоя или на друга вътрешна система за управление и контрол на риска, според случая, с цел да се избегнат конфликти на интереси;

з) разглеждат водещи практики и, когато е приложимо, стандарти, определени в член 2, точка 1 от Регламент (ЕС) № 1025/2012;

и) установяват ролите и отговорностите за разработването, прилагането и поддържането на политиките, процедурите, протоколите и инструментите за сигурност на ИКТ;

й) се преразглеждат в съответствие с член 6, параграф 5 от Регламент (ЕС) 2022/2554;

к) вземат предвид съществените промени, засягащи финансовия субект, включително съществените промени в дейностите или процесите на финансовия субект, в обстановка по отношение на киберзаплахите или в приложимите правни задължения.

Раздел 2

Член 3

Управление на риска в областта на ИКТ

Финансовите субекти разработват, документират и прилагат политики и процедури за управление на риска в областта на ИКТ, които съдържат всички изброени по-долу елементи:

а) указание за одобрението на нивото на толерантност към риска в областта на ИКТ, установено в съответствие с член 6, параграф 8, буква б) от Регламент (ЕС) 2022/2554;

б) процедура и методика за провеждане на оценка на риска в областта на ИКТ, при която се установяват:

i) уязвимите места и заплахите, които засягат или може да засегнат поддържаните работни функции, системите на ИКТ и активите на ИКТ, поддържащи тези функции;

ii) количествените или качествените показатели за измерване на въздействието и вероятността от наличието на уязвимите места и заплахите, посочени в точка i);

в) процедурата за идентифициране, прилагане и документиране на мерките за третиране на риска в областта на ИКТ във връзка с идентифицираните и оценените рискове в областта на ИКТ, включително определянето на мерките за третиране на риска в областта на ИКТ, необходими за привеждане на рисковете в областта на ИКТ в рамките на нивото на толерантност към риска, посочено в буква а);

г) за остатъчните рискове в областта на ИКТ, които все още съществуват след прилагането на мерките за третиране на риска в областта на ИКТ, посочени в буква в):

i) разпоредбите относно установяването на тези остатъчни рискове в областта на ИКТ;

ii) разпределянето на ролите и отговорностите относно:

1) поемането на остатъчните рискове в областта на ИКТ, които надвишават нивото на толерантност към риска на финансовия субект, посочено в буква а);

2) за процеса на преглед, посочен в точка iv) от настоящата буква г);

iii) изготвяне на опис на поетите остатъчни рискове в областта на ИКТ, включително обосновка за тяхното поемане;

iv) разпоредбите относно извършвания поне веднъж годишно преглед на поетите остатъчни рискове в областта на ИКТ, включително:

1) установяването на всички промени в остатъчните рискове в областта на ИКТ;

2) оценката на наличните мерки за намаляване на риска;

3) оценката на това дали причините, обосноваващи поемането на остатъчни рискове в областта на ИКТ, са все още валидни и приложими към датата на прегледа;

д) разпореди относно наблюдението на:

i) всички промени в рисковете в областта на ИКТ и обстановката по отношение на киберзаплахите;

ii) вътрешни и външни уязвими места и заплахи:

iii) риск в областта на ИКТ за финансовия субект, който позволява своевременно откриване на промени, които биха могли да повлияят на рисковия му профил в областта на ИКТ;

е) разпоредби относно процес, с който да се гарантира, че са взети предвид всички промени в стратегията на финансовия субект във връзка със стопанската му дейност и в стратегията му за оперативна устойчивост на цифровите технологии.

За целите на параграф 1, буква в), посочената в същата буква процедура гарантира:

а) наблюдението на ефективността на приложените мерки за третиране на риска в областта на ИКТ;

б) оценката дали са постигнати установените нива на толерантност към риска за финансовия субект;

в) оценката дали финансовия субект е предприел действия за коригиране и подобряване на тези мерки, когато това е необходимо.

Раздел 3

Управление на активи на ИКТ

Член 4

Политика за управление на активи на ИКТ

(1) Като част от политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, финансовите субекти разработват, документират и прилагат политика за управление на активи на ИКТ.

2. С посочената в параграф 1 политика за управление на активи на ИКТ се постига следното:

а) предвиждат се наблюдението и управлението на жизнения цикъл на активи на ИКТ, установени и класифицирани в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554;

б) предвижда се съхраняването от финансовия субект на записи за всички изброени по-долу елементи:

i) уникалния идентификатор на всеки актив на ИКТ;

ii) информацията относно мястото, физическо или логическо, на всички активи на ИКТ;

iii) класификацията на всички активи на ИКТ, посочени в член 8, параграф 1 от Регламент (ЕС) 2022/2254;

iv) самоличността на собствениците на актив на ИКТ;

v) работните функции или услуги, поддържани от актива на ИКТ;

vi) изискванията за непрекъснатост на дейността на ИКТ, включително целевото време за възстановяване на информацията и целевата точка на възстановяване;

vii) дали активът на ИКТ може да бъде или е изложен на външни мрежи, включително интернет;

viii) връзките и взаимозависимостта между активи на ИКТ и работните функции, използващи всеки актив на ИКТ;

ix) когато е приложимо, по отношение на всички активи на ИКТ — крайните дати на редовните, разширените и персонализираните услуги за поддръжка, предоставяни от трети страни доставчици на услуги в областта на ИКТ, след които тези активи на ИКТ вече не се поддържат от доставчика им или от трета страна доставчик на услуги в областта на ИКТ;

в) за финансови субекти, различни от микропредприятия, се предвижда тези финансови субекти да съхраняват записи на информацията, необходима за извършване на специална оценка на риска в областта на ИКТ на всички наследени системи на ИКТ, посочени в член 8, параграф 7 от Регламент (ЕС) 2022/2554.

Член 5

Процедура за управление на активи на ИКТ

1. Финансовите субекти разработват, документират и прилагат процедура за управление на активи на ИКТ.

2. В посочената в параграф 1 процедура за управление на активи на ИКТ се доуточняват критериите за извършване на оценка на критичната значимост на информационните активи и активите на ИКТ, поддържащи работни функции. При тази оценка се отчитат:

а) рискът в областта на ИКТ, свързан с тези работни функции и с тяхната зависимост от информационните активи или активите на ИКТ;

б) начинът, по който загубата на поверителността, цялостността и наличността на такива информационни активи и активи на ИКТ би оказала въздействие върху работните процеси и дейности на финансовите субекти.

Раздел 4

Криптиране и криптография

Член 6

Криптиране и криптографски механизми за контрол

(1) Като част от своите политики, процедури, протоколи и инструменти за сигурност на ИКТ, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, финансовите субекти разработват, документират и прилагат политика относно криптирането и криптографските механизми за контрол.

2. Финансовите субекти разработват посочената в параграф 1 политика относно криптирането и криптографските механизми за контрол въз основа на резултатите от одобрена класификация на данните и оценка на риска в областта на ИКТ. Посочената политика съдържа правила за всички изброени по-долу елементи:

а) криптиране на данните при тяхното съхранение и предаване;

б) криптиране на данните при тяхното използване, когато е необходимо;

в) криптиране на вътрешни мрежови връзки и пренос с външни страни;

г) посоченото в член 7 управление на криптографския ключ, с което се установяват правила за правилното използване, защитата и жизнения цикъл на криптографските ключове.

За целите на буква б), когато криптирането на използваните данни не е възможно, финансовите субекти обработват използваните данни в отделна и защитена среда или предприемат еквивалентни мерки, за да гарантират поверителността, цялостността, автентичността и наличността на данните.

3. Финансовите субекти включват в посочената в параграф 1 политика относно криптирането и криптографските механизми за контрол критерии за подбора на криптографски техники и практики за използване, като вземат предвид водещите практики и стандарти, определени в член 2, точка 1 от Регламент (ЕС) № 1025/2012, и класификацията на съответните активи на ИКТ, установена в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554. Финансовите субекти, които не са в състояние да се придържат към водещите практики или стандарти, или да използват най-надеждните техники, приемат мерки за намаляване на риска и за наблюдение, които гарантират устойчивост срещу киберзаплахи.

4. Финансовите субекти включват в посочената в параграф 1 политика относно криптирането и криптографските механизми за контрол разпоредби за актуализиране или промяна, когато това е необходимо, на криптографската технология въз основа на развитието в областта на криптоанализа. Тези актуализации или промени гарантират, че криптографската технология остава устойчива срещу киберзаплахи, както се изисква в член 10, параграф 2, буква а). Финансовите субекти, които не са в състояние да актуализират или променят криптографската технология, приемат мерки за намаляване на риска и за наблюдение, които гарантират устойчивост срещу киберзаплахи.

5. Финансовите субекти включват в посочената в параграф 1 политика относно криптирането и криптографските механизми за контрол изискване за документиране на приемането на мерки за намаляване на риска и за наблюдение, приети в съответствие с параграфи 3 и 4, и за предоставяне на аргументирано обяснение за това.

Член 7

Управление на криптографски ключове

1. Финансовите субекти включват в политиката за управление на криптографски ключове, посочена в член 6, параграф 2, буква г), изисквания за управлението на криптографски ключове през целия им жизнен цикъл, включително генерирането, подновяването, съхраняването, запазването на резервни копия, архивирането, извличането, предаването, изтеглянето от употреба, отмяната и унищожаването на тези криптографски ключове.

2. Финансовите субекти установяват и прилагат механизми за контрол с цел защита на криптографските ключове през целия им жизнен цикъл срещу загуба, непозволен достъп, оповестяване и модификация. Финансовите субекти разработват тези механизми за контрол въз основа на резултатите от одобрено класифициране на данните и извършена оценка на риска в областта на ИКТ.

3. Финансовите субекти разработват и прилагат методи за замяна на криптографските ключове в случай на загуба, или когато тези ключове са компрометирани или повредени.

4. Финансовите субекти създават и поддържат регистър за всички сертификати и устройства за съхранение на сертификати поне за активи на ИКТ, поддържащи критични или важни функции. Финансовите субекти редовно актуализират този регистър.

5. Финансовите субекти гарантират бързото подновяване на сертификатите преди изтичането на валидността им.

раздел 5

Сигурност на основаните на ИКТ операции

Член 8

Политики и процедури за основаните на ИКТ операции

1. Като част от политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, финансовите субекти разработват, документират и прилагат политики и процедури за управление на основаните на ИКТ операции. С тези политики и процедури се определя начинът, по който финансовите субекти управляват, наблюдават, контролират и възстановяват своите активи на ИКТ, включително документирането на основаните на ИКТ операции.

2. Посочените в параграф 1 политики и процедури за основани на ИКТ операции съдържат всички изброени по-долу елементи:

а) описание на активите на ИКТ, включително всички изброени по-долу елементи:

   i) изисквания относно сигурното инсталиране, поддържане, конфигуриране и деинсталиране на дадена система на ИКТ;

   ii) изисквания относно управлението на информационни активи, използвани от активи на ИКТ, включително тяхната обработка и употреба, както автоматизирано, така и ръчно;

   iii) изисквания относно идентифицирането и контрола на наследените системи на ИКТ;

б) механизми за контрол и наблюдение на системи на ИКТ, включително всички изброени по-долу елементи:

   i) изисквания за резервни копия и възстановяване на системи на ИКТ;

   ii) изисквания за планиране, като се взема предвид взаимозависимостта между системите на ИКТ;

   iii) протоколи за одитна следа и информация за регистриране в система;

   iv) изисквания, с които се гарантира, че извършването на вътрешен одит и друго тестване свеждат до минимум смущенията в стопанските дейности;

   v) изисквания за отделяне на продукционните среди на ИКТ от среди за разработка, тестване и други непродукционни среди;

   vi) изисквания за провеждане на разработването и тестването в среди, които са отделени от продукционната среда;

   vii) изисквания за провеждане на разработването и тестването в продукционни среди;

в) отстраняване на грешки относно системи на ИКТ, включително всички изброени по-долу елементи:

i) процедури и протоколи за отстраняване на грешки;

ii) договори за поддръжка и пренасочване на управлението на инциденти, включително външни договори за поддръжка в случай на неочаквани оперативни или технически проблеми;

iii) процедури за рестартиране, премахване и възстановяване на система на ИКТ, които се използват в случай на смущение на система на ИКТ.

