СТАНОВИЩЕ НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА

от 11 април 2022 година

относно предложение за директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Въведение и правно основание

На 16 декември 2020 г. Европейската комисия прие предложение за директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 ([1]) (наричано по-долу „предложената директива“). На 3 декември 2021 г. Съветът на Европейския съюз постигна съгласие по общия си подход по предложената директива ([2]). Европейската централна банка (ЕЦБ) е компетентна да даде становище на основание член 127, параграф 4, втора алинея и член 127, параграф 5 от Договора за функционирането на Европейския съюз, тъй като предложената директива съдържа разпоредби, попадащи в областите на компетентност на ЕЦБ, по-специално насърчаването на нормалното функциониране на платежните системи, приноса за гладкото провеждане на следваните от компетентните органи политики, свързани със стабилността на системата на финансовите пазари, и задачите на ЕЦБ по отношение на пруденциалния надзор над кредитните институции съгласно член 127, параграф 2, четвърто тире и член 127, параграфи 5 и 6 от Договора. Управителният съвет прие настоящото становище съгласно член 17.5, изречение първо от Процедурния правилник на Европейската централна банка.

Общи забележки

ЕЦБ твърдо подкрепя целите на предложената директива за повишаване на нивото на киберустойчивост във всички съответни сектори, намаляване на разликите в рамките на вътрешния пазар и подобряване на равнището на ситуационна осведоменост и колективната способност за подготовка и реакция чрез осигуряване на ефективно сътрудничество в Съюза.

ЕЦБ признава, че е важно да се поддържат силни връзки между предложената директива и финансовия сектор, който трябва да остане част от екосистемата на мрежите и информационните системи (МИС), за да се насърчават последователната оценка на рисковете, свързани с информационните и комуникационните технологии (ИКТ) в целия Съюз, и ефективният междусекторен обмен на информация и сътрудничеството при справянето с киберзаплахи. За тази цел следва да бъде възможно компетентните органи съгласно предложения регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор ([3]) (наричан по-нататък „Регламентът DORA“) да участват в обсъжданията на стратегическите политики и в техническата работа на групата за сътрудничество за МИС, както и да обменят информация и да си сътрудничат допълнително с единните звена за контакт и националните екипи за реагиране при инциденти с компютърната сигурност, посочени в предложената директива ([4]).

1. Приложно поле на предложената директива

1.1 ЕЦБ разбира, че по отношение на субектите във финансовия сектор Регламентът DORA ще се счита за специфично за сектора законодателство, с което се въвеждат изисквания за управлението на риска, свързан с киберсигурността, и за уведомяването за инциденти, които са поне равностойни по ефект на предвидените в предложената директива ([5]). Поради това разпоредбите на предложената директива, които се отнасят до управлението на риска, свързан с киберсигурността, задълженията за уведомяване, обмена на информация, надзора и правоприлагането, няма да се прилагат за финансовите субекти, които попадат в приложното поле на Регламента DORA ([6]). Както е пояснено в

([1]) COM(2020) 823 final.
([2]) Достъпен на уебсайта на Съвета на Европейския съюз www.consilium.europa.eu
([3]) COM (2020) 595 final.
([4]) Виж параграф 1.5 от Становище CON/2021/20 на Европейската централна банка от 4 юни 2021 г. относно предложение за регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор (ОВ C 343, 26.8.2021 г., стр. 1). Всички становища на ЕЦБ се публикуват на EUR-Lex. Член 17, параграф 5 и член 42 от Регламента DORA; член 11 от предложената директива.
([5]) Член 2, параграф 6 от предложената директива.
([6]) Съображение 13 и член 2, параграф 6 от предложената директива.

съображенията на предложената директива, вместо нейните разпоредби следва да се прилагат разпоредбите на Регламента DORA във връзка с мерките за управление на риска при ИКТ, управлението на инцидентите при ИКТ и уведомяването за тях, изпитването на оперативната устойчивост на цифровите технологии, споразуменията за обмен на информация и риска при ИКТ, пораждан от участието на трети страна ([7]).

1.2 ЕЦБ отбелязва също така, че в общия си подход по предложената директива Съветът предлага изменение, с което „субектите, които извършват дейност в областта на съдебната власт, парламентите или централните банки“ ([8]) се изключват от прилагането на предложената директива. ЕЦБ разбира, че предложеното изменение ще разшири всички основни задачи и компетентности на Европейската система на централните банки (ЕСЦБ), посочени в член 127, параграф 2 от Договора и в член 3.1 от Устава на Европейската система на централните банки и на Европейската централна банка (наричан по-долу „Уставът на ЕСЦБ“), като например насърчаването на нормалното функциониране на платежните системи. В това отношение се счита, че притежаваните и управлявани от Евросистемата инфраструктури на финансовите пазари като TARGET2 и TARGET2-Securities попадат в приложното поле на предложеното от Съвета изключване на централните банки от прилагането на предложената директива.

