ЕВРОПЕЙСКИ РЕГЛАМЕНТ ЗА ДИГИТАЛНА ОПЕРАТИВНА УСТОЙЧИВОСТ (DORA)

КФН | КОМИСИЯ ЗА ФИНАНСОВ НАДЗОР

Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година 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 (DORA) влезе в сила на 16 януари 2023 г. и ще се прилага от 17 януари 2025 г. DORA има за цел да засили информационната сигурност на финансови субекти като банки, застрахователни компании и инвестиционни посредници и да гарантира, че финансовият сектор в Европа е в състояние да остане устойчив в случай на сериозни смущения в оперативната работа. DORA въвежда хармонизиране на правилата, свързани с оперативната устойчивост на финансовия сектор, приложими към 20 различни вида финансови субекти и към трети страни доставчици на услуги в областта на информационните и комуникационните технологии (ИКТ).

Тъй като този сектор е все по-зависим от технологиите и от технологичните компании за предоставяне на финансови услуги, финансовите субекти стават все по-уязвими на кибератаки и други инциденти, свързани с киберсигурността. Когато не се управляват правилно, ИКТ рисковете могат да доведат до прекъсване на предоставянето на финансовите услуги, а това от своя страна може да окаже въздействие върху други компании, сектори и дори върху останалата част от икономиката, което подчертава значението на цифровата оперативна устойчивост за финансовия сектор.

DORA изисква всички участници във финансовия сектор в Европейския съюз да поддържат информационен регистър за всички договорни споразумения за услуги в областта на ИКТ, сключени с трети страни доставчици на такива услуги. Регистърът трябва да бъде изчерпателен и да обхваща всички договорни споразумения на индивидуална, подконсолидирана и консолидирана основа, съгласно чл. 28, параграф 3 от DORA.

DORA ще се прилага за следните поднадзорни на Комисията за финансов надзор лица:

- инвестиционни посредници;
- доставчици на услуги за криптоактиви, лицензирани съгласно Регламент (ЕС) 2023/1114 на Европейския парламент и на Съвета от 31 май 2023 година относно

пазарите на криптоактиви и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на директиви 2013/36/ЕС и (ЕС) 2019/1937 (MiCAR), и емитенти на токени, обезпечени с активи;

- централни депозитари на ценни книжа;
- централни контрагенти;
- места на търговия;
- лица, управляващи алтернативни инвестиционни фондове;
- управляващи дружества;
- одобрените механизми за докладване и одобрените механизми за публикуване по чл. 1, ал. 3 от Закона за пазарите на финансови инструменти;
- застрахователни и презастрахователни предприятия;
- застрахователни посредници, презастрахователни посредници и посредници, предлагащи застрахователни продукти като допълнителна дейност;
- институции за професионално пенсионно осигуряване;
- администратори на критични бенчмаркове;
- доставчици на услуги за колективно финансиране.

От така посочените поднадзорни лица, за които ще се прилагат изискванията на DORA, изрично се изключват:

- лицата, управляващи алтернативни инвестиционни фондове, посочени в чл. 214 от Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране;
- застрахователи без право на достъп до единния пазар съгласно чл. 16 от Кодекса за застраховане;
- институциите за професионално пенсионно осигуряване, които управляват пенсионни схеми, в които участват общо не повече от 15 членове;
- лицата, посочени в чл. 5 от Закон за пазарите на финансови инструменти;
- застрахователните посредници, презастрахователните посредници и посредниците, предлагащи застрахователни продукти като допълнителна дейност, които са микро-, малки или средни предприятия.

При приемането в националното законодателство на мерки по прилагане на MiCAR се очаква поднадзорни лица на Комисията за финансов надзор да бъдат и доставчиците на услуги за криптоактиви и емитентите на токени, обезпечени с активи, които ще прилагат изискванията на DORA.

Изложение на основните разпоредби на DORA:

I. Общи разпоредби

В глава I от DORA са изброени финансовите субекти, за които се прилага DORA, както и финансовите субекти, които са изключени от обхвата му. Дават се легални дефиниции за целите на същия регламент и се закрепва изрично спазването на принципа на пропорционалност. Включват се и третите страни доставчици на услуги в областта на ИКТ сред субектите, за които ще се прилага DORA.