За целите на буква б), точка v) при отделянето се вземат предвид всички компоненти на средата, включително профили, данни или връзки, както се изисква в член 13, първа алинея, буква а).

За целите на буква б), точка vii) в посочените в параграф 1 политики и процедури се предвижда, че случаите, в които се извършва тестване в продукционна среда, са ясно идентифицирани, обосновани, за ограничени периоди от време са и са одобрени от съответната функция в съответствие с член 16, параграф 6. По време на дейностите по разработване и тестване в продукционна среда финансовите субекти гарантират наличността, поверителността, цялостността и автентичността на системите на ИКТ и на данните в продукционната среда.

Член 9

Управление на капацитета и ефективността

1. Като част от политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, финансовите субекти разработват, документират и прилагат процедури за управление на капацитета и ефективността за посочените по-долу елементи:

а) идентифицирането на изискванията във връзка с капацитета на техните системи на ИКТ;

б) прилагането на оптимизиране на ресурсите;

в) процедурите за наблюдение за поддържането и подобряването на:

i) наличността на данни и системи на ИКТ;

ii) ефикасността на системите на ИКТ;

iii) предотвратяването на недостига на капацитет във връзка с ИКТ.

2. С посочените в параграф 1 процедури за управление на капацитета и ефективността се гарантира, че финансовите субекти предприемат мерки, които са подходящи с оглед на спецификите на системите на ИКТ с дълги или сложни процеси на доставка или одобрение или системи на ИКТ, които изискват много ресурси.

Член 10

Уязвими места и управление на коригирането

1. Като част от политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, финансовите субекти разработват, документират и прилагат процедури за управление на уязвими места.

2. С посочените в параграф 1 процедури за управление на уязвими места се постига следното:

а) установяват се и се актуализират подходящи и надеждни информационни ресурси за изграждане и поддържане на осведомеността относно уязвимите места;

б) гарантира се извършването на автоматизирано сканиране за уязвимите места и оценки на активите на ИКТ, като честотата и обхватът на тези дейности са съизмерими с класификацията, установена в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554, и с цялостния рисков профил на актива на ИКТ;

в) проверява се дали:

i) трети страни доставчици на услуги в областта на ИКТ се справят с уязвимите места, свързани с предоставяните на финансовия субект услуги в областта на ИКТ;

ii) тези доставчици на услуги докладват своевременно на финансовия субект поне за критичните уязвими места и статистически данни и тенденции;

г) проследява се използването на:

i) библиотеки на трети страни, включително библиотеки с отворен код, използвани от услуги в областта на ИКТ, поддържащи критични или важни функции;

ii) услуги в областта на ИКТ, разработени от самия финансов субект или специално персонализирани или разработени за финансовия субект от трета страна доставчик на услуги в областта на ИКТ;

д) установяват се процедури за отговорно уведомяване на клиентите, контрагентите и на обществеността за уязвими места;

е) отдава се приоритет на внедряването на корекции и други мерки за намаляване на риска с цел отстраняване на установените уязвими места;

ж) наблюдава се и се проверява отстраняването на уязвимите места;

з) изискват се записване на всички открити уязвими места, засягащи системите на ИКТ, и наблюдение на намирането на решение за тях.

За целите на буква б) финансовите субекти извършват поне веднъж седмично автоматизирано сканиране за уязвими места и оценки на активи на ИКТ за активите на ИКТ, поддържащи критични или важни функции.

За целите на буква в) финансовите субекти искат от трети страни доставчици на услуги в областта на ИКТ да проучат съответните уязвими места, да определят първопричините и да приложат подходящи действия за намаляване на риска.

За целите на буква г), когато е подходящо и в сътрудничество с трета страна доставчик на услуги в областта на ИКТ, финансовите субекти наблюдават версията и възможните актуализации на библиотеките на трети страни. Когато се използват готови за употреба (стандартизирани) активи на ИКТ или компоненти на активи на ИКТ, придобити и използвани при осъществяването на услуги в областта на ИКТ, които не поддържат критични или важни функции, финансовите субекти проследяват доколкото е възможно използването на библиотеки на трети страни, включително библиотеки с отворен код.

За целите на буква е) финансовите субекти вземат предвид критичната значимост на уязвимото място, установената в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554 класификация и рисковия профил на активите на ИКТ, засегнати от установените уязвими места.

3. Като част от политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, финансовите субекти разработват, документират и прилагат процедури за управление на коригирането.

4. С посочените в параграф 3 процедури за управление на коригирането се постига следното:

а) доколкото е възможно, идентифицират се и се оценяват наличните софтуерни и хардуерни корекции и актуализации с помощта на автоматизирани инструменти;

б) идентифицират се процедурите при извънредни ситуации във връзка с коригирането и актуализирането на активи на ИКТ;

в) тестват се и се внедряват софтуерните и хардуерните корекции и актуализациите, посочени в член 8, параграф 2, буква б), точки v), vi) и vii);

г) определят се сроковете за инсталирането на софтуерни и хардуерни корекции и актуализации и процедурите за пренасочване на управлението, в случай че тези срокове не могат да бъдат спазени.

Член 11

Сигурност на данните и системата

1. Като част от политиките, процедурите, протоколите и инструментите за сигурност на ИКТ, посочени в член 9, параграф 2 от Регламент (ЕС) 2022/2554, финансовите субекти разработват, документират и прилагат процедура за сигурност на данните и системата.

2. Посочената в параграф 1 процедура за сигурност на данните и системата съдържа всички изброени по-долу елементи, свързани със сигурността на данните и системите на ИКТ, в съответствие с класификацията, установена съгласно член 8, параграф 1 от Регламент (ЕС) 2022/2554:

а) ограниченията за достъп, посочени в член 21 от настоящия регламент, в подкрепа на изискванията за защита за всяко ниво на класификация;

б) идентифицирането на базови стандарти за сигурно конфигуриране за активи на ИКТ, с които се свежда до минимум излагането на тези активи на ИКТ на киберзаплахи, и мерки за редовна проверка дали тези базови стандарти са ефективно внедрени;

в) идентифицирането на мерки за сигурност с цел да се гарантира, че в системите на ИКТ и крайните устройства е инсталиран само разрешен софтуер;

г) идентифицирането на мерки за сигурност срещу злонамерени кодове;

д) идентифицирането на мерки за сигурност с цел да се гарантира, че за предаването и съхранението на данни на финансовия субект се използват само разрешени носители за съхранение на данни, системи и крайни устройства;

е) посочените по-долу изисквания с цел да се гарантира използването на преносими крайни устройства и частни непреносими крайни устройства:

i) изискването за използване на решение за управление, предназначено за дистанционно управление на крайните устройства и дистанционно заличаване на данните на финансовия субект;

ii) изискването за използване на механизми за сигурност, които не могат да бъдат модифицирани, отстранени или заобиколени по непозволен начин от служителите или от трети страни доставчици на услуги в областта на ИКТ;

iii) изискването за използване на подвижни устройства за съхранение на данни само когато остатъчният риск в областта на ИКТ се запазва в рамките на нивото на толерантност към риска за финансовия субект, посочено в член 3, първа алинея, буква а);

ж) процеса за сигурно заличаване на данни, намиращи се в помещенията на финансовия субект или съхранявани външно, които финансовият субект вече не трябва да събира или съхранява;

з) процеса за сигурно унищожаване или извеждане от експлоатация на съдържащи поверителна информация устройства за съхранение на данни, намиращи се в помещенията на финансовия субект или съхранявани външно;

и) идентифицирането и прилагането на мерки за сигурност за предотвратяване на загуба и изтичане на данни за системи и крайни устройства;

й) прилагането на мерки за сигурност с цел да се гарантира, че работата от разстояние и използването на частни крайни устройства не оказват неблагоприятно въздействие върху сигурността на ИКТ на финансовия субект;

к) за активи на ИКТ или услуги в областта на ИКТ, управлявани от трета страна доставчик на услуги в областта на ИКТ — идентифицирането и изпълнението на изискванията за поддържане на оперативна устойчивост на цифровите технологии в съответствие с резултатите от класификацията на данните и оценката на риска в областта на ИКТ.

За целите на буква б) при посочените в същата буква базови стандарти за сигурно конфигуриране се вземат предвид водещите практики и подходящите техники, изложени в стандартите, определени в член 2, точка 1 от Регламент (ЕС) № 1025/2012.

За целите на буква к) финансовите субекти вземат предвид следното:

а) прилагането на препоръчаните от доставчика настройки на елементите, управлявани от финансовия субект;

б) ясно разпределение на ролите и отговорностите в областта на сигурността на информацията между финансовия субект и трета страна доставчик на услуги в областта на ИКТ в съответствие с принципа на пълната отговорност на финансовия субект спрямо неговата трета страна доставчик на услуги в областта на ИКТ, посочен в член 28, параграф 1, буква а) от Регламент (ЕС) 2022/2554, и за финансовите субекти, посочени в член 28, параграф 2 от същия регламент, и в съответствие с политиката на финансовия субект относно използването на услуги в областта на ИКТ, поддържащи критични или важни функции;

в) необходимостта от осигуряване и поддържане на необходимите компетентности в рамките на финансовия субект при управлението и сигурността на използваната услуга;

г) технически и организационни мерки за свеждане до минимум на рисковете, свързани с инфраструктурата, използвана от трета страна доставчик на услуги в областта на ИКТ за нейните услуги в областта на ИКТ, като се вземат предвид водещите практики и стандарти, определени в член 2, точка 1 от Регламент (ЕС) № 1025/2012.

Член 12

Регистриране

1. Като част от защитните механизми срещу проникване и срещу злоупотреба с данни финансовите субекти разработват, документират и прилагат процедури, протоколи и инструменти за регистриране.

2. Посочените в параграф 1 процедури, протоколи и инструменти за регистриране съдържат всички изброени по-долу елементи:

а) идентифицирането на събитията, които трябва да се регистрират, срока на съхранение на регистрационните файлове и мерките за защита и обработка на данните в регистрационните файлове, като се има предвид целта, за която се създават регистрационните файлове;

б) съгласуването на нивото на детайлност на регистрационните файлове с тяхното предназначение и употреба, за да се даде възможност за ефективно откриване на необичайни дейности, както е посочено в член 24;

в) изискването за регистриране на събития, свързани с всички изброени по-долу елементи:

i) логически и физически контрол на достъпа, както е посочено в член 21, и управление на самоличността;

ii) управление на капацитета;

iii) управление на промените;

iv) основани на ИКТ операции, включително дейности на системи на ИКТ;

v) дейности за мрежови пренос, включително функционирането на мрежата на ИКТ;

г) мерки за защита на системите за регистриране и на съдържащата се в регистрите информация срещу подправяне, заличаване и непозволен достъп при съхранение, предаване и, по целесъобразност, използване;

д) мерки за откриване на повреда на системите за регистриране;

е) без да се засягат каквито и да е приложими регулаторни изисквания съгласно правото на Съюза или националното право, синхронизирането на времето на всяка от системите на ИКТ на финансовия субект въз основа на документиран надежден референтен източник на време.