2. **Надзорни правомощия на ЕСЦБ и Евросистемата**

2.1 Наред с основната цел на ЕСЦБ да поддържа ценова стабилност и в съответствие с член 127, параграф 2 от Договора една от основните задачи, които се изпълняват чрез ЕСЦБ, е да се насърчава нормалното функциониране на платежните системи ([9]). При изпълнението на тази основна задача ЕЦБ и националните централни банки могат да осигурят улеснения, а ЕЦБ да приеме регламенти, гарантиращи ефикасни и стабилни клирингови и платежни системи в рамките на Съюза и с други страни ([10]). В изпълнение на надзорната си роля ЕЦБ прие Регламент (ЕС) № 795/2014 на Европейската централна банка (ЕЦБ/2014/28) ([11]) (наричан по-долу „Регламентът за СВПС“), с който принципите на КПСС-МОКЦК за инфраструктурите на финансовите пазари ([12]) се превръщат в пряко приложимо право. В Регламента за СВПС се определят изискванията както за платежните системи за големи плащания, така и за платежните системи за малки плащания от системно значение, независимо дали са публична или частна собственост. Изискванията съгласно Регламента за СВПС вече включват управлението на операционния риск и създаването на рамка за киберустойчивост ([13]).

2.2 В допълнение към системно важните платежни системи надзорът на Евросистемата обхваща платежните системи, които не са системно важни, електронните платежни инструменти, схеми и споразумения, както и други инфраструктури и доставчици на критични услуги, както е посочено в рамката на надзорната политика на Евросистемата ([14]). Платежните системи и другите споразумения, подлежащи на надзор от Евросистемата, не са изрично включени в приложното поле на предложената директива ([15]). В същото време, като се има предвид, че предложената директива е инструмент за минимална хармонизация ([16]), приетото от държавите членки законодателство за транспонирането ѝ би могло в крайна сметка да се припокрива с надзорната компетентност на Евросистемата. За да се избегне това, правомощията на ЕСЦБ съгласно Договора и Устава на ЕСЦБ, както и правомощията на Евросистемата съгласно Регламента за СВПС и като цяло съгласно рамката на надзорната политика на Евросистемата трябва да бъдат изрично посочени в съображенията на предложената директива.

([7]) Съображение 13 от предложената директива

([8]) Член 2, параграф 3а, първа алинея, буква б) от общия подход на Съвета по предложената директива.

([9]) Член 127, параграф 2 от ДФЕС, чието съдържание е отразено в член 3.1 от Устава на ЕСЦБ.

([10]) Член 22 от Устава на ЕСЦБ.

([11]) Регламент (ЕС) № 795/2014 на Европейската централна банка от 3 юли 2014 г. относно надзорните изисквания за системно важните платежни системи (ЕЦБ/2014/28) (ОВ L 217, 23.7.2014 г., стр. 16).

([12]) Виж Комитет за платежни и сетълмент системи (КПСС) и Технически комитет на Международната организация на комисиите за ценни книжа (МОКЦК), „Принципи за инфраструктурите на финансовите пазари“, април 2012 г., достъпни на уебсайта на Банката за международни разплащания: www.bis.org. Отговорност Г гласи, че „от всички членове на КПСС и МОКЦК се очаква да прилагат принципите към съответните инфраструктури на финансовите пазари в своята юрисдикция във възможно най-голяма степен, доколкото това е позволено от правната рамка в тяхната юрисдикция“.

([13]) Член 15 от Регламент (ЕС) № 795/2014 (ЕЦБ/2014/28).

([14]) Рамка на надзорната политика на Евросистемата, преработена версия (юли 2016 г.), достъпна на уебсайта на ЕЦБ www.ecb.europa.eu

([15]) Член 2 от предложената директива и приложения I и II към предложената директива.

([16]) Член 3 от предложената директива.

3. **иск при ИКТ, пораждан от участието на трета страна, управление на мащабни инциденти и кризи, обмен на информация и национална стратегия за киберсигурност**

3.1 *Управление на риска при ИКТ, пораждан от трета страна*

3.1.1 Предложената директива оправомощава компетентните органи, когато упражняват правомощията си за правоприлагане по отношение на съществените субекти, да издават обвързващи указания или разпореждане, изискващи от тези субекти да поправят установените пропуски или нарушенията на задълженията съгласно предложената директива ([17]). В същото време „водещият надзорник“, определен съгласно Регламента DORA, може да отправя препоръки към възловите доставчици–трети страни на услуги в областта на ИКТ да управляват потенциалните системни рискове, произтичащи от практиките на възлагане на дейности на външни изпълнители и концентрацията на доставчици–трети страни на услуги в областта на ИКТ ([18]).

3.1.2 Като се има предвид, че съгласно предложената директива съществен субект може да бъде определен и за възлов доставчик–трета страна на услуги в областта на ИКТ съгласно Регламента DORA, ЕЦБ отново подчертава ([19]), че трябва да се избягва издаването на противоречащи си препоръки и обвързващи указания. Във връзка с това ЕЦБ приветства общия подход на Съвета по предложената директива. Съгласно този подход компетентните органи трябва да информират създадения съгласно Регламента DORA „надзорен форум“, когато упражняват надзорните и правоприлагащите си правомощия по отношение на съществен субект, определен като възлов доставчик–трета страна на услуги в областта на ИКТ съгласно Регламента DORA ([20]).