II. Управление на риска в областта на ИКТ

Член 5 от DORA регламентира отговорността на ръководния орган на финансовия субект за определяне, одобряване, упражняване надзор върху изпълнението на всички действия във връзка с рамката за управление на риска в областта на ИКТ, като са посочени конкретни действия и мерки, които финансовият субект е необходимо да предприеме за постигане на тази цел.

Установява се задължението финансовите субекти да разполагат с вътрешна рамка за управление и контрол, която гарантира ефективно и разумно управление на риска в областта на ИКТ в съответствие с чл. 6, параграф 4 от DORA, с оглед постигането на високо равнище на оперативна устойчивост на цифровите технологии.

Съгласно чл. 6 от DORA финансовите субекти разполагат с надеждна, широкообхватна и добре документирана рамка за управление на риска в областта на ИКТ, като част от цялостната им система за управление на риска, която позволява да се справят бързо, ефикасно и широкообхватно с риска в областта на ИКТ и да поддържат високо равнище на оперативна устойчивост на цифровите технологии. Рамката включва най-малко стратегии, политики, процедури,

протоколи за ИКТ и инструменти, основани на ИКТ, които са необходими за надлежната и подходяща защита на всички информационни активи и активи на ИКТ, включително компютърен софтуер, хардуер, сървъри, както и за защитата на всички относими физически компоненти и инфраструктури, като например помещения, центрове за данни и зони. При поискване те се предоставят на компетентния орган. Рамката се документира и се преразглежда поне веднъж годишно - или периодично за микропредприятията - както и при съществени инциденти с ИКТ. Същата подлежи на редовен вътрешен одит от одитори в съответствие с плана за одит на финансовите субекти. Въз основа на заключенията от вътрешния одитен преглед финансовите субекти въвеждат официален процес на последващи действия, включително правила за своевременна проверка и отстраняване на критично важните проблеми, посочени в заключенията от одита на ИКТ. В рамката се включва стратегия за оперативна устойчивост на цифровите технологии. Финансовите субекти, без микропредприятията, възлагат на дадена контролна функция отговорността за управление и надзор на риска в областта на ИКТ и осигуряват подходящо ниво на независимост на тази контролна функция. На компетентния орган се представя доклад за прегледа на рамката за управление на риска в областта на ИКТ при поискване от негова страна. Финансовите субекти могат да определят цялостна стратегия за прибягване до множество доставчици на ИКТ, на равнище група или субект, в която се посочват ключовите зависимости от третите страни доставчици на услуги в областта на ИКТ. Финансовите субекти могат да възлагат задачите по проверка на спазването на изискванията за управление на риска в областта на ИКТ на вътрешногрупови или външни предприятия.

Съгласно чл. 7 от DORA, с цел да се справят с риска в областта на ИКТ и да го управляват, финансовите субекти използват и поддържат в актуален вид системи и протоколи на ИКТ и основани на ИКТ инструменти, които изпълняват определени изисквания: съобразени с мащаба на операциите; надеждни; с достатъчен капацитет за точното обработване на данните; технологично устойчиви.

Съгласно чл. 8 от DORA, като част от рамката за управление на риска в областта на ИКТ, финансовите субекти идентифицират, класифицират и документират по подходящ начин:

- всички поддържани от ИКТ работни функции, роли и отговорности;
- информационните активи и активите на ИКТ, поддържащи тези функции, както и техните роли и зависимости във връзка с рисковете в областта на ИКТ;
- всички процеси, които зависят от трети страни доставчици на услуги в областта на ИКТ, и идентифицират взаимовръзките.

Когато е необходимо, но поне веднъж годишно, финансовите субекти правят преглед на адекватността на тази класификация и на съответната документация. Финансовите субекти поддържат съответните списъци и ги актуализират периодично и всеки път, когато настъпи съществена промяна.

Съгласно чл. 9 от DORA, с цел адекватна защита на системите на ИКТ и с оглед на организирането на мерките за реакция, финансовите субекти са задължени да проектират, възлагат и прилагат политики, процедури, протоколи и инструменти за сигурност на ИКТ, които имат за цел да осигурят устойчивостта, непрекъснатостта и наличността на системите на ИКТ. ИКТ решенията и процесите следва да отговарят на следните изисквания:

- да гарантират сигурността на средствата за предаване на данни;
- да свеждат до минимум риска от увреждане или загуба на данните, непозволен

достъп и технически недостатъци, които могат да попречат на стопанската дейност;

- да предотвратяват липсата на наличност, нарушаването на автентичността, цялостността и поверителността и загубата на данни.

