

## Задължения на финансовите субекти, съгласно Регламент (ЕС) 2022/2554 (DORA)

**Регламент (ЕС) 2022/2554** относно оперативната устойчивост на цифровите технологии във финансовия сектор (“DORA”, или „Регламент“) цели да укрепи устойчивостта на цифровите технологии във финансовия сектор, като наложи хармонизирани изисквания за управление на риска, докладване, тестване и управление на отношенията с трети страни. DORA влезе в сила на 16 януари 2023 г. и се прилага от 17 януари 2025 г.

Регламентът е с пряко приложение като на национално ниво следва да бъдат определени и правомощията на компетентните органи за надзор и налагане на имуществени санкции. В България правомощията на надзорните органи се очаква да бъдат уредени с минимални изменения в секторното законодателство, регулиращо дейността на финансовите субекти. Необходимите изменения са предмет на [проекта](#) на Закон за пазарите на криптоактиви, внесен за разглеждане от Народно събрание.

### Кои са задължените субекти и основните им задължения, съгласно DORA?

DORA се прилага спрямо широка група финансови субекти, като Регламентът оказва съдействие и върху третите страни доставчици на услуги в областта на ИКТ. В България се очаква надзорният орган за спазване на Регламента да бъде компетентният орган по отношение на основната дейност на съответния финансов субект, а именно:

#### Българска народна банка („БНБ“)

- Кредитни институции, които подлежат на надзор от БНБ
- Платежни институции
- Институции за електронни пари
- Доставчици на услуги по предоставяне на информация за сметка
- Администратори на критични бенчмаркове за лихвени проценти

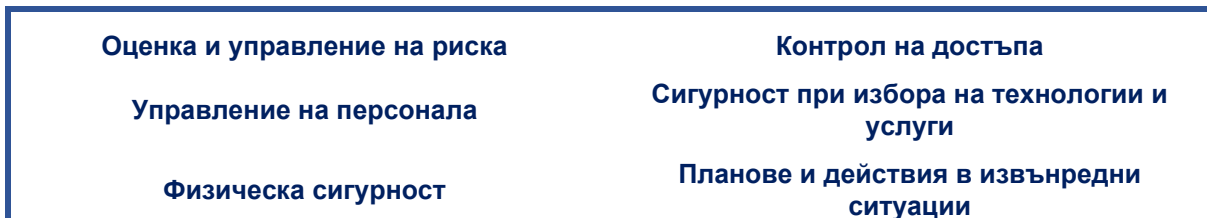
#### Комисия за финансов надзор („КФН“)

- Инвестиционни посредници с лиценз по ЗПФИ
- Доставчици на услуги за криптоактиви
- Издателите на токени, обезпечени с активи
- Централни депозитари на ценни книжа
- Централните контрагенти по ЗПФИ
- Места за търговия с лиценз по ЗПФИ
- Одобрени механизми за докладване и одобрени механизми за публикуване по ЗПФИ
- Лицата, управляващи алтернативни инвестиционни фондове (над определена стойност на активите)
- Управляващите дружества по ЗДКИСДПКИ
- Застрахователни и презастрахователни предприятия
- Застрахователни и презастрахователни посредници и посредници, предлагащи застрахователни продукти като допълнителна дейност (големи предприятия)
- Пенсионноосигурителните дружества, управляващи фонд за допълнително доброволно пенсионно осигуряване по професионални схеми (15+ лица)
- Администратори на критични бенчмаркове по ЗПФИ;
- Доставчици на услуги за колективно финансиране по ЗППЦК



### Управление на риска

Финансовите субекти трябва да установяват и внедрят рамка за управление на ИКТ риска, която гарантира идентифицирането, оценяването, контрола и смекчаването на заплахите:



Изискванията относно управлението на ИКТ рисковете са определени с DORA и [Делегиран регламент \(ЕС\) 2024/1774](#), с цел осигуряване на оперативна устойчивост на цифровите технологии и защита на данните. Рамката за управление на ИКТ рискове включва документирани политики и процедури за осигуряване на непрекъснатост на дейността, съхранение на резервни копия на данни и възстановяване на информацията.

