2025/301

20.2.2025 г.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2025/301 НА КОМИСИЯТА

от 23 октомври 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 съдържанието и сроковете за първоначалното уведомление и неокончателния и окончателния доклад за съществени инциденти с ИКТ, както и съдържанието на уведомлението на доброволен принцип за значителни киберзаплахи

(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 20, третата алинея от него,

като има предвид, че:

(1) За да се гарантира хармонизирането и опростяването на изискванията за уведомяване и докладване на съществени инциденти с ИКТ, посочени в член 19, параграф 4 от Регламент (ЕС) 2022/2554, за всички видове финансови субекти следва да се прилага съгласуван подход за сроковете за докладване на съществени инциденти с ИКТ. Поради тези причини за сроковете следва също така, във възможно най-голяма степен, да се прилага съгласуван подход с изискванията, посочени в Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([2]), както и те да бъдат поне равностойни като резултат на тези изисквания.

(2) За да се избегне налагането на прекомерна тежест за докладване на финансовите субекти в момент, когато работят по отстраняването на инцидент с ИКТ, съдържанието на първоначалното уведомление следва да бъде ограничено до най-съществената информация. За да могат да предприемат подходящи надзорни действия, компетентните органи трябва да получават информация за съществени инциденти с ИКТ възможно най-бързо, след като финансовият субект е класифицирал даден инцидент с ИКТ като съществен. Следователно срокът за подаване на първоначалното уведомление, посочен в член 19, параграф 4, буква а) от Регламент (ЕС) 2022/2554, следва да бъде възможно най-кратък след класифицирането на инцидент с ИКТ като съществен, като същевременно се допуска гъвкавост, по-специално за моделите на стопанска дейност, при които предоставянето на услуги не е особено ограничено във времето, в случай че финансовите субекти се нуждаят от повече време за справяне с инцидента с ИКТ, след като са узнали за него.

(3) След като са получили първоначалното уведомление, компетентните органи следва да получат по-подробна информация за инцидента с ИКТ в неокончателния доклад, а цялата необходима информация — в окончателния доклад. Информацията в тези доклади следва да даде възможност на компетентните органи да направят допълнителна оценка на инцидента с ИКТ и да преценят надзорните действия, които биха желали да предприемат.

(4) Следователно със сроковете за докладване, посочени в член 20, първа алинея, буква а), точка ii) от Регламент (ЕС) 2022/2554, следва да се постигне баланс между необходимостта компетентните органи да получат информацията бързо и необходимостта да се предостави на финансовите субекти достатъчно време за получаване на пълна и точна информация.

(5) Като се вземат предвид критериите, посочени в член 20, първа алинея, буква а) от Регламент (ЕС) 2022/2554, сроковете за докладване не следва да представляват непропорционална тежест за микропредприятията и за други финансови субекти, които не са значими. Освен това, за да се избегне непропорционалната тежест за финансовите субекти, в сроковете за докладване следва да се вземат предвид почивните дни и официалните празници.

([1]) ОВ L 333, 27.12.2022 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. 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) (ОВ L 333, 27.12.2022 г., стр. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Тъй като уведомяването за значителни киберзаплахи е на доброволен принцип, съдържанието на такива уведомления не следва да създава тежест за финансовите субекти и следва да бъде по-ограничено от информацията, която се изисква за съществени инциденти с ИКТ.

(7) Настоящият регламент е изготвен въз основа на проектите на регулаторни технически стандарти, представени на Комисията от европейските надзорни органи.

(8) Европейските надзорни органи проведоха открити обществени консултации по проектите на регулаторните технически стандарти, въз основа на които е изготвен настоящият регламент, анализираха потенциалните разходи и ползи и поискаха становище от групите на заинтересовани страни, създадени в съответствие с член 37 от регламенти (ЕС) № 1093/2010 ([3]), (ЕС) № 1094/2010 ([4]) и (ЕС) № 95/2010 ([5]) на Европейския парламент и на Съвета.