Съгласно чл. 10 от DORA финансовите субекти са задължени да разполагат с механизми за бързо откриване на необичайните дейности — включително проблеми с функционирането на мрежата на ИКТ и инциденти с ИКТ, както и за идентифицирането на потенциалните точки, чиято повреда може да доведе до общ отказ на системите. Механизмите за откриване позволяват множество нива на контрол, определят прагове за отправяне на предупреждение и критерии за

задействане и иницииране на процеси за реакция при инциденти с ИКТ, включително автоматични механизми за предупреждаване на съответните служители, отговорни за реагирането при инциденти с ИКТ. Наред с това, доставчиците на услуги за докладване на данни разполагат и със системи, които могат да извършват надеждна проверка за пълнота на отчетите на сделките, да откриват пропуски и явни грешки и да изискват повторното предоставяне на посочените отчети.

Съгласно чл. 11 от DORA, като част от рамката за управление на риска в областта на ИКТ (РУР), финансовите субекти въвеждат широкообхватна политика за непрекъснатост на дейността на ИКТ (чрез документирани правила, планове, процедури и механизми), която може да бъде приета като специална отделна политика, явяваща се неразделна част от цялостната политика на финансовите субекти за непрекъснатост на дейността. Плановете за реакция и възстановяване на ИКТ, при всички финансови субекти освен микропредприятията, подлежат на независими вътрешни одитни прегледи. Финансовите субекти е необходимо да въведат, поддържат и периодично тестват подходящи планове за непрекъснатост на дейността на ИКТ, по-специално по отношение на критичните или важните функции, възложени с договори на трети страни доставчици на услуги в областта на ИКТ. Финансовите субекти следва да пазят леснодостъпни записи на действията преди и по време на събитията, нарушили обичайното функциониране. Централните депозитари на ценни книжа предоставят на компетентния орган копия от резултатите от тестовете за непрекъснатост на дейността на ИКТ или от подобни упражнения. Финансовите субекти, без микропредприятията, докладват на компетентния орган по тяхно искане предварителна оценка на агрегираните годишни разходи и загуби, причинени от съществени инциденти с ИКТ.

Член 12 от DORA налага изискването финансовите субекти да разработят и документират, като част от РУР в областта на ИКТ, политики и процедури за съхраняване на резервни копия на данните и процедури и методи за възстановяване на информацията.

Други задължения относно оперативния капацитет и персонал на финансовите субекти според чл. 13 от DORA са: събирането на информация за уязвимите места, киберзаплахите, инцидентите с ИКТ, като се прави преглед на възникналите инциденти с ИКТ, добавя се натрупания опит от проведените тестове на оперативната устойчивост на цифровите технологии от реални инциденти с ИКТ. Най-малко веднъж годишно висшите служители, работещи с ИКТ, представят на ръководния орган констатации и правят препоръки. Финансовите субекти разработват и включват като задължителни модули в схемите си за обучение на персонала програми за повишаване на осведомеността за сигурността на ИКТ и обучения по оперативна устойчивост на цифровите технологии.

Съгласно чл. 14 от DORA финансовите субекти е необходимо да разполагат с планове за комуникация при криза, които предвиждат отговорно уведомяване на собствения персонал и на клиентите и контрагентите, а по необходимост — и на обществеността, поне за съществените инциденти с ИКТ или уязвими места.

III. Инциденти с ИКТ — управление, класифициране и докладване

Член 17 от DORA налага изисквания за финансовите субекти да определят, въвеждат и прилагат процес за управление на инцидентите с ИКТ, чрез който да се откриват, управляват и докладват инцидентите с ИКТ. Целта е да се документират всички инциденти с ИКТ и значителни киберзаплахи. Чрез процеса за управление на инцидентите с ИКТ се постига следното:

- определят се показатели за ранно предупреждение;
- въвеждат се процедури за установяване, проследяване, регистриране, категоризиране и класифициране на инцидентите с ИКТ според техния приоритет и тежест и според критичността на засегнатите услуги;
- определят се ролите и задачите, които трябва да се задействат при отделните видове и сценарии на инциденти с ИКТ;
- изготвят се планове за комуникация с персонала, външните заинтересовани страни и медиите, клиенти и контрагенти;
- гарантира се, че поне съществените инциденти с ИКТ се докладват на съответното висше ръководство;

- въвеждат се процедури за реакция при инцидент с ИКТ, за да се ограничат последиците и своевременно да се възобнови обичайното и сигурно функциониране на услугите.