За целите на буква а) финансовите субекти определят срока на съхранение, като вземат предвид целите за стопанска сигурност и сигурност на информацията, причините за записване на събитието в регистрационните файлове и резултатите от оценката на риска в областта на ИКТ.

Раздел 6

Сигурност на мрежата

Член 13

Управление на сигурността на мрежата

Като част от защитните механизми, гарантиращи сигурността на мрежите срещу проникване и срещу злоупотреба с данни, финансовите субекти разработват, документират и прилагат политики, процедури, протоколи и инструменти за управление на сигурността на мрежата, включващи всички изброени по-долу елементи:

а) разделянето и сегментирането на системите и мрежите на ИКТ, като се вземат предвид:

i) критичната значимост или важността на функцията, която поддържат тези системи и мрежи на ИКТ;

ii) класификацията, установена в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554;

iii) цялостният рисков профил на активите на ИКТ, използващи тези системи и мрежи на ИКТ;

б) документацията за всички мрежови връзки и информационни потоци на финансовия субект;

в) използването на отделна и специализирана мрежа за управлението на активи на ИКТ;

г) идентифицирането и прилагането на механизми за контрол на достъпа до мрежата за предотвратяване и откриване на връзки към мрежата на финансовия субект от всяко неупълномощено устройство или система или всяка крайна точка, която не отговаря на изискванията за сигурност на финансовия субект;

д) криптирането на мрежовите връзки, преминаващи през корпоративни мрежи, обществени мрежи, домашни мрежи, мрежи на трети страни и безжични мрежи, за използваните комуникационни протоколи, като се вземат предвид резултатите от одобрената класификация на данните, резултатите от оценката на риска в областта на ИКТ и криптирането на мрежови връзки, посочено в член 6, параграф 2;

е) проектирането на мрежи в съответствие с установените от финансовия субект изисквания за сигурност на ИКТ, като се вземат предвид водещите практики за осигуряване на поверителността, цялостността и наличността на мрежата;

ж) защитата на мрежовия пренос между вътрешните мрежи и интернет и други външни връзки;

з) установяването на ролите и отговорностите, както и на етапите за спецификацията, прилагането, одобрението, промяната и прегледа на правилата на защитната стена и филтрите за връзка;

и) извършването на прегледи на архитектурата на мрежата и проектирането на мрежовата сигурност веднъж годишно, а за микропредприятията — периодично, с цел установяване на потенциални уязвими места;

й) мерките за временно обособяване, когато е необходимо, на подмрежи и мрежови компоненти и устройства;

к) прилагането на базови стандарти за сигурно конфигуриране за всички компоненти на мрежата и укрепване на мрежата и мрежовите устройства в съответствие с всички указания на доставчика, когато е приложимо — със стандартите, както са определени в член 2, точка 1 от Регламент (ЕС) № 1025/2012, както и с водещите практики;

л) процедурите за ограничаване, заключване и прекратяване на системни сесии и сесии от разстояние след определен период на неактивност;

м) за споразумения за мрежови услуги:

i) идентифицирането и спецификацията на ИКТ и мерки за сигурност на информацията, нива на обслужване и изисквания за управление на всички мрежови услуги;

ii) дали тези услуги са предоставени от вътрешногрупов доставчик на услуги в областта на ИКТ или от трети страни доставчици на услуги в областта на ИКТ.

За целите на буква з) финансовите субекти извършват редовен преглед на правилата на защитната стена и филтрите за връзка в съответствие с установената в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554 класификация и цялостния рисков профил на включените системи на ИКТ. За системи на ИКТ, които поддържат критични или важни функции, финансовите субекти проверяват адекватността на съществуващите правила на защитната стена и филтрите за връзка най-малко на всеки 6 месеца.

Член 14

Защита на информация при предаване

1. Като част от защитните механизми за запазване на наличността, автентичността, цялостността и поверителността на данните финансовите субекти разработват, документират и прилагат политики, процедури, протоколи и инструменти за защитата на информацията при предаване. По-специално финансовите субекти гарантират всичко изброено по-долу:

а) наличността, автентичността, цялостността и поверителността на данните при предаване по мрежата и установяването на процедури за достъп в съответствие с тези изисквания;

б) предотвратяването и откриването на изтичане на данни и сигурно предаване на информация между финансовия субект и външни страни;

в) прилагането, документирането и редовното преразглеждане на изискванията за поверителност или правилата за неоповестяване, отразяващи нуждите на финансовия субект за защита на информацията както за служителите на финансовия субект, така и за трети страни.

2. Финансовите субекти разработват политики, процедури, протоколи и инструменти за защита на посочената в параграф 1 информация при предаване въз основа на резултатите от одобрено класифициране на данните и извършена оценка на риска в областта на ИКТ.

Раздел 7

Управление на проекти в областта на ИКТ и на промените в ИКТ

Член 15

Управление на проекти в областта на ИКТ

1. Като част от защитните механизми за запазване на наличността, автентичността, цялостността и поверителността на данните финансовите субекти разработват, документират и прилагат политика за управление на проекти в областта на ИКТ.

2. С посочената в параграф 1 политика за управление на проекти в областта на ИКТ се определят елементите, които гарантират ефективното управление на проектите в областта на ИКТ, свързани с придобиването, поддържането и, когато е приложимо, развитието на системите на ИКТ на финансовия субект.

3. Посочената в параграф 1 политика за управление на проекти в областта на ИКТ съдържа всички изброени по-долу елементи:

а) цели на проектите в областта на ИКТ;

б) управление на проектите в областта на ИКТ, включително роли и отговорности;

в) планиране, времева рамка и етапи на проектите в областта на ИКТ;

г) оценка на риска на проектите в областта на ИКТ;

д) съответните ключови етапи;

е) изисквания за управление на промените;

ж) тестването на всички изисквания, включително изискванията за сигурност, и съответния процес на одобрение при внедряване на система на ИКТ в продукционната среда.

4. С посочената в параграф 1 политика за управление на проекти в областта на ИКТ се гарантира сигурното изпълнение на проекта в областта на ИКТ чрез предоставяне на необходимата информация и експертен опит от сферата на дейност или функциите, засегнати от проекта в областта на ИКТ.

5. В съответствие с оценката на риска на проекта в областта на ИКТ, посочена в параграф 3, буква г), в посочената в параграф 1 политика за управление на проекти в областта на ИКТ се предвижда, че създаването и напредъкът на проектите в областта на ИКТ, засягащи критични или важни функции на финансовия субект и свързаните с тях рискове, се докладват на ръководния орган, както следва:

а) индивидуално или групово, в зависимост от важността и размера на проектите в областта на ИКТ;

б) периодично и, когато е необходимо, въз основа на събития.

Член 16

Придобиване, разработване и поддръжка на системи на ИКТ

1. Като част от защитните механизми за запазване на наличността, автентичността, цялостността и поверителността на данните финансовите субекти разработват, документират и прилагат политика, с която се уреждат придобиването, разработването и поддържането на системи на ИКТ. С тази политика се постига следното:

а) установяват се практиките и методиките за сигурност, свързани с придобиването, разработването и поддържането на системи на ИКТ;

б) изисква се идентифицирането на:

i) технически спецификации, както и на технически спецификации за ИКТ, както са определени в член 2, точки 4 и 5 от Регламент (ЕС) № 1025/2012;

ii) изисквания, свързани с придобиването, разработването и поддържането на системи на ИКТ, като се поставя специален акцент върху изискванията за сигурност на ИКТ и тяхното одобрение от съответната работна функция и от собственика на актив на ИКТ в съответствие с вътрешните правила за управление на финансовия субект;

в) определят се мерки за намаляване на риска от непреднамерена промяна или преднамерено манипулиране на системи на ИКТ по време на разработването, поддържането и внедряването на тези системи на ИКТ в продукционната среда.

2. Финансовите субекти разработват, документират и прилагат процедура за придобиване, разработване и поддържане на системи на ИКТ за тестване и одобрение на всички системи на ИКТ преди тяхното използване и след поддръжка, в съответствие с член 8, параграф 2, буква б), точки v), vi) и vii). Равнището на тестване е съизмеримо с критичната значимост на съответните работни процедури и съответните активи на ИКТ. Целта на тестването е да се провери дали новите системи на ИКТ са подходящи за своето предназначение, включително качеството на разработения вътрешно софтуер.

В допълнение към посочените в първата алинея изисквания, при проектирането и провеждането на тестването, посочено в първа алинея, централните контрагенти по целесъобразност включват като участници:

а) клирингови членове и клиенти;

б) оперативно съвместими централни контрагенти;

в) други заинтересовани страни.

В допълнение към посочените в първата алинея изисквания при проектирането и провеждането на тестването, посочено в първа алинея, централните депозитари на ценни книжа по целесъобразност включват като участници:

а) ползватели;

б) доставчици на критични комунални услуги и доставчици на критични услуги;

в) други централни депозитари на ценни книжа;

г) други пазарни инфраструктури;

д) всички други институции, по отношение на които централните депозитари на ценни книжа са установили взаимозависимости в политиката си за осигуряване на непрекъснатост на дейността.

3. Процедурата, посочена в параграф 2, включва извършването на преглед на първичния код, обхващащ статично и динамично тестване. Това тестване включва тестване на сигурността за системи и приложения, изложени на достъп до интернет, в съответствие с член 8, параграф 2, буква б), точки v), vi) и vii). Финансовите субекти:

а) установяват и анализират уязвими места и аномалии в първичния код;

б) приемат план за действие за отстраняване на тези уязвими места и аномалии;

в) наблюдават прилагането на този план за действие.

4. В посочената в параграф 2 процедура е включено тестване за сигурност на софтуерни пакети не по-късно от етапа на интегриране в съответствие с член 8, параграф 2, буква б), точки v), vi) и vii).

5. В посочената в параграф 2 процедура се предвижда, че:

а) в непродукционните среди се съхраняват само анонимизирани, псевдонимизирани или произволни данни от продукционната среда;

б) финансовите субекти трябва да защитават цялостността и поверителността на данните в непродукционните среди.

6. Чрез дерогация от параграф 5, в посочената в параграф 2 процедура може да се предвидят разпоредби за това, че данните от продукционната среда се съхраняват само за конкретни случаи на тестване, за ограничени периоди от време и след одобрение от съответната функция, както и разпоредби за докладването на такива случаи на функцията за управление на риска в областта на ИКТ.

7. Посочената в параграф 2 процедура съдържа прилагането на механизмите за контрол за защита на цялостността на първичния код на системи на ИКТ, които са разработени вътрешно или от трета страна доставчик на услуги в областта на ИКТ и доставени на финансовия субект от трета страна доставчик на услуги в областта на ИКТ.

8. В посочената в параграф 2 процедура се предвижда, че лицензираният софтуер и, когато е осъществимо, първичният код, предоставен от трета страна доставчик на услуги в областта на ИКТ или получен от проекти с отворен код, трябва да бъдат анализирани и тествани в съответствие с параграф 3 преди внедряването им в продукционната среда.