(9) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([6]) беше проведена консултация с Европейския надзорен орган по защита на данните, който прие положително становище на 22 юли 2024 г. Всяко обработване на лични данни в обхвата на настоящия регламент следва да се извършва в съответствие с приложимите принципи и разпоредби за защита на данните на Регламент (ЕС) 2018/1725,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Обща информация, която трябва да бъде предоставена в първоначалните уведомления и неокончателните и окончателните доклади за съществени инциденти с ИКТ

Финансовите субекти включват в първоначалното уведомление, неокончателния доклад и окончателния доклад, както са посочени в член 19, параграф 4 от Регламент (ЕС) 2022/2554, следната обща информация:

а) вида на подаването (първоначално уведомление, неокончателен доклад или окончателен доклад);

б) наименованието на финансовия субект, неговия ИКПС и вида на финансовия субект, както е посочено в член 2, параграф 1 от Регламент (ЕС) 2022/2554;

в) наименованието и идентификационния код на субекта, който подава първоначалното уведомление, неокончателния доклад или окончателния доклад за финансовия субект;

г) когато е приложимо, наименованията и ИКПС на всички финансови субекти, обхванати от обобщеното първоначално уведомление или неокончателния или окончателния доклад;

д) данните за контакт на лицата, отговарящи за комуникацията с компетентния орган относно съществения инцидент с ИКТ;

е) когато е приложимо, идентификацията на предприятието майка на групата, към която принадлежи финансовият субект;

ж) когато има парично въздействие, валутата, в която са сумите.

([3]) 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: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. 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).

Член 2

Специфична информация, която трябва да се предостави в първоначалните уведомления

Първоначалните уведомления, посочени в член 19, параграф 4, буква а) от Регламент (ЕС) 2022/2554, съдържат най-малко следната специфична информация:

а) референтен код на инцидента, определен от финансовия субект;

б) датата на откриване, часа на откриване и класификацията на инцидента съгласно член 8 от Делегиран регламент (ЕС) 2024/1772 на Комисията ([7]);

в) описание на инцидента с ИКТ;

г) критериите, посочени в членове 1—8 от Делегиран регламент (ЕС) 2024/1772, въз основа на които финансовият субект е класифицирал инцидента с ИКТ като съществен;

д) държавите членки, които са засегнати от инцидент с ИКТ;

е) информация за това как е открит инцидентът с ИКТ;

ж) когато е налична, информация за произхода на инцидента с ИКТ;

з) информация за това дали финансовият субект е задействал план за непрекъснатост на дейността;

и) когато е приложимо, информация за прекласифицирането на инцидента с ИКТ от съществен в несъществен;

й) когато е приложимо, всяка друга информация от значение.

Член 3

Специфична информация, която трябва да се предостави в неокончателните доклади

Неокончателните доклади, посочени в член 19, параграф 4, буква б) от Регламент (ЕС) 2022/2554, съдържат най-малко следната специфична информация:

а) когато е приложимо, референтния код на инцидента, предоставен от компетентния орган;

б) датата и часа на възникване на инцидента с ИКТ;

в) когато е приложимо, датата и часа на възстановяване на редовните дейности на финансовия субект;

г) информация за това как са изпълнени критериите, посочени в членове 1—8 от Делегиран регламент (ЕС) 2024/1772, въз основа на които финансовият субект е класифицирал инцидента с ИКТ като съществен;

д) вида на инцидента с ИКТ;

е) когато е приложимо, заплахите и техниките, използвани от автора на заплахата;

ж) засегнатите функционални области и работни процеси;

з) засегнатите инфраструктурни компоненти, които поддържат работните процеси;

и) въздействие върху финансовите интереси на клиентите;

й) информация за докладване за инцидент с ИКТ на други органи;

к) временни действия или мерки, предприети или планирани да бъдат предприети от финансовия субект за възстановяване след инцидента с ИКТ;

л) когато е приложимо, информация за показатели за компрометиране на системите.

([7]) Делегиран регламент (ЕС) 2024/1772 на Комисията от 13 март 2024 г. 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).

Член 4

Специфична информация, която трябва да се предостави в окончателните доклади

Окончателните доклади, посочени в член 19, параграф 4, буква в) от Регламент (ЕС) 2022/2554, съдържат следната специфична информация:

а) информация за първопричините за инцидента с ИКТ;

б) датите и часовете на разрешаване на инцидента с ИКТ и отстраняване на първопричината(ите);

в) информация за разрешаването на инцидента с ИКТ;

г) когато е приложимо, информация от значение за органите за преструктуриране;

д) информация за преките и непреките разходи и загуби, произтичащи от инцидента с ИКТ, и информация за финансовите възстановявания;

е) когато е приложимо, информация за повтарящи се инциденти с ИКТ.