Съгласно чл. 19 от DORA финансовият субект докладва на съответния компетентен орган за съществените инциденти с ИКТ чрез изготвяне на първоначално уведомление, неокончателен доклад и окончателен доклад по образци. Компетентният орган може да докладва на Европейския орган за ценни книжа и пазари (ЕОЦКП), Европейския банков орган (ЕБО), Европейския орган за застраховане и професионално пенсионно осигуряване (ЕОЗППО) и други европейски органи. Финансовите субекти могат да докладват и доброволно по тяхна преценка. Образците на документите за докладване се хармонизират на основата на издаден регулаторен технически стандарт. В чл. 21 от DORA е установен начин за централизирано докладване на съществени инциденти с ИКТ. Централизираното докладване ще може да се осъществява с въвеждането на единен портал на ЕС за докладване на съществени инциденти с ИКТ, чрез който пряко да се получават съответните доклади и автоматично да се уведомяват националните компетентни органи, или би могъл само да централизира съответните доклади, препращани от националните компетентни органи, изпълнявайки координационни функции.

IV. Тестване на оперативната устойчивост на цифровите технологии

Член 24 от DORA поставя изискване на финансовите субекти, без микропредприятията, за въвеждане, поддържане и актуализиране на стабилна и всеобхватна програма за тестване на оперативната устойчивост на цифровите технологии, като неразделна част от РУР. Програмата за тестване на оперативната устойчивост на цифровите технологии съдържа набор от оценки, тестове, методи, практики и инструменти и отчита специфичните за финансовите субекти рискове. Тестването се извършва от независими лица - вътрешни или външни (поне веднъж годишно за критично важните функции). Въвеждат се процедури и политики за подреждане по важност, класифициране и

отстраняване на всички констатирани при тестването проблеми, както и вътрешни методики за валидиране, така че всички установени слабости, недостатъци или пропуски да бъдат изцяло преодолени.

Примерни тестови инструменти са описани в чл. 25 от DORA: оценки и сканиране на уязвимите места, анализ на приложенията с отворен код, оценки на сигурността на мрежата, анализ на пропуските, преглед на физическата сигурност, анкети и сканиране на програмните продукти, преглед на първичния код, когато такъв е осъществим, тестване на различни сценарии, тестване на съвместимостта, тестване на функционирането, тестване по цялата верига и тестване за проникване.

Финансовите субекти (без микропредприятия и други с малък обхват и значимост) провеждат най-малко веднъж на 3 години обстойно тестване посредством тестване за проникване. Този период може да се промени от компетентния орган при промяна в рисковия профил на финансовите субекти. Всяко тестване за проникване включва няколко или всички критични или важни функции на финансовия субект, като се тестват оперативните производствени системи, поддържащи тези функции. Когато тестването за проникване обхваща трети страни доставчици на услуги в областта на ИКТ, то може да се делегира на външно лице и да се извърши съвкупно, когато услугата се предлага на повече финансови субекти. В чл. 27 от DORA са посочени изискванията за вътрешни и външни акредитирани лица за провеждане на тестове за проникване. Когато тестването приключи и бъдат приети докладите и плановете за корективни мерки, финансовите субекти предоставят на единен публичен орган обобщение на констатациите, плановете за корективни мерки и документацията, която доказва, че тестването за проникване е било проведено в съответствие с изискванията. Органите издават на финансовите субекти удостоверение, с което потвърждават, че тестването е извършено в съответствие с изискванията. Компетентните органи определят финансовите субекти, от които се изисква да извършват тестване за проникване, въз основа на критерии за тяхната значимост и критичност, рисков профил и дейност.