9. Параграфи 1—8 от настоящия член се прилагат по отношение на системи на ИКТ, разработени или управлявани от ползватели извън функцията на ИКТ, използващи подход, при който се отчита рискът.

Член 17

Управление на промените в ИКТ

1. Като част от защитните механизми за запазване на наличността, автентичността, цялостността и поверителността на данните финансовите субекти включват в управлението на промените в ИКТ процедурите, посочени в член 9, параграф 4, буква д) от Регламент (ЕС) 2022/2554, по отношение на всички промени в софтуера, хардуера, компонентите на софтуера на производителя, системите или параметрите за сигурност всички изброени по-долу елементи:

а) проверка дали са изпълнени изискванията за сигурност на ИКТ;

б) механизми за гарантиране на независимостта на функциите, които одобряват промените, и функциите, отговарящи за искането и прилагането на тези промени;

в) ясно описание на ролите и отговорностите, за да се гарантира, че:

i) промените са определени и планирани;

ii) предвиден е подходящ преход;

iii) промените се тестват и се финализират по контролиран начин;

iv) налице е ефективно осигуряване на качеството;

г) документацията и съобщаването на подробности за промените, включително:

i) целта и обхвата на промяната;

ii) срокът за прилагането на промяната;

iii) очакваните резултати:

д) идентифицирането на аварийните процедури и отговорности, включително процедури и отговорности за прекъсване прилагането на промени или възстановяване при неуспешно приложени промени;

е) процедурите, протоколите и инструментите за управление на промени при извънредни ситуации, които предоставят подходящи защитни механизми;

ж) процедурите за документиране, повторно оценяване, оценяване и одобрение на промени при извънредни ситуации след тяхното прилагане, включително временни решения и корекции;

з) идентифицирането на потенциалното въздействие на промяната върху съществуващите мерки за сигурност на ИКТ и оценка дали такава промяна изисква приемането на допълнителни мерки за сигурност на ИКТ.

2. След като са направили значителни промени в своите системи на ИКТ, централните контрагенти и централните депозитари на ценни книжа подлагат своите системи на ИКТ на строго тестване чрез симулиране на неблагоприятни условия.

При проектирането и провеждането на тестването, посочено в първа алинея, централните контрагенти по целесъобразност включват като участници:

а) клирингови членове и клиенти;

б) централни контрагенти, сключили споразумение за оперативна съвместимост с друг централен контрагент;

в) други заинтересовани страни.

При проектирането и провеждането на тестването, посочено в първа алинея, централните депозитари на ценни книжа по целесъобразност включват като участници:

а) ползватели;

б) доставчици на критични комунални услуги и доставчици на критични услуги;

в) други централни депозитари на ценни книжа;

г) други пазарни инфраструктури;

д) всички други институции, по отношение на които централните депозитари на ценни книжа са установили взаимозависимости в политиката си за осигуряване на непрекъснатост на дейността на ИКТ.

Раздел 8

Член 18

Физическа сигурност и сигурност на заобикалящата среда

1. Като част от защитните механизми за запазване на наличността, автентичността, цялостността и поверителността на данните финансовите субекти определят, документират и прилагат политика за физическа сигурност и сигурност на заобикалящата среда. Финансовите субекти разработват тази политика с оглед на обстановката по отношение на киберзаплахите в съответствие с установената в член 8, параграф 1 от Регламент (ЕС) 2022/2554 класификация и с оглед на цялостния рисков профил на активите на ИКТ и достъпните информационни активи.

2. Посочената в първа алинея политика за физическа сигурност и сигурност на заобикалящата среда съдържа всички изброени по-долу елементи:

а) препратка към раздела относно политиката за правата за управление на контрола на достъпа, посочен в член 21, параграф 1, буква ж);

б) мерки за защита от атаки, аварии и заплахи и опасности, свързани със заобикалящата среда, на помещенията, центровете за данни на финансовия субект и на зони, определени от него като чувствителни, където се намират активи на ИКТ и информационни активи;

в) мерки за обезопасяване на активи на ИКТ, както в помещенията на финансовия субект, така и извън тях, като се вземат предвид резултатите от оценката на риска в областта на ИКТ, свързана със съответните активи на ИКТ;

г) мерки за осигуряване на наличността, автентичността, цялостността и поверителността на активи на ИКТ, информационни активи и физически устройства за контрол на достъпа на финансовия субект чрез подходящо поддържане;

д) мерки за запазване на наличността, автентичността, цялостността и поверителността на данните, включително:

i) политика на „чистото бюро“ във връзка с документи;

ii) политика на „изчистения екран“ за съоръжения за обработка на информация.

За целите на буква б) мерките за защитата от заплахи и опасности, свързани със заобикалящата среда, са съизмерими със значението на помещенията, центровете за данни и зоните, определени като чувствителни, както и с критичната значимост на операциите или системите на ИКТ, разположени в тях.

За целите на буква в) посочената в параграф 1 политика за физическа сигурност и сигурност на заобикалящата среда съдържа мерки за предоставяне на подходяща защита на активи на ИКТ, намиращи се извън служебните помещения.

ГЛАВА II

Политика в областта на човешките ресурси и контрол на достъпа

Член 19

Политика в областта на човешките ресурси

Финансовите субекти включват в своята политика в областта на човешките ресурси или други съответни политики всички изброени по-долу елементи, свързани със сигурността на ИКТ:

а) идентифицирането и разпределянето на всякакви специфични отговорности във връзка със сигурността на ИКТ;

б) изисквания по отношение на служителите на финансовия субект и на други трети страни доставчици на услуги в областта на ИКТ, използващи или имащи достъп до активите на ИКТ на финансовия субект относно следното:

i) да бъдат информирани за политиките, процедурите и протоколите за сигурност на ИКТ на финансовия субект и да се придържат към тях;

ii) да бъдат запознати с въведените от финансовия субект канали за докладване за откриване на необичайно поведение, включително, когато е приложимо, каналите за докладване, установени в съответствие с Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета ([11]);

iii) при прекратяване на трудовото правоотношение служителите да върнат на финансовия субект всички активи на ИКТ и материални информационни активи, с които разполагат и които принадлежат на финансовия субект.

Член 20

Управление на самоличността

1. Като част от своите права за управление на контрола на достъп финансовите субекти разработват, документират и прилагат политики и процедури за управление на самоличността, които гарантират уникалната идентификация и удостоверяване на физическите лица и системите, които имат достъп до информацията на финансовите субекти, за да се даде възможност за прехвърляне на правата на достъп на ползвателите в съответствие с член 21.

2. Посочените в параграф 1 политики и процедури за управление на самоличността съдържат всички изброени по-долу елементи:

а) без да се засяга член 21, първа алинея, буква в), на всеки служител на финансовия субект или служители на трети страни доставчици на услуги в областта на ИКТ, които имат достъп до информационните активи и активите на ИКТ на финансовия субект, се предоставя уникална самоличност, съответстваща на уникален потребителски профил;

б) процес на управление на жизнения цикъл за самоличности и профили, управляващ създаването, промяната, прегледа и актуализирането, временното деактивиране и прекратяването на всички профили.

За целите на буква а) финансовите субекти поддържат записи за всички предоставяния на самоличност. Тези записи се съхраняват след реорганизация на финансовия субект или след края на договорните отношения, без да се засягат изискванията за съхранение, определени в приложимото право на Съюза и национално право.

За целите на буква б) финансовите субекти внедряват, когато това е осъществимо и целесъобразно, автоматизирани решения за процеса на управление на самоличността през жизнения цикъл.

Член 21

Контрол на достъпа

Като част от своите права за управление на контрола на достъпа финансовите субекти разработват, документират и прилагат политика, която съдържа всички изброени по-долу елементи:

а) предоставянето на права на достъп до активи на ИКТ въз основа на принципите „необходимост да се знае“, „необходимост да се използва“ и „функциониране с най-малка привилегия“, включително при отдалечен достъп и достъп при извънредни ситуации;

б) разделянето на функциите, което има за цел да се предотврати необоснован достъп до критични данни или да се предотврати разпределянето на комбинации от права за достъп, които може да бъдат използвани за заобикаляне на механизмите за контрол;

в) разпоредба относно отчетността на ползвателите, като използването на общи и споделени потребителски профили се ограничава до възможната степен и се гарантира, че самоличността на ползвателите може да бъде установена по всяко време във връзка с извършвани в системите на ИКТ действия;

([11]) Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета от 23 октомври 2019 г. относно защитата на лицата, които подават сигнали за нарушения на правото на Съюза (ОВ L 305, 26.11.2019 г., стр. 17, ELI: https://eur-lex.europa.eu/eli/dir/2019/1937/oj).

г) разпоредба относно ограниченията на достъпа до активи на ИКТ, с която се определят механизми за контрол и инструменти за предотвратяване на непозволен достъп;

д) процедури за управление на профили за предоставяне, промяна или отнемане на права на достъп за потребителски и общи профили, в това число общи профили на администратори, включително предоставяне на всички изброени по-долу елементи:

i) разпределяне на роли и отговорности за предоставяне, преглед и отнемане на права на достъп;

ii) предоставяне на привилегирован и администраторски достъп и достъп при извънредни ситуации въз основа на принципа „необходимост да се знае“ или на *ad-hoc* основа за всички системи на ИКТ;

iii) отнемане на правата за достъп без неоправдано забавяне при прекратяване на трудовото правоотношение, или когато достъпът вече не е необходим;

iv) актуализиране на правата за достъп, когато са необходими промени, и най-малко веднъж годишно за всички системи на ИКТ, различни от системи на ИКТ, поддържащи критични или важни функции, и поне на всеки 6 месеца за системи на ИКТ, поддържащи критични или важни функции;

е) методи за удостоверяване на автентичността, включително всички изброени по-долу елементи:

i) използването на методи за удостоверяване на автентичността, съизмерими с установената в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554 класификация и с цялостния рисков профил на активите на ИКТ, и като се вземат предвид водещите практики;

ii) използването на сигурни методи за удостоверяване на автентичността в съответствие с водещите практики и техники за отдалечен достъп до мрежата на финансовия субект, за привилегирован достъп, за достъп до активи на ИКТ, поддържащи критични или важни функции или до публично достъпни активи на ИКТ;

ж) мерки за контрол на физическия достъп, включително:

i) идентифицирането и регистрирането на физически лица, които са упълномощени за достъп до помещения, центрове за данни и зони, определени от финансовия субект като чувствителни, където се намират активи на ИКТ и информационни активи;

ii) предоставянето на права на физически достъп до активи на ИКТ само на упълномощени лица в съответствие с принципите „необходимост да се знае“ и функциониране с най-малка привилегия, както и на *ad hoc* основа;

iii) наблюдението на физическия достъп до помещения, центрове за данни и зони, определени от финансовия субект като чувствителни, където се намират активи на ИКТ и информационни активи или и двете;

iv) преглед на правата на физически достъп с цел да се гарантира незабавната отмяна на ненужните права за достъп.

За целите на буква д), точка i) финансовите субекти определят срока на съхранение, като вземат предвид целите за стопанска сигурност и сигурност на информацията, причините за записване на събитието в регистрационните файлове и резултатите от оценката на риска в областта на ИКТ.

За целите на буква д), точка ii) финансовите субекти използват, когато това е възможно, специални профили за изпълнение на административни задачи на системи на ИКТ. Когато е осъществимо и подходящо, финансовите субекти внедряват автоматизирани решения за управление на привилегирования достъп.