Член 5

Срокове за първоначалното уведомяване и за неокончателния и окончателния доклад

1. Финансовите субекти подават първоначалното уведомление, неокончателния доклад и окончателния доклад, както са посочени в член 19, параграф 4, букви а), б) и в) от Регламент (ЕС) 2022/2554, в следните срокове:

а) за първоначалния доклад: възможно най-рано, но във всички случаи в рамките на четири часа от класифицирането на инцидента с ИКТ като съществен инцидент с ИКТ, и не по-късно от 24 часа от момента, в който финансовият субект е узнал за инцидента с ИКТ;

б) за неокончателния доклад: най-късно в рамките на 72 часа от подаването на първоначалното уведомление, дори когато статусът на инцидента или справянето с него не са се променили, както е посочено в член 19, параграф 4, буква б) от Регламент (ЕС) 2022/2554. Финансовите субекти представят актуализиран неокончателен доклад без неоправдано забавяне и във всички случаи, когато редовните дейности са възстановени;

в) за окончателния доклад: не по-късно от един месец след подаването на неокончателния доклад или, когато е приложимо, след последния актуализиран неокончателен доклад.

2. Когато финансовият субект не е класифицирал инцидент с ИКТ като съществен в рамките на 24 часа от момента, в който е узнал за него, но класифицира този инцидент с ИКТ като съществен на по-късен етап, финансовият субект подава първоначалното уведомление в рамките на четири часа от класифицирането на инцидента с ИКТ като съществен инцидент.

3. Финансовите субекти, които не са в състояние да подадат първоначалното уведомление, неокончателния доклад или окончателния доклад в сроковете, посочени в параграф 1, информират компетентния орган за това без неоправдано забавяне, но не по-късно от съответните срокове за подаването на уведомлението или доклада, и обясняват причините за забавянето.

4. Когато срокът за подаване на първоначално уведомление, неокончателен доклад или окончателен доклад съвпада с почивен или празничен ден в държавата членка на предоставящия информацията финансов субект, същият може да подаде първоначалното уведомление, неокончателния или окончателния доклад до обяд на следващия работен ден.

5. Параграф 4 не се прилага за подаване на първоначално уведомление или неокончателен доклад от кредитни институции, централни контрагенти, оператори на места на търговия и други финансови субекти, определени като съществени или важни субекти съгласно член 3 от Директива (ЕС) 2022/2555.

6. Компетентните органи могат да решат, че параграф 4 не се прилага за подаване на първоначално уведомление или неокончателен доклад от финансови субекти, различни от посочените в параграф 5, които са значими или имат системен характер за финансовия сектор на национално равнище или на равнището на Съюза. Компетентните органи уведомяват така определените финансови субекти за своето решение. Решението на компетентния орган се прилага само по отношение на инциденти, докладвани след датата на уведомяване на определените финансови субекти за решението от компетентния орган.

Член 6

Съдържание на уведомлението на доброволен принцип за значителни киберзаплахи

Съдържанието на уведомлението на доброволен принцип за значителни киберзаплахи, както е посочено в член 19, параграф 2 от Регламент (ЕС) 2022/2554, обхваща всички изброени по-долу елементи:

а) обща информация за уведомяващия финансов субект, както е посочено в член 1;

б) датата и часа на откриване на значителната киберзаплаха и всички други съответни електронни времеви печати, свързани със значителната киберзаплаха;

в) описание на значителната киберзаплаха;

г) информация за потенциалното въздействие на значителната киберзаплаха върху финансовия субект, неговите клиенти или финансови контрагенти;

д) критериите за класифициране, посочени в членове 1—8 от Делегиран регламент (ЕС) 2024/1772, които биха довели до задействането на процедура за докладване на съществен инцидент, ако киберзаплахата се е реализирала;

е) информация за състоянието на значителната киберзаплаха и за всички промени в нейната активност;

ж) когато е приложимо, описание на действията, предприети от финансовия субект за предотвратяване на реализирането на значителните киберзаплахи;

з) информация за всяко уведомяване на други финансови субекти или органи за значителна киберзаплаха;

и) когато е приложимо, информация за показатели за компрометиране на системите;

й) когато е приложимо, всяка друга информация от значение.

Член 7

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 23 октомври 2024 година.

За Комисията
Председател
Ursula VON DER LEYEN