V. Управление на риска в областта на ИКТ, пораждан от трети страни

Финансовите субекти се задължават да управляват риска в областта на ИКТ, пораждан от трети страни, като неразделна част от компонента „риск в областта на ИКТ" на РУР в областта на ИКТ. Приемат и редовно преразглеждат стратегия за риска в областта на ИКТ, пораждан от трети страни, като вземат предвид, когато е приложимо, стратегията за прибягване до множество доставчици. Стратегията за риска в областта на ИКТ, пораждан от трети страни, включва политика за използването на услуги в областта на ИКТ, поддържащи критичните или важните функции, предоставяни от трети страни доставчици на такива услуги. Необходимо е финансовите субекти да поддържат и актуализират на индивидуална, подконсолидирана и консолидирана основа информационен регистър за всички договорни споразумения за услуги в областта на ИКТ, сключени с трети страни доставчици на такива услуги. Поне веднъж годишно финансовите субекти е необходимо да осведомяват компетентния орган за броя нови споразумения за услуги в областта на ИКТ, за категориите трети страни доставчици на такива услуги, за вида на договорните споразумения и за предоставяните услуги и функции в областта на ИКТ.

Финансовите субекти могат да сключват договорни споразумения само с трети страни доставчици на услуги в областта на ИКТ, които удовлетворяват подходящи стандарти за сигурност на информацията и гарантират, че договорните споразумения могат да бъдат прекратени при определени обстоятелства без това да прекъсне стопанската дейност, да ограничи спазването на регулаторните изисквания или да бъде в ущърб на непрекъснатостта и качеството на предоставяните на клиентите услуги.

Съгласно чл. 29 от DORA при идентифицирането и оценяването на риска от концентрация на ИКТ, финансовите субекти е необходимо да преценят дали предвижданото договорно споразумение би довело при сключването си до липса на заменяемост или до множество договорни споразумения с трети страни. Финансовите субекти преценяват дали и как потенциално дългите или сложни вериги от подизпълнители могат да засегнат способността им да следят изцяло

договорно възложените функции, както и способността на компетентния орган да упражнява върху тях ефективен надзор в това отношение.

Член 30 от DORA определя задължителните елементи на съдържанието на договорните споразумения с трети страни, както и към договорните споразумения, поддържащи критични или важни функции.

Съгласно чл. 31 от DORA европейските надзорни органи (ЕНО) определят критичните за финансовите субекти трети страни доставчици на услуги в областта на ИКТ въз основа на определени критерии за значимост/критичност/мащаб/заменяемост и определят за водещ надзорник на всяка от третите страни критични доставчици на услуги в областта на ИКТ отговорния ЕНО в съответствие с регламенти (ЕС) №1093/2010, (ЕС) №1094/2010 или (ЕС) №1095/2010 за финансовите субекти, които съвместно притежават най-големия дял от общите активи спрямо стойността на общите активи на всички финансови субекти, използващи услугите на съответната трета страна критичен доставчик на услуги в областта на ИКТ, в съответствие със сбора на отделните счетоводни баланси на тези финансови субекти. Когато третата страна доставчик на услуги в областта на ИКТ е част от група, критериите се вземат под внимание по отношение на услугите в областта на ИКТ, предоставяни от групата като цяло. Надзорните задължения спрямо критични трети страни доставчици са подробно разписани в чл. 31 и следващите.

Чрез съвместния си комитет ЕНО съставят, публикуват и годишно актуализират списък на третите страни критични за Съюза доставчици на услуги в областта на ИКТ. Компетентните органи ежегодно и в обобщен вид предават на създадения надзорен форум информацията за броя на споразуменията, сключени от доставчици трети страни. Третите страни доставчици на услуги в областта на ИКТ, които не са задължително определени като критични, могат да поискат да бъдат определени за такива. Финансовите субекти ползват услугите на трета страна доставчик на услуги в областта на ИКТ, която е определена за критичен доставчик само ако въпросната трета страна е регистрирала дъщерно предприятие в Съюза в рамките на 12 месеца след определянето. Третата страна критичен доставчик на услуги в областта на ИКТ, уведомява водещия надзорник за

всякакви промени в структурата на управление на дъщерното предприятие, регистрирано в Съюза.

Съвместният комитет създава надзорен форум като свой подкомитет, който да подпомага неговата работа и тази на водещия надзорник по въпросите на риска в областта на ИКТ, пораждан от трета страна за финансовите сектори. Надзорният форум подготвя проектите за съвместни позиции и проектите за общи актове на съвместния комитет в тази сфера. Надзорният форум представя на съвместния комитет общи референтни показатели за третите страни критични доставчици на услуги в областта на ИКТ, които показатели съвместният комитет да приеме, като съвместни позиции на ЕНО. Надзорният форум може, когато е целесъобразно, да потърси съвет от независими експерти.