За целите на буква ж), точка i) идентифицирането и регистрирането са съизмерими със значението на помещенията, центровете за данни и зоните, определени като чувствителни, както и с критичната значимост на операциите или системите на ИКТ, разположени в тях.

За целите на буква ж), точка iii) наблюдението е съизмеримо с установената в съответствие с член 8, параграф 1 от Регламент (ЕС) 2022/2554 класификация и с критичната значимост на зоната, до която се осъществява достъп.

ГЛАВА III

Процеси за откриване на инциденти с ИКТ и за реакция

Член 22

Политика за управление на инцидентите с ИКТ

Като част от механизмите за откриване на необичайни дейности, включително проблеми с функционирането на мрежата на ИКТ и инциденти с ИКТ, финансовите субекти разработват, документират и прилагат политика за инциденти с ИКТ, чрез която те:

а) документират процесът за управление на инциденти с ИКТ, посочен в член 17 от Регламент (ЕС) 2022/2554;

б) създават списък с подходящи контакти с вътрешни функции и външни заинтересовани страни, които са пряко ангажирани в сигурността на основаните на ИКТ операции, включително относно:

i) откриването и наблюдението на киберзаплахи;

ii) откриването на необичайни дейности;

iii) управлението на уязвими места;

в) създават, прилагат и управляват технически, организационни и оперативни механизми в подкрепа на процеса на управление на инциденти с ИКТ, включително механизми, позволяващи бързо откриване на необичайни дейности и поведения в съответствие с член 23 от настоящия регламент;

г) съхраняват всички доказателства, свързани с инциденти с ИКТ, за срок, който е не по-дълъг от необходимия за целите, за които се събират данните, съизмерим с критичната значимост на засегнатите работни функции, поддържащи процеси, активи на ИКТ и информационни активи, в съответствие с [член 15 от Делегиран регламент (ЕС) 2024/1772 на Комисията ([12]) и с всички приложими изисквания за съхранение съгласно правото на Съюза;

д) създават и прилагат механизми за анализиране на значими или повтарящи се инциденти с ИКТ и на модели при броя и възникването на инциденти с ИКТ.

За целите на буква г) финансовите субекти съхраняват посочените в същата буква доказателства по сигурен начин.

Член 23

Откриване на необичайни дейности и критерии за процесите за откриване на инциденти с ИКТ и за реакция

1. Финансовите субекти определят ясни роли и отговорности за ефективно откриване и реакция на инциденти с ИКТ и на необичайни дейности.

2. Механизмът за бързо откриване на необичайни дейности, включително проблеми с функционирането на мрежата на ИКТ и инциденти с ИКТ, както е посочено в член 10, параграф 1 от Регламент (ЕС) 2022/2554, позволява на финансовите субекти:

а) да събират, да наблюдават и да анализират всички изброени по-долу елементи:

i) вътрешни и външни фактори, включително най-малко регистрационните файлове, събрани в съответствие с член 12 от настоящия регламент, информация от работни функции и функции на ИКТ и всеки проблем, докладван от ползвателите на финансовия субект;

ii) потенциални вътрешни и външни киберзаплахи, като се вземат предвид сценариите, обичайно използвани от участниците в заплахи, и сценариите, базирани на разузнавателни сведения за заплахи;

([12]) Делегиран регламент (ЕС) 2024/1772 на Комисията от 13 март 2024 година за допълнение на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти, с които се определят подробно критериите за класифициране на инциденти с ИКТ и киберзаплахи, праговете на същественост и информацията в докладите за съществени инциденти (ОВ L, 2024/1772, 25.6.2024 г., ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) уведомление за инцидент с ИКТ от трета страна доставчик на услуги в областта на ИКТ на финансовия субект, като инцидентът е открит в системите и мрежите на ИКТ на третата страна доставчик на услуги в областта на ИКТ и може да засегне финансовия субект;

б) да идентифицират необичайни дейности и поведение и да прилагат инструменти, генериращи предупредителни сигнали за необичайни дейности и поведение, най-малкото за активи на ИКТ и информационни активи, поддържащи критични или важни функции;

в) да отдават приоритет на посочените в буква б) предупредителни сигнали, за да се даде възможност за управление на откритите инциденти с ИКТ в рамките на очакваното време за разрешаване, посочено от финансовите субекти, както през работното време, така и извън него;

г) автоматично или ръчно да записват, анализират и оценяват всяка съответна информация относно всички необичайни дейности и поведения.

За целите на буква б) посочените в същата буква инструменти съдържат инструментите, с които се предоставят автоматизирани предупредителни сигнали въз основа на предварително определени правила за идентифициране на аномалии, засягащи пълнотата и цялостността на източниците на данни или събирането на регистрационни файлове.

3. Финансовите субекти защитават всеки запис на необичайните дейности срещу подправяне и непозволен достъп при неговото съхранение, предаване и, по целесъобразност, при неговото използване.

4. Финансовите субекти регистрират цялата съответна информация за всяка открита необичайна дейност, което позволява:

а) идентифицирането на датата и часа на възникване на необичайната дейност;

б) идентифицирането на датата и часа на откриване на необичайната дейност;

в) идентифицирането на вида на необичайната дейност.

5. Финансовите субекти вземат предвид всички изброени по-долу критерии, за да задействат процесите за откриване на инциденти с ИКТ и за реакция, посочени в член 10, параграф 2 от Регламент (ЕС) 2022/2554:

а) указания, че може да е извършена злонамерена дейност в система или мрежа на ИКТ или че такава система или мрежа на ИКТ може да е била компрометирана;

б) открита загуба на данни във връзка с наличността, автентичността, цялостността и поверителността на данните;

в) открито неблагоприятно въздействие върху сделките и операциите на финансовия субект;

г) неналичност на системи и мрежи на ИКТ.

6. За целите на параграф 5 финансовите субекти вземат предвид и критичната значимост на засегнатите услуги.

ГЛАВА IV

Управление на непрекъснатостта на дейността на ИКТ

Член 24

Компоненти на политиката за непрекъснатост на дейността на ИКТ

1. Финансовите субекти включват в своята политика за непрекъснатост на дейността на ИКТ, посочена в член 11, параграф 1 от Регламент (ЕС) 2022/2554, всички посочени по-долу елементи:

а) описание на:

i) целите на политиката за непрекъснатост на дейността на ИКТ, включително взаимовръзката между ИКТ и цялостната непрекъснатост на дейността, и като се вземат предвид резултатите от анализа на въздействието върху дейността (АВД), посочен в член 11, параграф 5 от Регламент (ЕС) 2022/2554;

ii) обхватът на правилата, плановете, процедурите и механизмите за непрекъснатост на дейността на ИКТ, включително ограниченията и изключенията;

iii) времевата рамка, която трябва да се обхване от правилата, плановете, процедурите и механизмите за непрекъснатост на дейността на ИКТ;

iv) критериите за задействане и спиране на действието на плановете за непрекъснатост на дейността на ИКТ, плановете за реакция и възстановяване на ИКТ и плановете за комуникация при кризи;

б) разпоредби относно:

i) управлението и организацията на прилагането на политиката за непрекъснатост на дейността на ИКТ, включително роли, отговорности и процедури за пренасочване на управлението на инциденти, гарантиращи наличието на достатъчно ресурси;

ii) съответствието между плановете за непрекъснатост на дейността на ИКТ и цялостните планове за непрекъснатост на дейността, отнасящи се най-малко до всички изброени по-долу елементи:

1) потенциални сценарии за неизправност, включително сценариите, посочени в член 26, параграф 2 от настоящия регламент;

2) цели за възстановяването на информацията, в които се посочва, че след смущения финансовият субект е в състояние да възстанови изпълнението на своите критични или важни функции в рамките на целевото време за възстановяване на информацията и целевата точка на възстановяване;

iii) разработването на план за непрекъснатост на дейността на ИКТ за сериозни смущения в дейността като част от тези планове и отдаването на приоритет на действия за непрекъснатост на дейността на ИКТ с използване на подход, при който се отчита рискът;

iv) разработването, тестването и прегледа на планове за реакция и възстановяване на ИКТ в съответствие с членове 25 и 26 от настоящия регламент;

v) прегледа на ефективността на въведените правила, планове, процедури и механизми за непрекъснатост на дейността на ИКТ в съответствие с член 26 от настоящия регламент;

vi) привеждането в съответствие на политиката за непрекъснатост на дейността на ИКТ с:

1) с комуникационната политика, посочена в член 14, параграф 2 от Регламент (ЕС) 2022/2554;

2) действията за комуникация и действията за комуникация при криза, посочени в член 11, параграф 2, буква д) от Регламент (ЕС) 2022/2554.

2. В допълнение към посочените в параграф 1 изисквания, централните контрагенти гарантират, че в тяхната политика за непрекъснатост на дейността на ИКТ:

а) се съдържа максимален срок за възстановяване на техните критични функции, който не е по-дълъг от 2 часа;

б) се вземат предвид външни връзки и взаимозависимости в рамките на финансовите инфраструктури, включително места за търговия, преминаващи клиринг чрез централния контрагент, системи за сетълмент на ценни книжа и плащания и кредитни институции, използвани от централния контрагент или свързан централен контрагент;

в) изисквания, че са въведени правила за:

i) осигуряване на непрекъснатостта на критични или важни функции на централния контрагент въз основа на сценарии за бедствия;

ii) поддържане на допълнителен обект за обработка, който е идентичен на основния обект и е в състояние да осигури непрекъснатост на критичните или важните функции на централния контрагент;

iii) поддържане или осигуряване на незабавен достъп до допълнителен обект за обработка с цел да се позволи на служителите да осигурят непрекъснатост на услугата, ако основното място на стопанска дейност не е достъпно;

iv) разглеждане на необходимостта от изграждане на допълнителни обекти за обработка особено когато диверсификацията на рисковите профили на основния и алтернативния обект не е достатъчна, за да гарантира изцяло, че целите по отношение на непрекъснатостта на стопанската дейност на централните контрагенти ще бъдат изпълнени при всички сценарии.

За целите на буква а) централните контрагенти завършват при всички обстоятелства процедурите и плащанията в края на деня в необходимия час и ден.

За целите на буква в), точка i) посочените в същата буква правила се отнасят до наличието на необходимите човешки ресурси, максималната продължителност на прекъсване на критичните функции, както и преминаването към и възстановяването на допълнителен обект.

За целите на буква в), точка ii) допълнителният обект за обработка, посочен в същата буква, има географски рисков профил, който е различен от този на основния обект.

3. В допълнение към посочените в параграф 1 изисквания централните депозитари на ценни книжа гарантират, че в тяхната политика за непрекъснатост на дейността на ИКТ:

а) се вземат предвид всички връзки и взаимозависимости с ползватели, доставчици на критични комунални услуги и доставчици на критични услуги, различни от централни депозитари на ценни книжа и други пазарни инфраструктури;

б) се изисква правилата им за непрекъснатост на дейността на ИКТ да гарантират, че целевото време за възстановяване на техните критични или важни функции няма да бъде по-дълго от 2 часа.

4. В допълнение към посочените в параграф 1 изисквания, местата за търговия гарантират, че в тяхната политика за непрекъснатост на дейността на ИКТ се гарантира, че:

а) търговията може да бъде възобновена в рамките на или до 2 часа след водещ до смущения инцидент;

б) максималното количество данни, което може да бъде загубено от която и да е ИТ услуга на мястото на търговия след водещ до смущения инцидент, е почти нулево.