3.2 *Управление на мащабни инциденти и кризи*

3.2.1 Съгласно предложената директива ([21]) държавите членки трябва да определят един или повече компетентни органи, които да отговарят за управлението на мащабни инциденти и кризи. Както се пояснява в съображенията на предложената директива, мащабен инцидент следва да означава инцидент със значително въздействие върху поне две държави членки или инцидент, смущението от който надхвърля капацитета за отговор на една държава членка. Широкомащабните инциденти могат да се превърнат в същински кризи, нарушавайки правилното функциониране на вътрешния пазар ([22]).

3.2.2 Въпреки че компетентните органи, определени съгласно Регламента DORA, продължават да носят отговорност за управлението на инциденти с киберсигурността, засягащи финансовите субекти, сътрудничеството със структурите и органите, създадени съгласно предложената директива, ще бъде от решаващо значение за осигуряването на координиран отговор в целия Съюз. За тази цел ЕЦБ би приветствала участието на компетентните органи, определени съгласно Регламента DORA, включително ЕЦБ, в Европейската мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe) ([23]), когато мащабните киберинциденти и кризи засягат финансовия сектор.

3.3 *Обмен на информация*

3.3.1 Както е посочено по-горе, ЕЦБ твърдо подкрепя сътрудничеството между компетентните органи, определени съгласно Регламента DORA, и структурите и органите, създадени съгласно предложената директива. По-специално обменът на информация между органите може да даде възможност за междусекторен обмен на знания и опит, да допринесе за предотвратяването и ефективното управление на кибератаки и да насърчи последователната оценка на рисковете, свързани с ИКТ, в целия Съюз. Въпреки това ЕЦБ подчертава, че обменът на информация трябва да се осъществява там, където има ясно установени механизми за класификация и обмен на информация, съчетани с подходящи гаранции за защита на поверителността ([24]). ЕЦБ приветства общия подход на Съвета по предложената директива, в

([17]) Член 29, параграф 4, подточка б) от предложената директива.
([18]) Член 31 от Регламента DORA.
([19]) Вж. параграф 1,2 от Становище CON/2021/20.
([20]) Член 29, параграф 10 от общия подход на Съвета по предложената директива.
([21]) Член 7, параграф 1 от предложената директива.
([22]) Съображение 27 от предложената директива
([23]) Член 14 от предложената директива.
([24]) Вж. параграф 1.5 от Становище CON/2021/20.

който се предлагат редовен обмен на съответната информация между органите ([25]), установяване на договорености за сътрудничество, определящи механизъм за обмен на информация ([26]), и автоматично и пряко препращане на уведомленията за инциденти ([27]). В това отношение следва да се гарантира, че поверителната информация съгласно разпоредбите от Регламента DORA за служебната тайна ([28]) или съгласно съответното специално секторно законодателство ([29]) може да се обменя с компетентните органи, посочени в предложената директива, само когато този обмен им е необходим, за да прилагат разпоредбите ѝ ([30]).

3.4 *Национална стратегия за киберсигурност*

3.4.1 Съгласно предложената директива държавите членки трябва да приемат национална стратегия за киберсигурност, в която са определени стратегическите цели и подходящи мерки на политиката, както и подходящи регулаторни мерки за постигане и поддържане на високо ниво на киберсигурност ([31]). Както е пояснено в съображенията на предложената директива, държавите членки следва да продължат да включват финансовия сектор в съответните си стратегии за киберсигурност ([32]). Например, като част от националните си стратегии за киберсигурност, държавите членки следва да приемат политики, насочени към киберсигурността във веригата на доставки на ИКТ продукти и услуги, използвани от субектите за предоставяне на техните услуги. Доколкото засягат финансовия сектор, националните стратегии за киберсигурност трябва да бъдат в съответствие с регулаторната рамка, произтичаща от Регламента DORA. Във връзка с това ЕЦБ счита, че са необходими допълнителни разяснения, за да се гарантира, че националните стратегии за киберсигурност съответстват на специалното секторно законодателство.

Когато ЕЦБ отправя препоръки за изменения на предложената директива, конкретните предложения с обяснителен текст към нея се представят в технически работен документ. Техническият работен документ е достъпен на английски език на EUR-Lex.

Съставено във Франкфурт на Майн на 11 април 2022 година.

Председател на ЕЦБ
Christine LAGARDE

([25]) Член 11, параграф 5 от общия подход на Съвета по предложената директива.
([26]) Съображение 23а от общия подход на Съвета по предложената директива.
([27]) Съображение 13 от общия подход на Съвета по предложената директива.
([28]) Член 49 от Регламента DORA.
([29]) Членове 53–62 от Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО (ОВ L 176, 27.6.2013 г., стр. 338).
([30]) Виж член 2, параграф 5 и член 11, параграф 4 от предложената директива.
([31]) Член 5 от предложената директива.
([32]) Съображение 13 от предложената директива.