Минимум веднъж годишно или след инцидент следва да се извършва преглед на политиките и процедурите, включително на тези за управление на инциденти с ИКТ и тяхното въздействие върху функционирането на организацията. Осъществяват се периодични тестове на плановете за непрекъснатост на дейността и възстановяване на ИКТ системи.

**!** Отговорността за управлението на ИКТ рисковете се носи от ръководството на финансовите субекти, което трябва да въведе политики за осигуряване на сигурността на данните и да определи роли и отговорности на служителите, свързани с ИКТ.

Следва да се осигури оперативен капацитет и обучение на персонала, да бъде създадена контролна функция за наблюдение на рисковете, одиторска функция за провеждане на вътрешни одити на ИКТ системите и процесите, функция за наблюдение на договорите с трети страни доставчици на ИКТ услуги, управление на кризи и връзки с обществеността.

**Облекчен режим:** Микропредприятията прилагат опростена рамка за управление на риска (общи насоки и правила за защита на данните). Малките предприятия прилагат опростена рамка за управление на ИКТ риска, която подлежи на периодичен преглед и актуализация при инцидент.



### Докладване на инциденти

Финансовите субекти трябва да разработят процес за управление на ИКТ инциденти, включващ откриване, управление и докладване на инцидентите, както и тяхното класифициране спрямо въздействието им. Критериите за класификация на инцидентите обхващат фактори като броя на засегнатите клиенти, продължителността на инцидента и икономическите му последици. Съществени инциденти трябва да бъдат докладвани на КФН/БНБ в рамките на 24 часа, а допълнителни доклади се подават, когато се актуализират обстоятелствата или се променя въздействието. Финансовите субекти могат да уведомяват за киберзаплахи доброволно.

Финансовите субекти трябва да класифицират инцидентите и заплахите по определени критерии и да документират всичко с цел проследяване и превенция. Възникнал инцидент се счита за съществен инцидент, когато е засегнал критични услуги и са достигнати праговете на същественост, съгласно [Делегиран регламент \(ЕС\) 2024/1772](#). С [делегиран регламент](#) на Европейската комисия ще бъдат определени сроковете за подаване на първоначален, междинен и окончателен доклад, както и тяхното съдържание:



Първоначалният доклад трябва да съдържа обща информация, докато междинният и окончателният доклад включват подробности за развитието на инцидента и предприетите мерки. За целите на стандартизирането на процесите са въведени регулаторни технически стандарти, които гарантират ефективно и унифицирано управление на инцидентите в сектора. Прилагането на тези стандарти осигурява ефективното управление на инциденти с ИКТ и спазване на нормативните изисквания.



### Тестване на оперативната устойчивост

Финансовите субекти, с изключение на микропредприятията, са задължени да въведат програма за тестване на оперативната устойчивост, която е неразделна част от управлението на риска в областта на ИКТ. Основната цел на тази програма е идентифициране на слабостите и пропуските в устойчивостта на ИКТ, както и въвеждане на пропорционални корективни мерки за тяхното отстраняване. Подходът при изпълнението на програмата е базиран на риска и включва анализ на специфичните рискове, на които финансовият субект може да бъде изложен, оценка на критичността на информационните активи и предоставяните услуги, както и други релевантни фактори. Програмата обхваща различни методи и инструменти, включително анализ на уязвимости, мрежова сигурност, физическа сигурност и тестване на функционирането. Тестването се провежда поне веднъж годишно за всички критични системи и приложения и се извършва от вътрешни или външни лица с гарантирана независимост и липса на конфликт на интереси.

**Обстойното тестване чрез проникване (TLP)** се извършва **най-малко веднъж на три години** и обхваща критични ИКТ функции по преценка на компетентния орган. Финансовите субекти подават обобщение на констатациите и корективните мерки след тестването. TLP може да включва трети страни, които трябва да осигурят спазването на стандартите за сигурност. В случай, че се използват вътрешни лица за провеждане на тестовете, тези лица подлежат на одобрение от компетентния орган и трябва да отговарят на изискванията за компетентност.