Член 25

Тестване на плановете за непрекъснатост на дейността на ИКТ

1. При тестването на плановете за непрекъснатост на дейността на ИКТ в съответствие с член 11, параграф 6 от Регламент (ЕС) 2022/2554 финансовите субекти вземат предвид анализа на въздействието върху дейността (АВД) на финансовия субект и оценката на риска в областта на ИКТ, посочена в член 3, параграф 1, буква б) от настоящия регламент.

2. Чрез тестването на своите планове за непрекъснатост на дейността на ИКТ, посочени в параграф 1, финансовите субекти преценяват дали плановете са в състояние да осигурят непрекъснатостта на критичните или важните функции на финансовия субект. Посоченото тестване:

а) се извършва въз основа на тестови сценарии, при които се симулират потенциални смущения, включително подходящ набор от тежки, но правдоподобни сценарии;

б) включва тестване на услугите в областта на ИКТ, предоставяни от трети страни доставчици на услуги в областта на ИКТ, когато е приложимо;

в) що се отнася до финансовите субекти, различни от микропредприятия, както е посочено в член 11, параграф 6, втора алинея от Регламент (ЕС) 2022/2554 — съдържа сценарии на преминаване от първична инфраструктура на ИКТ към възпроизвеждащия я капацитет, резервни копия и възпроизвеждащи системи;

г) е разработено така, че да постави под съмнение допусканията, на които се основават плановете за непрекъснатост на дейността, включително правилата за управление и планове за комуникация при кризи;

д) съдържа процедури за проверка на способността за адекватна реакция на служителите на финансовите субекти, на третите страни доставчици на услуги в областта на ИКТ, на системите на ИКТ и на услугите в областта на ИКТ по отношение на надлежно взетите предвид сценарии в съответствие с член 26, параграф 2.

За целите на буква а) финансовите субекти винаги включват в тестването сценариите, взети предвид при разработването на плановете за непрекъснатост на дейността.

За целите на буква б) финансовите субекти надлежно вземат предвид сценарии, свързани с изпадането в несъстоятелност или възникването на други проблеми при трети страни доставчици на услуги в областта на ИКТ или свързани с политическия риск в юрисдикциите на трети страни доставчици на услуги в областта на ИКТ, когато е приложимо.

За целите на буква в) при тестването се проверява дали най-малко критичните или важните функции могат да изпълняват по подходящ начин за достатъчен период от време и дали нормалното функциониране може да бъде възстановено.

3. В допълнение към посочените в параграф 2 изисквания, при тестването на своите планове за непрекъснатост на дейността на ИКТ, посочени в параграф 1, централните контрагенти включват като участници:

а) клирингови членове;

б) външни доставчици;

в) съответните институции във финансовата инфраструктура, с които централните контрагенти са установили взаимозависимости в своите политики за непрекъснатост на дейността.

4. В допълнение към посочените в параграф 2 изисквания, при тестването на своите планове за непрекъснатост на дейността на ИКТ, посочени в параграф 1, централните депозитари на ценни книжа по целесъобразност включват като участници:

а) ползватели на централните депозитари на ценни книжа;

б) доставчици на критични комунални услуги и доставчици на критични услуги;

в) други централни депозитари на ценни книжа;

г) други пазарни инфраструктури;

д) всички други институции, по отношение на които централните депозитари на ценни книжа са установили взаимозависимости в политиката си за осигуряване на непрекъснатост на дейността.

5. Финансовите субекти документират резултатите от посоченото в параграф 1 тестване. Всички установени недостатъци, произтичащи от това тестване, се анализират, отстраняват се и се докладват на ръководния орган.

Член 26

Планове за реакция и възстановяване на ИКТ

1. При разработването на плановете за реакция и възстановяване на ИКТ, посочени в член 11, параграф 3 от Регламент (ЕС) 2022/2554, финансовите субекти вземат предвид резултатите от анализа на въздействието върху дейността (АВД) на финансовия субект. С тези планове за реакция и възстановяване на ИКТ се постига следното:

а) посочват се условията, които налагат тяхното активиране или деактивиране, както и всички изключения за такова активиране или деактивиране;

б) описват се действията, които трябва да бъдат предприети, за да се гарантират наличността, цялостността, непрекъснатостта и възстановяването поне на системи на ИКТ и услуги в областта на ИКТ, поддържащи критични или важни функции на финансовия субект;

в) разработват се така, че да отговарят на целите за възстановяване на дейността на финансовите субекти;

г) документират се и се предоставят на служителите, участващи в изпълнението на плановете за реакция и възстановяване на ИКТ, и са лесно достъпни при извънредна ситуация;

д) предвиждат се както краткосрочни, така и дългосрочни възможности за възстановяване, включително частично възстановяване на системите;

е) определят се целите на плановете за реакция и възстановяване на ИКТ и условията за деклариране на успешното изпълнение на тези планове.

За целите на буква г) финансовите субекти ясно определят ролите и отговорностите.

2. В посочените в параграф 1 планове за реакция и възстановяване на ИКТ се определят съответните сценарии, включително сценарии на сериозни смущения в стопанската дейност и по-голяма вероятност от появата на смущения. В тези планове се разработват сценарии въз основа на актуална информация за заплахи и на поуки, извлечени от предишни случаи на смущения в дейността. Финансовите субекти надлежно вземат предвид всички изброени по-долу сценарии:

а) кибератаки и преминаване от първична инфраструктура на ИКТ към възпроизвеждащия я капацитет, резервни копия и възпроизвеждащи системи;

б) сценарии, при които критична или важна функция се предоставя с неприемливо ниско качество или не се предоставя изобщо, както и потенциалното въздействие на изпадането в несъстоятелност или възникването на други проблеми при съответните трети страни доставчици на услуги в областта на ИКТ;

в) частична или пълна повреда на помещенията, включително офиси и търговски помещения и центрове за данни;

г) значителна повреда на активи на ИКТ или комуникационна инфраструктура;

д) липсата на критичен брой служители или на служители, отговарящи за осигуряване на непрекъснатостта на дейността;

е) въздействието на събития, свързани с изменението на климата и разрушаване на околната среда, природни бедствия, пандемии и физически нападения, включително проникванията и терористични нападения;

ж) вътрешни атаки;

з) политическа и социална нестабилност, включително, когато е приложимо, в юрисдикцията на трета страна доставчик на услуги в областта на ИКТ и мястото, където данните се съхраняват и обработват;

и) широкоразпространени прекъсвания на електрозахранването.

3. Когато първичните мерки за възстановяване може да не са осъществими в краткосрочен план поради разходи, рискове, логистика или непредвидени обстоятелства, в посочените в параграф 1 планове за реакция и възстановяване на ИКТ се разглеждат алтернативни варианти.

4. Като част от посочените в параграф 1 планове за реакция и възстановяване на ИКТ финансовите субекти обмислят и прилагат мерки за непрекъснатост за намаляване на повредите при трети страни доставчици на услуги в областта на ИКТ, поддържащи критични и важни функции на финансовия субект.

ГЛАВА V

Доклад за прегледа на рамката за управление на риска в областта на ИКТ

Член 27

Формат и съдържание на доклада за прегледа на рамката за управление на риска в областта на ИКТ

1. Финансовите субекти представят доклада за прегледа на рамката за управление на риска в областта на ИКТ, посочена в член 6, параграф 5 от Регламент (ЕС) 2022/2554, в електронен формат с възможност за търсене.

2. Финансовите субекти включват в доклада по параграф 1 цялата изброена по-долу информация:

а) уводен раздел, в който:

i) ясно се посочва финансовият субект, за който се изготвя докладът, и се описва структурата на групата му, когато е целесъобразно;

ii) се описва контекстът на доклада по отношение на естеството, мащаба и сложността на услугите, дейностите и операциите на финансовия субект, неговата организация, идентифицираните критични функции, стратегия, големи текущи проекти или дейности, взаимоотношенията и зависимостта му от вътрешно предоставяни и от възложени по договор услуги в областта на ИКТ и системи на ИКТ или евентуалните последици от пълната загуба или сериозното влошаване на такива системи по отношение на критични или важни функции и пазарната ефективност;

iii) се прави обобщение на съществените промени в рамката за управление на риска в областта на ИКТ след представянето на предишния доклад;

iv) се предоставя обобщение на изпълнително равнище на текущия и краткосрочния рисков профил в областта на ИКТ, развитието на заплахите, оценената ефективност на неговите механизми за контрол и състоянието на сигурността на финансовия субект;

б) датата на одобрение на доклада от ръководния орган на финансовия субект;

в) описание на причината за прегледа на рамката за управление на риска в областта на ИКТ в съответствие с член 6, параграф 5 от Регламент (ЕС) 2022/2554;

г) началната и крайната дата на периода на преглед;

д) посочване на функцията, която отговаря за извършването на прегледа;

е) описание на съществените промени и подобрения в рамката за управление на риска в областта на ИКТ след предишния преглед;

ж) обобщение на констатациите от прегледа и подробен анализ и оценка на сериозността на слабостите, недостатъците и пропуските в рамката за управление на риска в областта на ИКТ през периода на прегледа;

з) описание на мерките за преодоляване на установените слабости, недостатъци и пропуски, включително всички изброени по-долу елементи:

i) обобщение на предприетите мерки за коригиране на установените слабости, недостатъци и пропуски;

ii) очаквана дата за изпълнение на мерките и дати, свързани с вътрешния контрол на изпълнението, включително информация за състоянието на напредъка на изпълнението на тези мерки към датата на изготвяне на доклада, като се предоставят разяснения, когато е приложимо, за това дали има риск от неспазване на сроковете;

iii) инструменти, които ще се използват, и идентифициране на функцията, отговаряща за изпълнението на мерките, като се уточнява дали инструментите и функциите са вътрешни или външни;

iv) описание на въздействието на предвидените в мерките промени върху бюджетните, човешките и материалните ресурси на финансовия субект, включително ресурсите, предназначени за прилагането на евентуални корективни мерки;

v) информация за процеса на информиране на компетентния орган, когато е подходящо;

vi) когато за установените слабости, недостатъци или пропуски не се прилагат корективни мерки — подробно обяснение на критериите, използвани за анализ на въздействието на тези слабости, недостатъци или пропуски, за оценка на свързания остатъчен риск в областта на ИКТ, както и на критериите, използвани за поемане на свързания остатъчен риск;

и) информация относно планираните допълнителни промени в рамката за управление на риска в областта на ИКТ;

й) заключения, произтичащи от прегледа на рамката за управление на риска в областта на ИКТ;

к) информация относно предишни прегледи, включително:

i) списък с предишни прегледи до момента;

ii) когато е приложимо, състояние на прилагането на корективните мерки, посочени в последния доклад;

iii) когато предложените корективни мерки при минали прегледи са се оказали неефективни или са породили неочаквани предизвикателства — описание на възможния начин за подобрение на тези корективни мерки или на посочените неочаквани предизвикателства;

л) източници на информация, използвани при изготвянето на доклада, включително всички изброени по-долу елементи:

i) за финансови субекти, различни от микропредприятия, както е посочено в член 6, параграф 6 от Регламент (ЕС) 2022/2554 — резултатите от вътрешните одити;

ii) резултатите от оценките на съответствието;

iii) резултатите от тестването на оперативната устойчивост на цифровите технологии и, когато е приложимо, резултатите от обстойното тестване на инструментите, системите и процесите на ИКТ чрез тестване за проникване (TLPT).

iv) външни източници.