В състава на надзорния форум влизат:

- председателите на ЕНО;
- по един представител на високо равнище от настоящия персонал на съответния компетентен орган, посочен в чл. 46 от DORA, от всяка държава членка. Законопроектът за пазарите на криптоактиви предвижда управителният съвет на Българската народна банка да приема решение за определяне на представител на високо равнище от персонала на Българската народна банка за участие в надзорния форум по чл. 32, параграф 4, буква "б" от DORA;
- изпълнителните директори на всеки ЕНО, както и по един представител от Комисията, от Европейския съвет за системен риск, от Европейската централна банка и от Агенцията на Европейския съюз за киберсигурност, като наблюдатели;
- когато е целесъобразно, по един допълнителен представител на компетентен орган, посочен в чл. 46 от DORA, от всяка държава членка като наблюдател; Законопроектът за пазарите на криптоактиви предвижда Комисията за финансов надзор да определя неин представител за участие в надзорния форум по чл. 32, параграф 4, буква "г" от DORA;
- ако е приложимо, по един представител на компетентните органи, определени или установени в съответствие с DORA, отговарящи за надзора на съществен или важен субект, попадащ в обхвата на посочената директива, който

е определен за трета страна критичен доставчик на услуги в областта на ИКТ, като наблюдател.

В чл. 33 - 41 от DORA са регламентирани задачите на водещия надзорник, оперативната координация между водещите надзорници, правомощията на водещия надзорник в Съюза и извън него, подаването на искане за информация от водещия надзорник, извършването на общи разследвания и проверки, осъществяването на текущ надзор. Компетентните органи имат задължение да информират съответните финансови субекти за рисковете, установени в препоръките след проведените проверки, а финансовите субекти е необходимо да се съобразят с тях. В противен случай, след съвместна комуникация с националния компетентен орган, може да се премине към прилагане на изходните стратегии и преходните планове.

В съответствие с Делегиран регламент (ЕС) 2024/1505 на Комисията от 22 февруари 2024 година за допълнение на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета чрез определяне на размера на таксите за надзор, които водещият надзорник трябва да начислява на критичните трети доставчици на услуги в областта на ИКТ, и на начина за плащането им, който влиза в сила на 19.06.2024 г., водещият надзорник определя на третите страни критични доставчици на услуги в областта на ИКТ, такси, които изцяло покриват необходимите разходи на водещия надзорник във връзка с изпълнението на надзорните задачи.

ЕБО, ЕОЦКП и ЕОЗППО могат да сключват административни споразумения с регулаторните и надзорните органи на трети държави за насърчаване на международното сътрудничество във връзка с риска в областта на ИКТ, пораждан от трети страни, в различните финансови сектори, по специално чрез разработването на най-добри практики за преглед на практиките и контролните механизми за управление на риска в областта на ИКТ, мерки за ограничаване на риска и реакция при инциденти.

VI. Споразумения за обмен на информация и разузнавателни сведения за киберзаплахи

Финансовите субекти могат да обменят помежду си информация и разузнавателни сведения за киберзаплахи, включително показатели за застрашена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността и инструменти за конфигуриране, доколкото този обмен на информация и разузнавателни сведения е с цел да подобри оперативната устойчивост на цифровите технологии при финансовите субекти. Също така финансовите субекти задължително уведомяват компетентните органи за участието си в споразуменията за обмен на информация при потвърждаване на членството им или при ефективното му прекратяване.

VII. Компетентни органи

Установени са правилата за сътрудничество със структурите и органите, създадени с Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2), както и за симулации, комуникация и сътрудничество сред финансовите сектори чрез създаване механизми за споделяне на ефективните практики и разработване на симулационни сценарии за управление на кризи и действие при извънредни ситуации в резултат на кибератаки, с цел да се изграждане на комуникационни канали.

В чл. 50 - 54 от DORA са заложени правила за определяне на административни санкции и коригиращи мерки, упражняване на правомощия за налагането им и публикуването на решенията за налагане на административни санкции.

В DORA са установени и изисквания за опазване на професионалната тайна и за защитата на личните данни.