Микропредприятията прилагат ограничен набор от тестове, включващи анализ на уязвимости, мрежова сигурност и функционалност.



### Управление на риска, пораждан от трети страни

Финансовите субекти са длъжни да управляват риска в областта на ИКТ, произтичащ от трети страни, като интегрират този риск в рамката за управление на риска в областта на ИКТ. Подходът е пропорционален и отчита специфичните зависимости/рискове, произтичащи от договорите с доставчици на ИКТ услуги, и се отчитат мащаба, сложността и потенциалното въздействие върху предоставяните финансови услуги.

Финансовите субекти приемат и редовно актуализират стратегията за управление на риска в областта на ИКТ, породен от трети страни, включваща политики за използването на критични и важни ИКТ услуги. Те извършват периодичен преглед на тези рискове и договори. Създава се регистър на всички договори за ИКТ услуги с трети страни, като договорите за критични и важни функции е отделена. Финансовите субекти ежегодно информират компетентните органи за нови договори, като уведомяват и за намеренията си да сключват договори за критични функции или за трансформацията на дадена функция в критична. При поискване предоставят пълния регистър и друга информация, необходима за надзора.

Договори за критични или важни функции се сключват с доставчици, които отговарят на високи стандарти за сигурност. Преди сключването им, финансовите субекти извършват оценка на рисковете, потенциалните конфликти на интереси и съответствието с регулаторните изисквания. Договорите включват гаранции, че прекратяването им няма да повлияе на непрекъснатостта и качеството на услугите, и определят условия за прекратяване при нарушения или други обстоятелства. Съдържанието на договорите следва да се съобразено с DORA.

За критични или важни функции се разработват изходни планове, които се актуализират и тестват редовно. Те включват рисковете при прекратяване на договорите и осигуряват непрекъснатост на дейността. Одитите на доставчици се извършват съобразно риска и в съответствие с признати одитни стандарти, като се гарантира, че вътрешните и външни одитори притежават необходимата експертиза за одити и оценки по технически сложни договори.



### Сътрудничество и обмен на информация

Финансовите субекти могат да обменят информация и разузнавателни сведения за киберзаплахи и уязвимости с цел повишаване на оперативната устойчивост на ИКТ. Това включва споделяне на показатели за сигурност, тактики, техники, процедури, предупреждения за киберсигурност и инструменти за конфигуриране. Обменът на информация се осъществява в рамките на доверени общности от финансови субекти, които сключват споразумения за сътрудничество. Участници могат да бъдат и трети страни доставчици на ИКТ услуги и публични органи. Споразуменията трябва да гарантират поверителността на информацията, защита на личните данни, търговската тайна и да бъдат в съответствие с приложимото законодателство, включително конкурентното право. Финансовите субекти са задължени да уведомяват компетентните органи за участието или прекратяването на участие в такива споразумения.



### Какво да очакваме и следващи стъпки

Регламентът се прилага независимо от забавянето на влизане в сила на измененията в секторните закони в България и към настоящия момент задължените субекти следва да са предприели всички необходими мерки, съгласно DORA и регламентите за изпълнение. С приемането и влизането в сила на Закона за пазарите на криптоактиви ще се определят изрично органите с правомощия за надзор за спазване на DORA.

Към спазването на DORA трябва да се подходи комплексно, като ИТ екипът, правният отдел и екипите по осигуряване на съответствието на задължените субекти работят съвместно. Особено внимание трябва да се обърне на привиждането на договорните споразумения в съответствие с изискванията на DORA, като се насърчава яснотата в споразуменията за определено ниво на обслужване и задълженията на доставчиците. Доколкото третите страни доставчици на услуги в областта на ИКТ също са засегнати от Регламента, е необходимо да се въведат мерки и спрямо тях като например процедури за комуникация при инциденти, процедури за одит/контрол, обучение.