За целите на буква в), когато прегледът е започнал вследствие на указания от страна на надзорните органи или в отговор на заключения, направени в резултат на съответни тестове на оперативната устойчивост на цифровите технологии или одитни процеси, в доклада се включва изрична препратка към тези указания или заключения, което дава възможност за установяване на причината за започване на прегледа. Когато прегледът е започнал след инцидент с ИКТ, в доклада се включва списък на всички инциденти с ИКТ, заедно с анализ на първопричините.

За целите на буква е) описанието съдържа анализ на въздействието на промените върху стратегията за оперативна устойчивост на цифровите технологии на финансовия субект, върху рамката за вътрешен контрол на ИКТ на финансовия субект и върху управлението на риска в областта на ИКТ на финансовия субект.

ДЯЛ III

ОПРОСТЕНА РАМКА ЗА УПРАВЛЕНИЕ НА РИСКА В ОБЛАСТТА НА ИКТ ЗА ФИНАНСОВИТЕ СУБЕКТИ, ПОСОЧЕНИ В ЧЛЕН 16, ПАРАГРАФ 1 ОТ РЕГЛАМЕНТ (ЕС) 2022/2554

ГЛАВА I

Опростена рамка за управление на риска в областта на ИКТ

Член 28

Управление и организация

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, разполагат с вътрешна рамка за управление и контрол, която гарантира ефективно и разумно управление на риска в областта на ИКТ с оглед постигането на високо равнище на оперативна устойчивост на цифровите технологии.

2. Посочените в параграф 1 финансови субекти гарантират, като част от своята опростена рамка за управление на риска в областта на ИКТ, че техният ръководен орган:

а) носи цялостната отговорност за гарантиране, че опростената рамка за управление на риска в областта на ИКТ позволява постигането на стопанската стратегията на финансовия субект в съответствие със склонността на този финансов субект за поемане на рискове, и гарантира, че рискът в областта на ИКТ се разглежда в този контекст;

б) определя ясни роли и отговорности за всички задачи, свързани с ИКТ;

в) залага ясни цели за сигурност на информацията и изисквания във връзка с ИКТ;

г) одобрява, надзирава и периодично прави преглед на:

i) класификацията на информационните активи на финансовия субект, посочени в член 30, параграф 1 от настоящия регламент, списъкът на идентифицираните основни рискове и анализът на въздействието върху дейността и свързаните политики;

ii) плановете за непрекъснатост на дейността на финансовия субект и мерките за реакция и възстановяване, посочени в член 16, параграф 1, буква е) от Регламент (ЕС) 2022/2554;

д) разпределя и най-малкото веднъж годишно прави преглед на необходимия бюджет за покриване на потребностите на финансовия субект във връзка с оперативната устойчивост на цифровите технологии по отношение на всички видове ресурси, включително съответните програми за повишаване на осведомеността за сигурността на ИКТ и обучението за оперативната устойчивост на цифровите технологии, както и уменията в областта на ИКТ на всички служители;

е) доуточнява и прилага политиките и мерките, включени в глави I, II и III от настоящия раздел с цел да се установи, оцени и управлява риска в областта на ИКТ, на който е изложен финансовия субект;

ж) установява и прилага процедурите, протоколите и инструментите в областта на ИКТ, които са необходими за защитата на всички информационни активи и активи на ИКТ;

з) гарантират, че служителите на финансовия субект поддържат достатъчно актуални знания и умения, за да разбират и оценяват рисковете в областта на ИКТ и тяхното въздействие върху дейността на финансовия субект, съизмеримо с управлявания риск в областта на ИКТ;

и) установява правила за докладване, включително честотата, формата и съдържанието на докладване до ръководния орган относно сигурността на информацията и оперативната устойчивост на цифровите технологии.

3. В съответствие с правото на Съюза и националното секторно право посочените в параграф 1 финансови субекти може да възлагат задачите по проверка на спазването на изискванията за управление на риска в областта на ИКТ на вътрешногрупови доставчици или трети страни доставчици на услуги в областта на ИКТ. В случай на такова възлагане на външен изпълнител финансовите субекти продължават да носят цялата отговорност за проверката на спазването на изискванията за управление на риска в областта на ИКТ.

4. Посочените в параграф 1 финансови субекти гарантират подходящото разделяне и независимостта на контролните функции и функциите за вътрешен одит.

5. Посочените в параграф 1 финансови субекти гарантират, че тяхната опростена рамка за управление на риска в областта на ИКТ подлежи на вътрешен одит от одитори в съответствие с плана за одит на финансовия субект. Одитори притежават достатъчно знания, умения и експертен опит във връзка с риска в областта на ИКТ и са независими. Честотата и насочеността на одитите на ИКТ са съизмерими с риска в областта на ИКТ на финансовия субект.

6. Въз основа на резултата от посочения в параграф 5 одит, посочените в параграф 1 финансови субекти гарантират своевременна проверка и отстраняване на критично важните проблеми, посочени в заключенията от одита на ИКТ.

Член 29

Политика и мерки за сигурност на информацията

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, разработват, документират и прилагат политика за сигурност на информацията в контекста на опростената рамка за управление на риска в областта на ИКТ. В тази политика за сигурност на информацията се определят принципите и правилата на високо равнище, необходими за защита на поверителността, цялостността, наличността и автентичността на данните и на услугите на тези финансови субекти.

2. Въз основа на своята политика за сигурност на информацията, посочена в параграф 1, посочените в същия параграф финансови субекти установяват и прилагат мерки за сигурност на ИКТ с цел да намалят излагането си на риск в областта на ИКТ, включително прилаганите от трети страни доставчици на услуги в областта на ИКТ мерки за намаляване на риска.

Мерките за сигурност на ИКТ включват всички мерки, посочени в членове 30—38.

Член 30

Класификация на информационните активи и на активите на ИКТ

1. Като част от опростената рамка за управление на риска в областта на ИКТ, посочена в член 16, параграф 1, буква а) от Регламент (ЕС) 2022/2554, посочените в параграф 1 от същия член финансови субекти идентифицират, класифицират и документират всички критични или важни функции, информационните активи и активите на ИКТ, които ги поддържат, и техните взаимозависимости. Финансовите субекти правят преглед на тази идентификация и класификация, ако това е необходимо.

2. Посочените в параграф 1 финансови субекти идентифицират всички критични или важни функции, поддържани от трети страни доставчици на услуги в областта на ИКТ.

Член 31

Управление на риска в областта на ИКТ

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, включват в своята опростена рамка за управление на риска в областта на ИКТ всичко, изброено по-долу:

а) определянето на нивата на толерантност към риска в областта на ИКТ в съответствие със склонността на финансовия субект за поемане на риск;

б) идентификацията и оценката на рисковете в областта на ИКТ, на които е изложен финансовия субект;

в) спецификацията на стратегиите за намаляване на риска най-малкото за рисковете в областта на ИКТ, които не попадат в рамките на нивата на толерантност към риска за финансовия субект;

г) наблюдението на ефективността на стратегиите за намаляване на риска, посочени в буква в);

д) идентифицирането и оценката на всякакви рискове в областта на ИКТ и сигурността на информацията, произтичащи от всяка съществена промяна в системата на ИКТ или услугите, процесите или процедурите в областта на ИКТ, както и от резултатите от тестовете за сигурност на ИКТ и след всеки съществен инцидент с ИКТ.

2. Посочените в параграф 1 финансови субекти извършват и документират периодично оценката на риска в областта на ИКТ, съизмерима с рисковия профил в областта на ИКТ на финансовите субекти.

3. Посочените в параграф 1 финансови субекти непрекъснато наблюдават заплахите и уязвимите места, които са от значение за техните критични или важни функции, както и за информационните активи и активите на ИКТ, и редовно правят преглед на рисковите сценарии, оказващи въздействие върху тези критични или важни функции.

4. Посочените в параграф 1 финансови субекти определят прагове за отправяне на предупреждение и критерии за задействане и инициране на процеси за реакция при инциденти с ИКТ.

Член 32

Физическа сигурност и сигурност на заобикалящата среда

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, идентифицират и прилагат мерки за физическа сигурност, разработени въз основа на обстановката по отношение на заплахите и в съответствие с посочената в член 30, параграф 1 от настоящия регламент класификация, с цялостния рисков профил на активите на ИКТ и с достъпните информационни активи.

2. С посочените в параграф 1 мерки помещенията на финансовите субекти и, когато е приложимо, центровете за данни на финансовите субекти, където се намират активите на ИКТ и информационните активи, се защитават от непозволен достъп, атаки и аварии, както и от заплахи и опасности, свързани със заобикалящата среда.

3. Защитата от заплахи и опасности, свързани със заобикалящата среда, е съизмерима със значението на съответните помещения и, когато е приложимо, на центровете за данни, както и с критичната значимост на операциите или системите на ИКТ, разположени в тях.

ГЛАВА II

Допълнителни елементи на системи, протоколи и инструменти за свеждане до минимум на въздействието на риска в областта на ИКТ

Член 33

Контрол на достъпа

Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, разработват, документират и прилагат процедури за контрол на логическия и физическия достъп и налагат, наблюдават и периодично правят преглед на тези процедури. Тези процедури съдържат следните елементи за контрол на логическия и физическия достъп:

а) правата на достъп до информационни активи, активи на ИКТ и на поддържаните от тях функции, както и до критични за дейността на финансовия субект места, се управляват въз основа на принципите „необходимост да се знае“, „необходимост да се използва“ и „функциониране с най-малка привилегия“, включително по отношение на отдалечен достъп и достъп при извънредни ситуации;

б) отчетност на ползвателите, която гарантира, че самоличността на ползвателите може да бъде установена във връзка с извършваните в системите на ИКТ действия;

в) процедури за управление на профили за предоставяне, промяна или отнемане на права на достъп за потребителски и общи профили, в това число общи профили на администратори;

г) методи за удостоверяване на автентичността, които са съизмерими с посочената в член 30, параграф 1 класификация и с цялостния рисков профил на активите на ИКТ, и които се основават на водещите практики;

д) правата на достъп се преразглеждат периодично и се отнемат, когато вече не са необходими.

За целите на буква в) финансовият субект предоставя привилегирован достъп, достъп при извънредни ситуации и администраторски достъп въз основа на принципа „необходимост да се знае“ или на *ad-hoc* основа за всички системи на ИКТ и той се регистрира в съответствие с член 34, първа алинея, буква е).

За целите на буква г) финансовите субекти използват сигурни методи за удостоверяване на автентичността, които се основават на водещи практики за отдалечен достъп до мрежата на финансовите субекти, за привилегирован достъп и за достъп до активи на ИКТ, поддържащи критични или важни функции, които са публично достъпни.

Член 34

Сигурност на основаните на ИКТ операции

Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, като част от своите системи, протоколи и инструменти и във връзка с всички активи на ИКТ:

а) наблюдават и управляват жизнения цикъл на всички активи на ИКТ;

б) наблюдават дали активите на ИКТ са поддържани от трети страни доставчици на услуги в областта на ИКТ на финансови субекти, когато е приложимо;

в) идентифицират изискванията във връзка с капацитета на своите активи на ИКТ, както и мерки за поддържане и подобряване на наличността и ефикасността на системите на ИКТ, и предотвратяват недостига на капацитет, преди такъв да настъпи;

г) извършват автоматизирано сканиране за уязвими места, както и оценки на активите на ИКТ, съизмерими с тяхната класификация, посочена в член 30, параграф 1, и с цялостния рисков профил на активите на ИКТ, и внедряват корекции за отстраняване на установените уязвими места;

д) управляват рисковете, свързани с остарели, неподдържани или наследени активи на ИКТ;

е) регистрират събития, свързани с контрол на логическия и физическия достъп, основани на ИКТ операции, включително дейности по системен и мрежови пренос и управление на промените в областта на ИКТ;

ж) идентифицират и прилагат мерки за наблюдение и анализ на информация за необичайни дейности и поведение във връзка с критични или важни основани на ИКТ операции;

з) прилагат мерки за наблюдение на подходяща и актуална информация за киберзаплахи;

и) прилагат мерки за идентифициране на възможни изтичания на информация, злонамерен код и други заплахи за сигурността и публично известни уязвими места в софтуера и хардуера и проверяват за съответните нови актуализации във връзка със сигурността.

За целите на буква е) финансовите субекти привеждат в съответствие нивото на детайлност на регистрационните файлове с целта и употребата на своя актив на ИКТ, за който се създават тези регистрационни файлове.

Член 35

Сигурност на данните, системата и мрежата

Като част от своите системи, протоколи и инструменти, посочените в член 16, параграф 1 от Регламент (ЕС) 2022/2554 финансови субекти разработват и прилагат защитни механизми, които гарантират сигурността на мрежите срещу проникванията и злоупотреба с данни и които запазват наличността, автентичността, цялостността и поверителността на данните. По-специално като вземат предвид класификацията, посочена в член 30, параграф 1 от настоящия регламент, финансовите субекти установяват всичко, изброено по-долу:

а) идентифицирането и прилагането на мерки за защита на данните при тяхното използване, предаване и съхранение;

б) идентифицирането и прилагането на мерки за сигурност относно използването на софтуер, носители за съхранение на данни, системи и крайни устройства, с които се предават и съхраняват данни на финансовия субект;

в) идентифицирането и прилагането на мерки за предотвратяване и откриване на непозволени връзки към мрежата на финансовия субект и за защита на мрежовия пренос между вътрешните мрежи на финансовия субект и интернет и други външни връзки;

г) идентифицирането и прилагането на мерки, които осигуряват наличността, автентичността, цялостността и поверителността на данните по време на предаванията в мрежата;

д) процес за сигурно заличаване на данни относно помещения или съхранявани външно, които финансовият субект вече не трябва да събира или съхранява;

е) процес за сигурно унищожаване или извеждане от експлоатация на съдържащи поверителна информация устройства за съхранение на данни, намиращи се в помещения, или устройства за съхранение на данни, които се съхраняват външно;

ж) идентифицирането и прилагането на мерки с цел да се гарантира, че работата от разстояние и използването на частни крайни устройства не оказват неблагоприятно въздействие върху способността на финансовия субект да извършва критичните си дейности по подходящ, навременен и сигурен начин.

Член 36

Тестване на сигурността на ИКТ

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, създават и изпълняват план за тестване на сигурността на ИКТ, за да потвърдят ефективността на своите мерки за сигурност на ИКТ, разработени в съответствие с членове 33, 34 и 35 и членове 37 и 38 от настоящия регламент. Финансовите субекти гарантират, че в този план се вземат предвид заплахите и уязвимите места, идентифицирани като част от посочената в член 31 от настоящия регламент опростена рамка за управление на риска в областта на ИКТ.

2. Посочените в параграф 1 финансови субекти преразглеждат, оценяват и тестват мерките за сигурност на ИКТ, като вземат предвид цялостния рисков профил на активите на ИКТ на финансовия субект.

3. Посочените в параграф 1 финансови субекти наблюдават и оценяват резултатите от тестовете на сигурността и актуализират без неоправдано забавяне своите мерки за сигурност в случай на системи на ИКТ, поддържащи критични или важни функции.

Член 37

Придобиване, разработване и поддържане на системи на ИКТ

Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, разработват и прилагат, когато е целесъобразно, процедура, с която се урежда придобиването, разработването и поддържането на системи на ИКТ, като следват подход, при който се отчита рискът. С тази процедура се постига следното:

а) гарантира се, че преди придобиването или разработването на системи на ИКТ, функционалните и нефункционалните изисквания, включително изискванията за сигурност на информацията, са ясно посочени и одобрени от съответната работна функция;

б) гарантират се тестването и одобрението на системите на ИКТ преди първото им използване и преди въвеждането на промени в продукционната среда;

в) определят се мерки за намаляване на риска от непреднамерена промяна или преднамерено манипулиране на системи на ИКТ по време на разработването и прилагането в продукционната среда.

Член 38

Управление на проекти в областта на ИКТ и на промените в ИКТ

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, разработват, документират и прилагат процедура за управление на проекти в областта на ИКТ и определят ролите и отговорностите за нейното изпълнение. Тази процедура обхваща всички етапи на проектите в областта на ИКТ — от началото им до тяхното приключване.

2. Посочените в параграф 1 финансови субекти разработват, документират и прилагат процедура за управление на промените в ИКТ с цел да се гарантират контролираните записване, тестване, оценяване, одобряване, прилагане и проверяване на всички промени в системите на ИКТ, заедно с подходящи защитни механизми за запазване на оперативната устойчивост на цифровите технологии на финансовия субект.

ГЛАВА III

Управление на непрекъснатостта на дейността на ИКТ

Член 39

Компоненти на плана за непрекъснатост на дейността на ИКТ

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, разработват своите планове за непрекъснатост на дейността в областта на ИКТ, като вземат предвид резултатите от анализа на експозициите си към сериозни смущения в дейността и потенциалното им въздействие, както и сценарии, при които техните активи на ИКТ, поддържащи критични или важни функции, могат да бъдат изложени на тях, включително сценарий за кибератака.

2. С посочените в параграф 1 планове за непрекъснатост на дейността на ИКТ се постига следното:

а) те се одобряват от ръководния орган на финансовия субект;

б) те се документират и са лесно достъпни в случай на извънредна ситуация или криза;

в) с тях се разпределят достатъчно ресурси за изпълнението им;

г) идентифицират се планирани равнища на възстановяване и времеви рамки за възстановяване и възобновяване на функции и ключови вътрешни и външни зависимости, включително трети страни доставчици на услуги в областта на ИКТ;

д) идентифицират се условията, при които може да се предизвика задействането на плановете за непрекъснатост на дейността на ИКТ, и действията, които трябва да бъдат предприети, за да се гарантират наличността, непрекъснатостта и възстановяването на активите на ИКТ на финансовите субекти, поддържащи критични или важни функции;

е) идентифицират се мерките за възстановяване на критични или важни работни функции, поддържащи процеси, информационни активи и техните взаимозависимости, с цел да се избегнат неблагоприятните последици за функционирането на финансовите субекти;

ж) идентифицират се процедури и мерки, в които се определят обхватът на данните, за които се съхраняват резервни копия, както и минималната честота на това копиране, в зависимост от критичната значимост на функцията, използваща тези данни;

з) обмислят се алтернативни варианти, при които възстановяването може да не е осъществимо в краткосрочен план поради разходи, рискове, логистика или непредвидени обстоятелства;

и) доуточняват се вътрешните и външните планове за комуникация, включително плановете за пренасочване на управлението;

й) плановете се актуализират в съответствие с извлечените поуки от инциденти, тестове, идентифицирани нови рискове и заплахи, променени цели за възстановяване на информацията, съществени промени в организацията на финансовия субект и в активите на ИКТ, поддържащи критични или работни функции.

За целите на буква е) мерките, посочени в същата буква, предвиждат намаляване на проблемите при трети страни критични доставчици на услуги.

Член 40

Тестване на плановете за непрекъснатост на дейността

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, тестват своите планове за непрекъснатост на дейността, посочени в член 39 от настоящия регламент, включително сценариите, посочени в същия член, поне веднъж годишно по отношение на процедурите за съхраняване на резервни копия и възстановяване или при всяка съществена промяна на плана за непрекъснатост на дейността.

2. Тестването на посочените в параграф 1 планове за непрекъснатост на дейността показва, че посочените в същия параграф финансови субекти са в състояние да поддържат жизнеспособността на своята стопанска дейност, докато бъдат възстановени критичните операции, и чрез него се идентифицират всички недостатъци в тези планове.

3. Посочените в параграф 1 финансови субекти документират резултатите от тестването на плановете за непрекъснатост на дейността и всички недостатъци, установени в резултат на това тестване, се анализират, разглеждат и докладват на ръководния орган.

ГЛАВА IV

Доклад за прегледа на опростената рамка за управление на риска в областта на ИКТ

Член 41

Формат и съдържание на доклада за прегледа на опростената рамка за управление на риска в областта на ИКТ

1. Финансовите субекти, посочени в член 16, параграф 1 от Регламент (ЕС) 2022/2554, представят доклада за прегледа на рамката за управление на риска в областта на ИКТ, посочена в параграф 2 от посочения член, в електронен формат с възможност за търсене.

2. В посочения в параграф 1 доклад се съдържа цялата описана по-долу информация:

а) уводен раздел, в който се предоставят:

i) описание на контекста на доклада по отношение на естеството, мащаба и сложността на услугите, дейностите и операциите на финансовия субект, неговата организация, идентифицираните критични функции, стратегия, големи текущи проекти или дейности и взаимоотношенията и зависимостта му от собствени и възложени на подизпълнител услуги в областта на ИКТ и системи на ИКТ или евентуалните последици от пълната загуба или сериозното влошаване на състоянието на такива системи по отношение на критични или важни функции и на пазарната ефективност;

ii) обобщение на изпълнително равнище на установения текущ и краткосрочен риск в областта на ИКТ, обстановката по отношение на заплахите, оценената ефективност на неговите механизми за контрол и състоянието на сигурността на финансовия субект;

iii) информация за областта, по отношение на която се докладва;

iv) обобщение на съществените промени в рамката за управление на риска в областта на ИКТ след представянето на предишния доклад;

v) обобщение и описание на въздействието на съществените промени върху опростената рамка за управление на риска в областта на ИКТ след представянето на предишния доклад;

б) когато е приложимо, датата на одобрение на доклада от ръководния орган на финансовия субект;

в) описание на причините за прегледа, включително:

i) когато прегледът е започнал вследствие на указания от страна на надзорните органи — доказателства за тези указания;

ii) когато прегледът е започнал след възникването на инцидент с ИКТ — списък на всички инциденти с ИКТ, заедно с анализ на първопричините;

г) началната и крайната дата на периода на преглед;

д) лицето, отговорно за прегледа;

е) обобщение на констатациите и самооценка на сериозността на установените слабости, недостатъци и пропуски в рамката за управление на риска в областта на ИКТ през периода на прегледа, включително техен подробен анализ;

ж) установени коригиращи мерки за преодоляване на слабостите, недостатъците и пропуските в опростената рамка за управление на риска в областта на ИКТ и очакваната дата за прилагане на тези мерки, включително последващите действия по отношение на слабостите, недостатъците и пропуските, идентифицирани в предишни доклади, когато тези слабости, недостатъци и пропуските все още не са отстранени;

з) общи заключения относно прегледа на опростената рамка за управление на риска в областта на ИКТ, включително всички по-нататъшни планирани промени.

ДЯЛ IV

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 42

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 13 март 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN