РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/302 НА КОМИСИЯТА

от 23 октомври 2024 година

за определяне на технически стандарти за изпълнение с оглед на прилагането на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета по отношение на стандартните формуляри, образци и процедури за докладване от страна на финансовите субекти за съществен инцидент с ИКТ и за уведомяване за значителна киберзаплаха

(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, четвърта алинея от него,

като има предвид, че:

(1) за да се гарантира, че финансовите субекти докладват за съществените инциденти на своите компетентни органи по последователен начин, и за да се гарантира, че те предоставят на тези органи данни с добро качество, следва да се уточни кои полета за данни трябва да предоставят финансовите субекти на различните етапи от докладването, посочени в член 19, параграф 4 от Регламент (ЕС) 2022/2554. Важно е тази информация да бъде представена по начин, който дава възможност за единен преглед на инцидента. Поради това е необходимо да се определи единен образец за докладване за тези цели.

(2) Финансовите субекти следва да попълват тези полета за данни в образеца за докладване, които съответстват на информацията, изисквана в съответното уведомление или доклад. Все пак следва да се разреши на финансовите субекти, които вече разполагат с информация, която трябва да предоставят на по-късен етап от докладването, т.е. в неокончателния или окончателния доклад, да представят данните по-рано.

(3) Тъй като многобройни или повтарящи се инциденти могат да съставляват съществен инцидент, както е посочено в член 8 от Делегиран регламент (ЕС) 2024/1772 на Комисията ([2]), структурата на образеца за докладване и на полетата за данни следва да дава възможност на финансовите субекти да докладват такива повтарящи се инциденти.

(4) За да се осигури точна и актуална информация, образецът за докладване следва да дава възможност на финансовите субекти при подаването на неокончателния и окончателния доклад да актуализират всяка информация, която е била подадена по-рано, и при необходимост да прекласифицират съществени инциденти като несъществени.

(5) Правната идентификация на субектите следва да бъде приведена в съответствие с идентификаторите, посочени в техническите стандарти за изпълнение, приети съгласно член 28, параграф 9 от Регламент (ЕС) 2022/2554.

(6) Когато финансовите субекти възлагат задълженията за докладване на съществени инциденти с ИКТ на трета страна, компетентните органи следва да са запознати със самоличността на третата страна, която докладва от името на финансовия субект, преди подаването на първото уведомление или докладване, за да проверят легитимността на докладващата трета страна.

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

([2]) 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: https://eur-lex.europa.eu/eli/reg_del/2024/1772/oj).

(7) За да може лесно да се установи въздействието на инцидент, който е възникнал или е бил причинен от трета страна доставчик и който засяга множество финансови субекти в рамките на една държава членка, и за да се намалят усилията за докладване на финансовите субекти, образецът за докладване следва да позволява представянето на обобщен доклад, включващ обобщена информация за въздействието на инцидента върху всички засегнати финансови субекти, които са класифицирали инцидента като съществен.

(8) Образецът за докладване следва да бъде разработен по технологично неутрален начин, за да може да бъде внедрен в различни решения за докладване на инциденти, които вече съществуват или може да бъдат разработени за изпълнение на изискванията на Регламент (ЕС) 2022/2554.

(9) Структурата на образеца за докладване и полетата за данни следва да улеснят докладването на съществени инциденти с ИКТ от трети страни, на които финансовите субекти са възложили задължението си за докладване в съответствие с член 19, параграф 5 от Регламент (ЕС) 2022/2554.

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

(11) Европейските надзорни органи проведоха открити обществени консултации по проектите на техническите стандарти за изпълнение, въз основа на които е изготвен настоящият регламент, анализираха потенциалните разходи и ползи и поискаха становище от Групата на участниците от банковия сектор, създадена в съответствие с член 37 от Регламент (ЕС) № 1093/2010 ([3]), (ЕС) № 1094/2010 ([4]), (ЕС) № 1095/2010 ([5]) на Европейския парламент и на Съвета.

(12) 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, установени в Регламент (ЕС) 2018/1725,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Образец за докладване на съществени инциденти с ИКТ

1. Финансовите субекти използват образеца, установен в приложение I, за да подадат първоначалното уведомление, неокончателния доклад и окончателния доклад, посочени в член 19, параграф 4 от Регламент (ЕС) 2022/2554, както следва:

а) финансовите субекти, които подават първоначално уведомление, попълват полетата за данни в образеца, които съответстват на информацията, която трябва да бъде предоставена в съответствие с член 2 от Делегиран регламент (ЕС) 2025/301 на Комисията ([7]), а когато вече разполагат с тази информация, могат да попълнят полетата за данни, чието попълване не се изисква за първоначалното уведомление, но се изисква за неокончателния или окончателния доклад;

([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).

([7]) Делегиран регламент (ЕС) 2025/301 на Комисията от 23 октомври 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 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 (ОВ L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

б) финансовите субекти, които подават неокончателен доклад, попълват полетата за данни в образеца, които съответстват на информацията, която трябва да бъде предоставена в съответствие с член 3 от Делегиран регламент (ЕС) 2025/301, а когато вече разполагат със съответната информация, могат да попълнят полетата за данни, чието попълване не се изисква за неокончателния доклад, но се изисква за окончателния доклад;

в) финансовите субекти, които подават окончателен доклад, попълват полетата за данни в образеца, които съответстват на информацията, която трябва да бъде предоставена в съответствие с член 4 от Делегиран регламент (ЕС) 2025/301.

2. Финансовите субекти гарантират, че информацията, съдържаща се в първоначалното уведомление, както и в неокончателния и окончателния доклад, е пълна и точна.

3. Финансовите субекти предоставят прогнозни стойности въз основа на други налични данни и информация, доколкото това е възможно, когато към момента на докладване за първоначалното уведомление или неокончателния доклад не са налични точни данни.

4. При представянето на неокончателен или окончателен доклад финансовите субекти използват образеца, посочен в приложение I, за да представят цялата необходима информация и да актуализират, когато е приложимо, информацията, която е била предоставена преди това в първоначалното уведомление или в неокончателния доклад.

5. При попълването на образеца, установен в приложение I, финансовите субекти следват речника на данните и инструкциите, посочени в приложение II.

Член 2

Съвместно подаване на първоначалното уведомление, неокончателния и окончателния доклад

Финансовите субекти могат да комбинират подаването на първоначалното уведомление, неокончателния доклад и окончателния доклад, за да предоставят два или всички тях едновременно, когато редовните дейности са възстановени или анализът на първопричината е завършен, и при условие че са спазени сроковете, определени в член 5 от Делегиран регламент (ЕС) 2025/301.

Член 3

Повтарящи се инциденти с ИКТ

Финансовите субекти, които предоставят информация за несъществени повтарящи се инциденти с ИКТ, които съвкупно отговарят на условията за един съществен инцидент с ИКТ, както е посочено в член 8, параграф 2 от Делегиран регламент (ЕС) 2024/1772, предоставят тази информация в обобщен вид.

Член 4

Използване на защитени електронни канали

1. Финансовите субекти използват защитени електронни канали, предоставени от техния компетентен орган, за подаване на първоначалното уведомление и на неокончателния и окончателния доклад.

2. Финансовите субекти, които не са в състояние да използват защитените електронни канали, предоставени от техния компетентен орган, информират същия за съществен инцидент с ИКТ чрез други защитени средства, съгласувани с компетентния орган. Ако това се изисква от компетентния орган, финансовите субекти подават отново първоначалното уведомление или неокончателния или окончателния доклад чрез защитения електронен канал, предоставен от техния компетентен орган, след като са в състояние да го направят.

Член 5

Прекласифициране на съществени инциденти с ИКТ

Когато след допълнителна оценка финансовият субект стигне до заключението, че инцидентът с ИКТ, за който преди това е било докладвано, че е съществен, в нито един момент не е отговарял на критериите за класифициране и праговете, посочени в член 8 от Делегиран регламент (ЕС) 2024/1772, финансовият субект уведомява компетентния орган, че е прекласифицирал инцидента с ИКТ от съществен в несъществен, като предоставя информация за това прекласифициране в образеца, установен в приложение II към настоящия регламент, в полетата „вид на доклада“ и „друга информация“.

Член 6

Уведомяване за възлагане на задължения за докладване

1. Финансовите субекти, които са възложили задължението за докладване за съществени инциденти с ИКТ в съответствие с член 19, параграф 5 от Регламент (ЕС) 2022/2554, информират своя компетентен орган за това споразумение за възлагане веднага след сключването му и най-късно преди първото уведомление или докладване.

2. Финансовите субекти предоставят на компетентния орган името, данните за контакт и идентификационния код на третата страна, която ще подава от тяхно име уведомленията или докладите за съществени инциденти с ИКТ.

3. Финансовите субекти информират своя компетентен орган веднага след като престанат да възлагат задълженията си за докладване, както е посочено в член 19, параграф 5 от Регламент (ЕС) 2022/2554.

Член 7

Предоставяне на обобщена информация

1. Трета страна доставчик на услуги, на която са възложени задължения за докладване, както е посочено в член 19, параграф 5 от Регламент (ЕС) 2022/2554, може да използва образеца, посочен в приложение I към настоящия регламент, за да предостави обобщена информация за съществен инцидент с ИКТ, който е засегнал множество финансови субекти, в едно-единствено уведомление или доклад и да подаде това уведомление или доклад на компетентния орган от името на всички засегнати финансови субекти, при условие че са изпълнени всички изброени по-долу условия:

а) същественият инцидент с ИКТ, който трябва да бъде докладван, произхожда или е причинен от трета страна доставчик на услуги в областта на ИКТ;

б) тази трета страна доставчик на услуги предоставя съответната услуга в областта на ИКТ на повече от един финансов субект или на група;

в) инцидентът с ИКТ е класифициран като съществен от всеки финансов субект, обхванат от уведомлението или доклада с обобщена информация;

г) същественият инцидент с ИКТ засяга финансови субекти в рамките на една държава членка и обобщеният доклад се отнася до финансови субекти, които са под надзора на един и същ компетентен орган;

д) компетентните органи изрично са разрешили на този вид финансов субект да предоставя обобщена информация.

2. Параграф 1 не се прилага за кредитните институции, които се считат за значими, както е посочено в член 2, точка 16 от Регламент (ЕС) № 468/2014 на Европейската централна банка ([8]), операторите на места на търговия и централните контрагенти, които използват образеца в приложение I само за индивидуално подаване на уведомления или доклади за съществени инциденти с ИКТ до своя компетентен орган.

3. Когато компетентните органи изискват информация за индивидуалното въздействие на съществен инцидент с ИКТ върху отделен финансов субект, по искане на компетентния орган финансовият субект подава индивидуално уведомление или доклад за съществения инцидент с ИКТ.

([8]) Регламент (ЕС) № 468/2014 на Европейската централна банка от 16 април 2014 г. за създаване на рамката за сътрудничество в единния надзорен механизъм между Европейската централна банка и националните компетентни органи и с определените на национално равнище органи (Рамков регламент за ЕНМ) (ЕЦБ/2014/17) (ОВ L 141, 14.5.2014 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj) .

Член 8

Уведомяване за значителни киберзаплахи

1. Финансовите субекти, които уведомяват компетентните органи за значителни киберзаплахи в съответствие с член 19, параграф 2 от Регламент (ЕС) 2022/2554, използват образеца, установен в приложение III към настоящия регламент, и следват речника на данните и инструкциите, установени в приложение IV към настоящия регламент.

2. Финансовите субекти гарантират, че информацията, съдържаща се в уведомлението за значителни киберзаплахи, е пълна и точна.

Член 9

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

ПРИЛОЖЕНИЕ I

Образци за докладване на съществени инциденти

Номер на полето	Поле за данни	
Обща информация за финансовия субект		
1.1	Вид подаване на данни	
1.2	Наименование на субекта, който подава доклада	
1.3	Идентификационен код на субекта, който подава доклада	
1.4	Вид на засегнатия финансов субект	
1.5	Наименование на засегнатия финансов субект	
1.6	ИКПС на засегнатия финансов субект	
1.7	Име на основното лице за контакт	
1.8	Адрес на електронната поща на основното лице за контакт	
1.9	Телефон на основното лице за контакт	
1.10	Име на второ лице за контакт	
1.11	Адрес на електронната поща на второто лице за контакт	
1.12	Телефон на второто лице за контакт	
1.13	Наименование на крайното предприятие майка	
1.14	ИКПС на крайното предприятие майка	
1.15	Отчетна валута	
Съдържание на първоначалното уведомление		
2.1	Референтен код на инцидента, определен от финансовия субект	
2.2	Дата и час на откриване на съществения инцидент с ИКТ	
2.3	Дата и час на класифициране на инцидента с ИКТ като съществен	
2.4	Описание на съществения инцидент с ИКТ	
2.5	Критерии за класифициране, които са довели до задействането на процедурата за докладване на инцидент	
2.6	Прагове на същественост за критерия за класифициране „Географски обхват“	
2.7	Откриване на съществения инцидент с ИКТ	

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Номер на полето	Поле за данни	
2.8	Посочване дали съществените инцидент с ИКТ произхожда от трета страна доставчик или от друг финансов субект	
2.9	Задействане на плана за непрекъснатост на дейността, ако е задействан	
2.10	Друга полезна информация	
Съдържание на неокончателния доклад		
3.1	Референтен код на инцидента, предоставен от компетентния орган	
3.2	Дата и час на възникване на съществения инцидент с ИКТ	
3.3	Дата и час на възстановяване на услугите, дейностите или операциите	
3.4	Брой на засегнатите клиенти	
3.5	Процент на засегнатите клиенти	
3.6	Брой на засегнатите финансови контрагенти	
3.7	Процент на засегнатите финансови контрагенти	
3.8	Въздействие върху значимите клиенти или финансови контрагенти	
3.9	Брой на засегнатите трансакции	
3.10	Процент на засегнатите трансакции	
3.11	Стойност на засегнатите трансакции	
3.12	Информация за това дали цифрите са действителни или приблизителни, или дали не е имало някакво въздействие	
3.13	Въздействие върху репутацията	
3.14	Контекстна информация относно въздействието върху репутацията	
3.15	Продължителност на съществения инцидент с ИКТ	
3.16	Период на прекъсване на услугата	
3.17	Информация дали цифрите за продължителността и периода на прекъсване на услугата са действителни или приблизителни.	
3.18	Видове въздействие в държавите членки	
3.19	Описание на начина, по който съществените инцидент с ИКТ оказва въздействие върху други държави членки	
3.20	Прагове на същественост за критерия за класифициране „Загуби на данни“	
3.21	Описание на загубите на данни	

Номер на полето	Поле за данни	
3.22	Критерий за класифициране „Засегнати критични услуги“	
3.23	Вид на съществения инцидент с ИКТ	
3.24	Други видове инциденти	
3.25	Заплахи и техники, използвани от автора на заплахата	
3.26	Други видове техники	
3.27	Информация за засегнатите функционални области и работни процеси	
3.28	Засегнати инфраструктурни компоненти, които поддържат работните процеси	
3.29	Информация за засегнатите инфраструктурни компоненти, които поддържат работните процеси	
3.30	Въздействие върху финансовите интереси на клиентите	
3.31	Докладване на други органи	
3.32	Уточняване на „други“ органи	
3.33	Временни действия/мерки, предприети или планирани да бъдат предприети за възстановяване от инцидента	
3.34	Описание на всички временни действия и мерки, предприети или планирани да бъдат предприети за възстановяване от инцидента	
3.35	Показатели за компрометиране на системите	
Съдържание на окончателния доклад		
4.1	Високо равнище на класификация на първопричините за инцидента	
4.2	Подробна класификация на първопричините за инцидента	
4.3	Допълнителна класификация на първопричините за инцидента	
4.4	Други видове първопричини	
4.5	Информация за първопричините за инцидента	
4.6	Резюме на разрешаването на инцидента	
4.7	Дата и час на отстраняване на първопричината за инцидента	
4.8	Дата и час на разрешаване на инцидента	
4.9	Информация за това дали датата на трайното разрешаване на инцидента се различава от първоначално планираната дата на изпълнение	
4.10	Оценка на риска за критичните функции за целите на разрешаването	
4.11	Информация от значение за органите за преструктуриране	

Номер на полето	Поле за данни	
4.12	Прагове на същественост за критерия за класифициране „Икономическо въздействие“	
4.13	Размер на брутните преки и непреки разходи и загуби	
4.14	Размер на финансовите възстановявания	
4.15	Информация за това дали несъществените инциденти са били повтарящи се	
4.16	Дата и час на възникване на повтарящи се инциденти	

ПРИЛОЖЕНИЕ II

Речник на данните и инструкции за докладване на съществени инциденти

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
Обща информация за финансовия субект					
1.1. Вид подаване на данни	Посочете вида на уведомлението или доклада за инцидента, подаван(о) до компетентния орган.	Да	Да	Да	Избор: — първоначално уведомление; — неокончателен доклад; — окончателен доклад; — съществен инцидент, прекласифициран като несъществен.
1.2. Наименование на субекта, който подава доклада	Пълно наименование на фирмата на субекта, който подава доклада	Да	Да	Да	Буквено-цифрово
1.3. Идентификационен код на субекта, който подава доклада	Идентификационен код на субекта, който подава доклада. Когато финансовите субекти подават уведомлението/доклада, идентификационният код е идентификационният код на правния субект (ИКПС), който представлява уникален код от 20 буквено-цифрови знака въз основа на ISO 17442-1:2020. Трета страна доставчик, която подава доклад за финансов субект, може да използва идентификационен код, както е посочено в техническите стандарти за изпълнение, приети съгласно член 28, параграф 9 от Регламент (ЕС) 2022/2554..	Да	Да	Да	Буквено-цифрово
1.4. Вид на засегнатия финансов субект	Вид на субекта, посочен в член 2, параграф 1, букви а)—у) от Регламент (ЕС) 2022/2554, за който се представя докладът. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, избраните различни видове финансови субекти, обхванати от обобщения доклад.	Да	Да	Да	Избор (може да изберете повече от един елемент) — кредитна институция; — платежна институция; — освободена платежна институция; — доставчик на услуги по предоставяне на информация за сметка; — институция за електронни пари; — освободена институция за електронни пари; — инвестиционен посредник; — доставчик на услуги за криптоактиви; — емитент на токени, обезпечени с активи; — централен депозитар на ценни книжа; — централен контрагент; — място на търговия; — регистър на трансакции;

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
					— лице, управляващо алтернативен инвестиционен фонд; — управляващо дружество; — доставчик на услуги за докладване на данни; — застрахователно и презастрахователно предприятие; — застрахователен посредник, презастрахователен посредник и посредник, предлагащ застрахователни продукти като допълнителна дейност; — институция за професионално пенсионно осигуряване; — агенция за кредитен рейтинг; — администратор на критични бенчмаркове; — доставчик на услуги за колективно финансиране; — регистър на секюритизации.
1.5. Наименование на засегнатия финансов субект	Пълно наименование на фирмата на финансовия субект, засегнат от съществен инцидент с ИКТ и задължен да докладва за съществения инцидент на своя компетентен орган съгласно член 19 от Регламент (ЕС) 2022/2554. В случай на предоставяне на обобщена информация: а) списък с имената на всички финансови субекти, засегнати от съществения инцидент с ИКТ, разделени с точка и запетая; б) третата страна доставчик, която подава уведомление за съществен инцидент или доклад под формата на обобщена информация, както е посочено в член 7 от настоящия регламент, следва да посочи имената на всички финансови субекти, засегнати от инцидента, разделени с точка и запетая.	Да, ако финансовият субект, засегнат от инцидента, е различен от субекта, който подава доклада, и в случай на предоставяне на обобщена информация.	Да, ако финансовият субект, засегнат от инцидента, е различен от субекта, който подава доклада, и в случай на предоставяне на обобщена информация	Да, ако финансовият субект, засегнат от инцидента, е различен от субекта, който подава доклада, и в случай на предоставяне на обобщена информация	Буквено-цифрово
1.6. ИКПС на засегнатия финансов субект	Идентификационен код на правния субект (ИКПС) на финансовия субект, засегнат от съществения инцидент с ИКТ, определен в съответствие с Международната организация по стандартизация. В случай на предоставяне на обобщена информация: а) списък на всички ИКПС на финансовите субекти, засегнати от съществения инцидент с ИКТ, разделени с точка и запетая;	Да, ако финансовият субект, засегнат от съществения инцидент с ИКТ, е различен от	Да, ако финансовият субект, засегнат от съществения инцидент с ИКТ, е различен от субекта, който	Да, ако финансовият субект, засегнат от съществения инцидент с ИКТ, е различен от	Уникален 20-буквено-цифров код въз основа на ISO 17442-1:2020

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
		б) третата страна доставчик, която подава уведомление за съществен инцидент или обобщен доклад, както е посочено в член 7 от настоящия регламент, следва да посочи ИКПС на всички финансови субекти, засегнати от инцидента, разделени с точка и запетая. Редът на изброяване на ИКПС и имената на финансовите субекти трябва да е идентичен.	субекта, който подава доклада, и в случай на предоставяне на обобщена информация.	подава доклада, и в случай на предоставяне на обобщена информация.	субекта, който подава доклада, и в случай на предоставяне на обобщена информация	
1.7.	Име на основното лице за контакт	Име и фамилия на основното лице за контакт на финансовия субект. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, името на основното лице за контакт на субекта, който подава обобщения доклад.	Да	Да	Да	Буквено-цифрово
1.8.	Адрес на електронната поща на основното лице за контакт	Адрес на електронната поща на основното лице за контакт, който може да бъде използван от компетентния орган за последваща комуникация. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, адресът на електронната поща на основното лице за контакт на субекта, който подава обобщения доклад.	Да	Да	Да	Буквено-цифрово
1.9.	Телефон на основното лице за контакт	Телефонният номер на основното лице за контакт, който може да бъде използван от компетентния орган за последваща комуникация. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, телефонният номер на основното лице за контакт на субекта, който подава обобщения доклад. Телефонният номер се съобщава с всички международни префикси (напр. +33XXXXXXXXX)	Да	Да	Да	Буквено-цифрово
1.10.	Име на второ лице за контакт	Име и фамилия на второто лице за контакт или име на отговорния екип на финансовия субект или на субекта, който подава доклада от името на финансовия субект	Да	Да	Да	Буквено-цифрово
1.11.	Адрес на електронната поща на второто лице за контакт	Адрес на електронната поща на второто лице за контакт или функционален адрес на електронната поща на екипа, който може да бъде използван от компетентния орган за последваща комуникация.	Да	Да	Да	Буквено-цифрово

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
1.12. Телефон на второто лице за контакт	Телефонният номер на второто лице за контакт или на екип, който може да бъде използван от компетентния орган за последваща комуникация. Телефонният номер се съобщава с всички международни префикси (напр. +33XXXXXXXXX)	Да	Да	Да	Буквено-цифрово
1.13. Наименование на крайното предприятие майка	Наименование на крайното предприятие майка на групата, към която принадлежи засегнатият финансов субект, когато е приложимо.	Да, ако ФС принадлежи към група.	Да, ако ФС принадлежи към група.	Да, ако ФС принадлежи към група.	Буквено-цифрово
1.14. ИКПС на крайното предприятие майка	ИКПС на крайното предприятие майка на групата, към която принадлежи засегнатият финансов субект, когато е приложимо. Определен в съответствие с Международната организация по стандартизация.	Да, ако ФС принадлежи към група.	Да, ако ФС принадлежи към група.	Да, ако ФС принадлежи към група.	Уникален 20-буквено-цифров код въз основа на ISO 17442-1:2020.
1.15. Отчетна валута	Валута, използвана за докладване на инциденти	Да	Да	Да	Изборът се попълва чрез използване на валутните кодове съгласно ISO 4217
Съдържание на първоначалното уведомление					
2.1. Референтен код на инцидента, определен от финансовия субект	Уникален референтен код, издаден от финансовия субект, с който недвусмислено се идентифицира съществения инцидент с ИКТ. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, референтният код на инцидента, определен от третата страна доставчик.	Да	Да	Да	Буквено-цифрово
2.2. Дата и час на откриване на инцидента с ИКТ	Дата и час на узнаване от страна на финансовия субект за инцидента с ИКТ. За повтарящи се инциденти — датата и часът на откриване на последният инцидент с ИКТ.	Да	Да	Да	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДД Тчч:мм:сс)

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
2.3.	Дата и час на класифициране на инцидента като съществен	Дата и час на класифициране на инцидента с ИКТ като съществен в съответствие с критериите за класифициране, установени в Делегиран регламент (ЕС) 2024/1772	Да	Да	Да	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДД Тчч:мм:сс)
2.4.	Описание на инцидента с ИКТ	Описание на най-съществените аспекти на съществения инцидент с ИКТ. Финансовите субекти предоставят общ преглед на следната информация, като например възможни причини, непосредствени въздействия, засегнати системи и други. Финансовите субекти, включват, когато е известно или може основателно да се очаква, дали инцидентът засяга трети страни доставчици или други финансови субекти, вида на доставчика или финансовия субект, тяхното наименование, съответните им идентификационни кодове и вида на идентификационния код (напр. ИКПС или ЕЕИК). В последващите доклади съдържанието на полетата може да бъде променяно с течение на времето, така че да отразява текущото разбиране за инцидента с ИКТ и да описва всяка друга значима информация за инцидента с ИКТ, която не е обхваната от полетата за данни, включително вътрешната оценка на сериозността, извършена от финансовия субект (напр. много ниска, ниска, средна, висока, много висока) и посочване на равнището и името на най-висшите структури за вземане на решения, които са участвали в реагирането на инцидента с ИКТ.	Да	Да	Да	Буквено-цифрово
2.5.	Критерии за класифициране, които са довели до задействането на процедурата за докладване на инцидент	Критерии за класифициране съгласно Делегиран регламент (ЕС) 2024/1772, които са довели до определянето на инцидента с ИКТ като съществен и до задействане на процедурата за последващо уведомяване и докладване. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, критериите за класифициране, които са довели до определянето на инцидента с ИКТ като съществен за поне един или повече финансови субекти.	Да	Да	Да	Избор (от няколко възможности): — засегнати клиенти, финансови контрагенти и трансакции; — въздействие върху репутацията; — продължителност и прекъсване на услугата; — географски обхват; — загуби на данни; — засегнати критични услуги; — икономическо въздействие.
2.6.	Прагове на същественост за критерия за класифициране „Географски обхват“	Държави членки на ЕИП, засегнати от съществен инцидент с ИКТ Когато оценяват въздействието на съществен инцидент с ИКТ в други държави членки, финансовите субекти вземат предвид членове 4 и 12 от Делегиран регламент (ЕС) 2024/1772.	Да, ако е достигнат прагът за критерия „Географски обхват“.	Да, ако е достигнат прагът за критерия „Географски обхват“.	Да, ако е достигнат прагът за критерия „Географски обхват“.	Изборът (от няколко възможности) се попълва чрез използване на ISO 3166 ALPHA-2 на засегнатите държави

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
2.7.	Откриване на съществения инцидент с ИКТ	Посочване на начина, по който е бил открит съществените инцидент с ИКТ.	Да	Да	Да	Избор: — сигурност на ИТ; — персонал; — вътрешен одит; — външен одит; — клиенти; — финансови контрагенти; — трета страна доставчик; — извършител на атаката; — системи за наблюдение; — орган/агенция/правоприлагащ орган; — други.
2.8.	Посочване дали инцидентът произхожда от трета страна доставчик или от друг финансов субект	Посочване дали съществените инцидент с ИКТ произхожда от трета страна доставчик или от друг финансов субект. Финансовите субекти посочват дали съществените инцидент с ИКТ произхожда от трета страна доставчик или от друг финансов субект (включително финансови субекти, принадлежащи към същата група като докладващия субект), както и името, идентификационния код на третата страна доставчик или на финансовия субект и вида на идентификационния код (напр. ИКПС или ЕЕИК).	Да, ако инцидентът произхожда от трета страна доставчик или от друг финансов субект	Да, ако инцидентът произхожда от трета страна доставчик или от друг финансов субект	Да, ако инцидентът произхожда от трета страна доставчик или от друг финансов субект	Буквено-цифрово
2.9.	Задействане на плана за непрекъснатост на дейността, ако е задействан	Посочване дали е имало официално задействане на мерките за реакция за непрекъснатост на дейността на финансовия субект.	Да	Да	Да	Булев вид данни (да или не).
2.10.	Друга полезна информация	Всякаква допълнителна информация, която не е включена в образеца. Финансовите субекти, които са прекласифицирали съществен инцидент с ИКТ като несъществен, описват причините, поради които инцидентът с ИКТ не отговаря и не се очаква да отговаря на критериите, за да бъде считан за съществен инцидент с ИКТ.	Да, ако има друга информация, която не е включена в образеца, или	Да, ако има друга информация, която не е включена в образеца, или ако	Да, ако има друга информация, която не е включена в образеца, или	Буквено-цифрово

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
			ако същественият инцидент с ИКТ е бил прекласифициран като несъществен.	същественият инцидент с ИКТ е бил прекласифициран като несъществен	ако същественият инцидент с ИКТ е бил прекласифициран като несъществен	
Съдържание на неокончателния доклад						
3.1.	Референтен код на инцидента, предоставен от компетентния орган	Уникален референтен код, определен от компетентния орган в момента на получаване на първоначалното уведомление за недвусмислено идентифициране на съществения инцидент с ИКТ.	Не	Да, ако е приложимо	Да, ако е приложимо	Буквено-цифрово
3.2.	Дата и час на възникване на инцидента	Дата и час на възникване на съществения инцидент с ИКТ, ако са различни от момента, в който финансовият субект е узнал за съществения инцидент с ИКТ. За повтарящи се съществени инциденти с ИКТ, датата и часът на възникване на последния съществен инцидент с ИКТ.	Не	Да	Да	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДДTчч:мм:сс)
3.3.	Дата и час на възстановяване на услугите, дейностите или операциите	Информация за датата и часа на възстановяване на услугите, дейностите или операциите, засегнати от съществения инцидент с ИКТ.	Не	Да, ако полето за данни 3.16. „Период на прекъсване на услугата“ е попълнено	Да, ако полето за данни 3.16. „Период на прекъсване на услугата“ е попълнено	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДДTчч:мм:сс)
3.4.	Брой на засегнатите клиенти	Брой клиенти, засегнати от съществения инцидент с ИКТ, които ползват услугата, предоставяна от финансовия субект. Когато оценяват броя на засегнатите клиенти, финансовите субекти вземат предвид член 1, параграф 1 и член 9, параграф 1, буква б) от Делегиран регламент (ЕС) 2024/1772 при своята оценка. Финансов субект, който не може да определи действителния брой на засегнатите клиенти, използва приблизителни оценки, основани на наличните данни от сравними референтни периоди. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, общият брой на засегнатите клиенти във всички финансови субекти.	Не	Да	Да	Цяло число

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
3.5.	Процент на засегнатите клиенти	Процент на клиентите, засегнати от съществения инцидент с ИКТ, спрямо общия брой клиенти, които ползват засегнатата услуга, предоставяна от финансовия субект. В случай на повече от една засегната услуга, услугите се предоставят по обобщен начин. Финансовите субекти вземат предвид член 1, параграф 1 и член 9, параграф 1, буква а) от Делегиран регламент (ЕС) 2024/1772 при своята оценка. Финансов субект, който не може да определи действителния процент на засегнатите клиенти, използва приблизителни оценки, основани на наличните данни от сравними референтни периоди. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, финансовият субект разделя сбора на всички засегнати клиенти на общия брой клиенти на всички засегнати финансови субекти.	Не	Да	Да	Изразено в процент — всяка стойност до 5 цифрови знака, в т.ч. до 1 цифра след десетичния знак, изразена като процент (напр. 2,4 вместо 2,4 %). Ако стойността има повече от 1 цифра след десетичния знак, докладващите контрагенти я закръглят нагоре.
3.6.	Брой на засегнатите финансови контрагенти	Брой финансови контрагенти, засегнати от съществен инцидент с ИКТ, които са сключили договор с финансовия субект. Когато оценяват броя на засегнатите финансови контрагенти, финансовите субекти вземат предвид член 1, параграф 2 от Делегиран регламент (ЕС) 2024/1772 при своята оценка. Финансов субект, който не може да определи действителния брой на засегнатите финансови контрагенти, използва приблизителни оценки, основани на наличните данни от сравними референтни периоди. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, общият брой на засегнатите финансови контрагенти във всички финансови субекти.	Не	Да	Да	Цяло число

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
3.7.	Процент на засегнатите финансови контрагенти	Процент на финансовите контрагенти, засегнати от съществен инцидент с ИКТ, спрямо общия брой финансови контрагенти, които са сключили договор с финансовия субект. Когато оценяват процента на засегнатите финансови контрагенти, финансовите субекти вземат предвид член 1, параграф 1 и член 9, параграф 1, буква в) от Делегиран регламент (ЕС) 2024/1772 при своята оценка. Финансов субект, който не може да определи действителния процент на засегнатите финансови контрагенти, използва приблизителни оценки, основани на наличните данни от сравними референтни периоди. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, се посочва сборът на всички засегнати финансови контрагенти, разделен на общия брой финансови контрагенти на всички засегнати финансови субекти.	Не	Да	Да	Изразено като процент — всяка стойност до 5 цифрови знака, в т.ч. до 1 цифра след десетичния знак, изразена като процент (напр. 2,4 вместо 2,4 %). Ако стойността има повече от 1 цифра след десетичния знак, докладващите контрагенти я закръглят нагоре.
3.8.	Въздействие върху значимите клиенти или финансови контрагенти	Всяко установено въздействие върху значимите клиенти или финансови контрагенти, както е посочено в член 1, параграф 3 и член 9, параграф 1, буква е) от Делегиран регламент (ЕС) 2024/1772.	Не	Да, ако е достигнат прагът за критерия „Значимост на клиентите и финансовите контрагенти“.	Да, ако е достигнат прагът за критерия „Значимост на клиентите и финансовите контрагенти“.	Булев вид данни (да или не).
3.9.	Брой на засегнатите трансакции	Брой трансакции, засегнати от съществен инцидент с ИКТ. Когато оценяват въздействието върху трансакциите, финансовите субекти вземат предвид член 1, параграф 4 от Делегиран регламент (ЕС) 2024/1772, включително всички засегнати вътрешни и трансгранични трансакции, съдържащи парична сума, при които поне една част от трансакцията се извършва в Съюза.	Не	Да, ако инцидентът е засегнал някоя трансакция	Да, ако инцидентът е засегнал някоя трансакция	Цяло число

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	Финансов субект, който не може да определи действителния брой на засегнатите трансакции, използва приблизителни оценки, основани на наличните данни от сравними референтни периоди. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, се посочва общият брой на засегнатите трансакции във всички финансови субекти.				
3.10. Процент на засегнатите трансакции	Процент на засегнатите трансакции спрямо среднодневния брой вътрешни и трансгранични трансакции, извършени от финансовия субект, свързани със засегнатата услуга. Финансовите субекти вземат предвид член 1, параграф 4 и член 9, параграф 1, буква г) от Делегиран регламент (ЕС) 2024/1772 при своята оценка. Финансов субект, който не може да определи действителния процент на засегнатите трансакции, използва приблизителни оценки. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, финансовият субект събира броя на всички засегнати трансакции и разделя сбора на общия брой трансакции на всички засегнати финансови субекти.	Не	Да, ако инцидентът е засегнал някоя трансакция	Да, ако инцидентът е засегнал някоя трансакция	Изразено в процент — всяка стойност до 5 цифрови знака, в т.ч. до 1 цифра след десетичния знак, изразена в процент (напр. 2,4 вместо 2,4 %). Ако стойността има повече от 1 цифра след десетичния знак, докладващите контрагенти я закръглят нагоре.
3.11. Стойност на засегнатите трансакции	Общата стойност на трансакциите, засегнати от съществен инцидент с ИКТ, се оценява в съответствие с член 1, параграф 4 и член 9, параграф 1, буква д) от Делегиран регламент (ЕС) 2024/1772. Финансов субект, който не може да определи действителната стойност на засегнатите трансакции, използва приблизителни оценки, основани на наличните данни от сравними референтни периоди. Финансовият субект докладва паричната сума като положителна стойност. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, общата стойност на засегнатите трансакции във всички финансови субекти.	Не	Да, ако инцидентът е засегнал някакви трансакции	Да, ако инцидентът е засегнал някоя трансакция	Парична стойност Финансовите субекти докладват данните в единици с минимална точност до хиляди единици (напр. 2,5 вместо 2 500 EUR).

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
3.12. Информация за това дали цифрите са действителни или приблизителни, или дали не е имало някакво въздействие	Информация за това дали стойностите, докладвани в полетата за данни 3.4.-3.11. са действителни или приблизителни, или дали не е имало някакво въздействие.	Не	Да	Да	Избор (от няколко възможности): — действителни стойности на засегнатите клиенти; — действителни стойности на засегнатите финансови контрагенти; — действителни стойности на засегнатите трансакции; — приблизителни стойности на засегнатите клиенти; — приблизителни стойности на засегнатите финансови контрагенти; — приблизителни стойности на засегнатите трансакции; — без въздействие върху клиентите; — без въздействие върху финансовите контрагенти; — без въздействие върху трансакциите.
3.13. Въздействие върху репутацията	Информация за въздействието върху репутацията в резултат на съществен инцидент с ИКТ, както е посочено в член 2 и член 10 от Делегиран регламент (ЕС) 2024/1772. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, категориите за въздействие върху репутацията, които се прилагат за поне един финансов субект.	Не	Да, ако е изпълнен критерият „Въздействие върху репутацията“.	Да, ако е изпълнен критерият „Въздействие върху репутацията“.	Избор (от няколко възможности): — съществените инцидент с ИКТ е отразен в медиите; — съществените инцидент с ИКТ е довел до повтарящи се оплаквания от различни клиенти или финансови контрагенти относно насочени към клиента услуги или критични стопански отношения; — в резултат на съществения инцидент с ИКТ финансовият субект няма да е в състояние или е вероятно да не е в състояние да изпълнява регулаторните изисквания; — в резултат на съществения инцидент с ИКТ финансовият субект ще загуби или е вероятно да загуби клиенти или финансови контрагенти със съществено въздействие върху дейността му.
3.14. Контекстна информация относно въздействието върху репутацията	Информация, описваща как съществените инцидент с ИКТ е засегнал или би могъл да засегне репутацията на финансовия субект, включително нарушения на закона, неспазени регулаторни изисквания, брой оплаквания от клиенти и други.	Не	Да, ако е изпълнен критерият „Въздействие върху репутацията“.	Да, ако е изпълнен критерият „Въздействие върху репутацията“.	Буквено-цифрово

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	Контекстуалната информация включва вида на медиите (напр. традиционни и цифрови медии, блогове, платформи за стрийминг) и медийното отразяване, включително обхвата на медиите (местен, национален, международен). Медийното отразяване в този контекст не означава няколко негативни коментара от последователи или потребители на социалните мрежи. Финансовият субект посочва също така дали в отразяването в медиите са изтъкнати значителни рискове за неговите клиенти във връзка със съществения инцидент с ИКТ, включително риска от неплатежоспособност на финансовия субект или риска от загуба на средства. Финансовите субекти посочват също така дали са предоставили информация на медиите, която е послужила за надеждно информиране на обществеността за съществения инцидент с ИКТ и неговите последици. Финансовите субекти могат също така да посочат дали в медиите е имало невярна информация във връзка с инцидента с ИКТ, включително информация, основана на умишлена дезинформация, разпространявана от участниците в заплахата, или информация, свързана с неразрешена промяна на облика на уебсайта на финансовия субект или илюстрираща това деяние.				
3.15. Продължителност на инцидента	Финансовите субекти определят продължителността на съществения инцидент с ИКТ от момента на възникване на инцидента до момента на разрешаването му. Финансовите субекти, които не могат да определят момента, в който е настъпил съществуващият инцидент с ИКТ, определят неговата продължителност от по-ранния момент между момента, в който финансовият субект е открил инцидента, и момента, в който финансовият субект е записал инцидента в мрежовите или системните регистри или в други източници на данни. Финансовите субекти, които все още не знаят кога ще бъде разрешен съществуващият инцидент с ИКТ, прилагат приблизителни оценки. Стойността се изразява в дни, часове и минути. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, финансовите субекти определят най-дългата продължителност на съществения инцидент с ИКТ, в случай на разлики между финансовите субекти.	Не	Да	Да	ДД:ЧЧ:ММ

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
3.16. Период на прекъсване на услугата	Периодът на прекъсване на услугата се определя от момента, в който услугата е напълно или частично недостъпна за клиенти, финансови контрагенти или други вътрешни или външни потребители, до момента, в който редовните дейности или операции бъдат възстановени до предоставяното преди съществения инцидент с ИКТ ниво на услугата. Когато прекъсването на услугата води до забавяне при предоставянето на услугата, след като редовните дейности или операции са били възстановени, финансовите субекти определят периода на прекъсване от началото на съществения инцидент с ИКТ до момента, в който тази забавена услуга бъде предоставена. Финансовите субекти, които не могат да определят момента, в който е започнало прекъсването на услугата, определят периода на прекъсване на услугата измежду по-ранния момент от момента на откриване на инцидента и момента на записване на инцидента в регистрите. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, финансовите субекти определят най-дългата продължителност на прекъсването на услугата, в случай на разлики между финансовите субекти.	Не	Да, ако инцидентът е причинил прекъсване на услугата	Да, ако инцидентът е причинил прекъсване на услугата	ДД:ЧЧ:ММ
3.17. Информация дали цифрите за продължителността и периода на прекъсване на услугата са действителни или приблизителни.	Информация дали стойностите, посочени в полетата за данни 3.15. и 3.16., са действителни или приблизителни.	Не	Да, ако е изпълнен критерият „ Продължителност и прекъсване на услугата“	Да, ако е изпълнен критерият „ Продължителност и прекъсване на услугата“	Избор: — Действителни стойности; — Приблизителни оценки; — Действителни стойности и приблизителни оценки; — Няма налична информация.
3.18. Видове въздействие в държавите членки	Вид въздействие в съответните държави — членки на ЕИП. Посочване на това дали съществуващият инцидент с ИКТ е оказал въздействие в други държави — членки на ЕИП (различни от държавата членка на компетентния орган, на който инцидентът е докладван пряко), в съответствие с член 4 от Делегиран регламент (ЕС) 2024/1772, и по-специално по отношение на значимостта на въздействието във връзка със: а) засегнати клиенти и финансови контрагенти в други държави членки; или	Не	Да, ако е достигнат прагът за критерия „Географски обхват“	Да, ако е достигнат прагът за критерия „Географски обхват“	Избор (от няколко възможности): — клиенти; — финансови контрагенти; — клон на финансовия субект; — финансови субекти в рамките на групата, извършващи дейности в съответната държава членка; — инфраструктура на финансовите пазари; — трети страни доставчици, които може да са общи с други финансови субекти.

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	б) клонове или други финансови субекти в рамките на групата, извършващи дейности в други държави членки; или в) инфраструктури на финансовите пазари или трети страни доставчици, които може да засегнат финансови субекти в други държави членки, на които те предоставят услуги.				
3.19. Описание на начина, по който инцидентът оказва въздействие върху други държави членки	Описание на въздействието и тежестта на съществения инцидент с ИКТ във всяка засегната държава членка, включително оценка на въздействието и тежестта върху: а) клиенти; б) финансови контрагенти; в) клонове на финансовия субект; г) други финансови субекти в рамките на групата, извършващи дейности в съответната държава членка; д) инфраструктури на финансовия пазар; е) трети страни доставчици, които може да са общи с други финансови субекти, както е приложимо в друга(и) държава(и) членка(и).	Не	Да, ако е достигнат прагът за критерия „Географски обхват“	Да, ако е достигнат прагът за критерия „Географски обхват“	Буквено-цифрово
3.20. Прагове на същественост за критерия за класифициране „Загуби на данни“	Вид на загубите на данни в резултат на съществения инцидент с ИКТ във връзка с наличността, автентичността, цялостността и поверителността на данните. Финансовите субекти вземат предвид член 5 и член 13 от Делегиран регламент (ЕС) 2024/1772 при своята оценка. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, загубите на данни, засягащи поне един финансов субект.	Не	Да, ако е изпълнен критерият „Загуби на данни“.	Да, ако е изпълнен критерият „Загуби на данни“.	Избор (от няколко възможности): — наличност — автентичност — цялостност — поверителност
3.21. Описание на загубите на данни	Описание на въздействието на съществения инцидент с ИКТ върху наличността, автентичността, цялостността и поверителността на критичните данни в съответствие с член 5 и член 13 от Делегиран регламент (ЕС) 2024/1772. Информация за въздействието върху изпълнението на стопанските цели на финансовия субект или върху изпълнението на регулаторните изисквания. Като част от предоставената информация финансовите субекти посочват дали засегнатите данни са данни на клиенти, данни на други субекти (напр. финансови контрагенти) или данни на самия финансов субект.	Не	Да, ако е изпълнен критерият „Загуби на данни“.	Да, ако е изпълнен критерият „Загуби на данни“.	Буквено-цифрово

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
		Финансовият субект може също така да посочи вида на данните, свързани с инцидента — по-специално дали данните са поверителни и за какъв вид поверителност става въпрос (напр. поверителност на търговска/служебна информация, лични данни, професионална тайна: банкова тайна, застрахователна тайна, тайна на платежните услуги и т.н.). Информацията може да включва и възможни рискове, свързани със загубите на данни, като например дали данните, засегнати от инцидента, могат да бъдат използвани за идентифициране на лица и дали могат да бъдат използвани от автора на заплахата за получаване на кредити или заеми без тяхно съгласие, за провеждане на атаки на насочен фишинг, за публично разкриване на информация. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, общо описание на въздействието на инцидента върху засегнатите финансови субекти. Когато има разлики във въздействието, в описанието на въздействието ясно се посочва конкретното въздействие върху различните финансови субекти.				
3.22.	Критерий за класифициране „Засегнати критични услуги“	Информация, свързана с критерия „Засегнати критични услуги“. Финансовите субекти вземат предвид член 6 от Делегиран регламент (ЕС) 2024/1772 при своята оценка, включително информация за: — засегнатите услуги или дейности, за които се изисква разрешение, регистрация или които са под надзора на компетентните органи; или — услугите в областта на ИКТ или мрежовите и информационните системи, които поддържат критични или важни функции на финансовия субект; както и — естеството на злонамерения и непозволен достъп до мрежовите и информационните системи на финансовия субект. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, въздействието върху критичните услуги, които се отнасят за поне един финансов субект.	Не	Да	Да	Буквено-цифрово

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
3.23. Вид инцидент	Класификация на инцидентите по видове.	Не	Да	Да	Избор (от няколко възможности): — Свързан с киберсигурността; — Неизправност в процеса; — Срив в системата; — Външно събитие; — Свързан с плащане; — Друго (моля, уточнете).
3.24. Други видове инциденти	Други видове инциденти с ИКТ: финансовите субекти, които са избрали „друг“ вид инциденти в полето за данни 3.23, посочват вида на инцидента с ИКТ.	Не	Да, ако в полето за данни 3.23 е избран „друг“ вид инциденти	Да, ако в полето за данни 3.23 е избран „друг“ вид инциденти	Буквено-цифрово
3.25. Заплахи и техники, използвани от автора на заплахата	Посочват се заплахите и техниките, използвани от автора на заплахата, включително: а) социално инженерство, включително фишинг; б) (D)DoS; в) кражба на самоличност; г) криптиране на данни за въздействие, включително софтуер за изнудване; д) неразрешен контрол върху компютърни ресурси; е) кражба и манипулиране на данни, с изключение на кражба на самоличност; ж) унищожаване на данни; з) неразрешена промяна на облика на уебсайт; и) атака на верига за доставки й) друго (моля, уточнете).	Не	Да, ако видът на инцидента с ИКТ е „свързан с киберсигурността“ в поле 3.23	Да, ако видът на инцидента с ИКТ е „свързан с киберсигурността“ в поле 3.23	Избор (от няколко възможности): — Социално инженерство (включително фишинг); — (D)DoS; — Кражба на самоличност; — Криптиране на данни за въздействие, включително софтуер за изнудване; — Неразрешен контрол върху компютърни ресурси; — Кражба и манипулиране на данни, с изключение на кражба на самоличност; — Унищожаване на данни; — Неразрешена промяна на облика на уебсайт; — Атака на верига за доставки. — Друго (моля, уточнете)
3.26. Други видове техники	Други видове техники Финансовите субекти, които са избрали „друг“ вид техника в полето за данни 3.25, посочват вида на техниката.	Не	Да, ако в полето за данни 3.25 е избран „друг“ вид техника	Да, ако в полето за данни 3.25 е избран „друг“ вид техника	Буквено-цифрово

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
3.27.	Информация за засегнатите функционални области и работни процеси	Посочване на функционалните области и работните процеси, които са засегнати от инцидента, включително продукти и услуги. Функционалните области включват, наред с другото: а) маркетинг и стопанско развитие; б) обслужване на клиенти; в) управление на продуктите; г) спазване на нормативните изисквания; д) управление на риска; е) финанси и счетоводство; ж) услуги в областта на човешките ресурси и общи услуги; з) информационни технологии; Работните процеси включват, наред с другото: — информация за сметка; — актюерски услуги; — придобиване на платежни операции; — удостоверяване на автентичността/разрешение; — орган; — приобщаване на клиент; — управление на обезщетенията; — управление на изплащането на обезщетения; — покупко-продажба на пакети със застрахователни полици между застраховки; — картови плащания; — управление на парични средства; — внасяне или теглене на пари в брой; — уреждане на застрахователни претенции; — обработване на застрахователни претенции; — клиринг; — конгломерати за корпоративни заеми; — колективни застраховки; — кредитни преводи; — отговорно пазене и съхранение на активи; — приобщаване на нови клиенти; — постъпване на данни; — обработка на данни; — директни дебити; — експортни застраховки; — финализиране на сделки; — предлагане на финансови инструменти; — счетоводно обслужване на фондове;	Не	Да	Да	Буквено-цифрово

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	— валутни сделки; — инвестиционна консултация; — управление на инвестиции; — емитиране на платежни инструменти; — управление на кредити; — обработване на плащанията по застраховка „Живот“; — налични парични преводи; — изчисляване на нетни активи; — нареждания; — иницииране на плащане; — застрахователна подписваческа дейност; — управление на портфейл; — събиране на застрахователни премии; — получаване/предаване/изпълнение; — презастраховане; — сетълмент; — мониторинг на операции; В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, засегнатите функционални области и работни процеси в поне един финансов субект.				
3.28. Засегнати инфраструктурни компоненти, които поддържат работните процеси	Информация за това дали инфраструктурните компоненти (сървъри, операционни системи, софтуер, сървъри за приложения, мидълуер, мрежови компоненти и други), които поддържат работните процеси, са били засегнати от съществения инцидент с ИКТ.	Не	Да	Да	Избор: — Да; — Не; — Информацията не е налична.
3.29. Информация за засегнатите инфраструктурни компоненти, които поддържат работните процеси	Описание на въздействието на съществения инцидент с ИКТ върху инфраструктурните компоненти, които поддържат работните процеси, включително хардуер и софтуер. Хардуерът включва сървъри, компютри, центрове за данни, комутатори, маршрутизатори, концентратори. Софтуерът включва операционни системи, приложения, бази данни, инструменти за сигурност, мрежови компоненти и други, моля, посочете. В описанията се посочват или назовават засегнатите инфраструктурни компоненти или системи и, когато е възможно: а) информация за версията; б) вътрешна инфраструктура/частично възложена на външен изпълнител/изцяло възложена на външен изпълнител — наименование на третата страна доставчик;	Не	Да, ако инцидентът е засегнал инфраструк-турни компоненти, които поддържат работните процеси	Да, ако инцидентът е засегнал инфраструк-турни компоненти, които поддържат работните процеси	Буквено-цифрово

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	в) дали инфраструктурата е използвана или споделена за множество работни функции; г) съответните мерки за устойчивост/непрекъснатост/възстановяване/заменяемост.				
3.30. Въздействие върху финансовите интереси на клиентите	Информация дали съществените инцидент с ИКТ е засегнал финансовите интереси на клиентите.	Не	Да	Да	Избор: — Да; — Не; — Информацията не е налична.
3.31. Докладване на други органи	Посочване на органите, които са били информирани за съществения инцидент с ИКТ. Като се вземат предвид различията, произтичащи от националното законодателство на държавите членки, понятието „правоприлагащи органи“ се разбира от финансовите субекти в широк смисъл и включва публичните органи, оправомощени да извършват наказателно преследване на киберпрестъпления, включително полицията, правоприлагащите служби и прокуратурата.	Не	Да	Да	Избор (от няколко възможности): — Полиция/правоприлагащи органи; — ЕРИКС; — Орган за защита на данните; — Национална агенция за киберсигурност; — Няма такива; — Други (моля, уточнете).
3.32. Уточняване на „други“ органи	Уточняване на „другите“ видове органи, които са били информирани за съществения инцидент с ИКТ. Ако е избрано в полето за данни 3.31. „Други“, описанието включва по-подробна информация за органа, на който финансовият субект е подал информация за съществения инцидент с ИКТ.	Не	Да, ако финансовият субект е информирал „други“ видове органи за съществения инцидент с ИКТ.	Да, ако финансовият субект е информирал „други“ видове органи за съществения инцидент с ИКТ	Буквено-цифрово
3.33. Временни действия/мерки, предприети или планирани да бъдат предприети за възстановяване от инцидента	Посочване дали финансовият субект е изпълнил (или планира да изпълни) всички временни действия, които са били предприети (или планирани да бъдат предприети) за възстановяване от съществения инцидент с ИКТ.	Не	Да	Да	Булев вид данни (да или не).

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
3.34. Описание на всички временни действия и мерки, предприети или планирани да бъдат предприети за възстановяване от инцидента	В информацията се описват предприетите незабавни действия, включително изолиране на инцидента на мрежово равнище, активиране на процедури за намиране на временно решение, блокиране на USB портове, активиране на сайт за възстановяване след бедствия, всякакви други временно въведени допълнителни мерки за сигурност. Финансовите субекти посочват датата и часа на изпълнение на временните действия и очакваната дата на връщане към основния сайт. За всички временни действия, които не са изпълнени, но все още са планирани, се посочва датата, до която се очаква тяхното изпълнение. Ако не са предприети временни действия/мерки, моля, посочете причината за това.	Не	Да, ако са предприети или се планира да бъдат предприети временни действия/мерки (поле за данни 3.33)	Да, ако са предприети или се планира да бъдат предприети временни действия/мерки (поле за данни 3.33)	Буквено-цифрово
3.35. Показатели за компрометиране на системите	Информация, свързана със съществения инцидент с ИКТ, която може да помогне за идентифициране на злонамерена дейност в мрежата или информационната система (показатели за компрометиране на системите), когато е приложимо. Полето се прилага само за финансовите субекти, които попадат в обхвата на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([1]), и за финансовите субекти, които са определени като съществени или важни субекти съгласно националните правила, с които се транспонира член 3 от Директива (ЕС) 2022/2555, когато е приложимо. Предоставените от финансовия субект показатели за компрометиране на системите включват следните категории данни: а) IP адреси; б) URL адреси; в) домейни; г) хешове на файлове; д) данни за зловреден софтуер (име на зловредния софтуер, имена на файлове и тяхното местоположение, специфични ключове в регистъра, свързани с дейността на зловредния софтуер); е) данни за мрежовата активност (портове, протоколи, адреси, препратки, потребителски агенти, заглавия, специфични регистри или характерни модели в мрежовия трафик); ж) данни за съобщения на електронната поща (подател, получател, тема, заглавие, съдържание);	Не	Да, ако в полето за данни 3.23. за вида инцидент е избран „свързан с киберсигурността“	Да, ако в полето за данни 3.23. за вида инцидент е избран „свързан с киберсигурността“	Буквено-цифрово

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	з) DNS заявки и конфигурации на регистъра; и) дейности, свързани с потребителски профили (влизане в системата, дейности, свързани с привилегировани потребителски профили, ескалация на привилегии); й) трафик на базата данни (четене/запис), заявки към същия файл. На практика този вид информация може да включва данни, свързани, наред с другото, с показатели, описващи модели в мрежовия трафик, съответстващи на известни атаки/съобщения от бот мрежи, IP адреси на машини, заразени със зловреден софтуер (ботове), данни, свързани със сървъри за управление и контрол, използвани от зловреден софтуер (обикновено домейни или IP адреси), и URL адреси, свързани с наблюдавани фишинг сайтове или уебсайтове, които хостват зловреден софтуер или комплекти с експлойти.				
Съдържание на окончателния доклад					
4.1. Високо равнище на класификация на първопричините за инцидента	Високо равнище на класификация на първопричината за съществения инцидент с ИКТ в рамките на видовете инциденти, включително следните категории от високо равнище: а) злонамерени действия; б) неизправност в процеса; в) срив/неизправност на системата; г) човешка грешка; д) външно събитие.	Не	Не	Да	Избор (от няколко възможности): — злонамерени действия; — неизправност в процеса; — срив/неизправност на системата; — човешка грешка; — външно събитие.
4.2. Подробна класификация на първопричините за инцидента	Подробна класификация на първопричините за съществения инцидент с ИКТ в рамките на видовете инциденти, включително следните подробни категории, свързани с категориите от високо равнище, които се докладват в полето за данни 4.1: 1. **Злонамерени действия** (ако е избрано, посочете един или повече от следните елементи): а) преднамерени вътрешни действия; б) умишлено физическо увреждане/манипулация/кражба; в) действия, свързани с измами. 2. **Неизправност в процеса** (ако е избрано, посочете един или повече от следните елементи): а) недостатъчен мониторинг или липса на мониторинг и контрол;	Не	Не	Да	Избор (от няколко възможности): — злонамерени действия: преднамерени вътрешни действия; — злонамерени действия: умишлено физическо увреждане/манипулация/ кражба; — злонамерени действия: действия, свързани с измами; — неизправност в процеса: недостатъчен мониторинг или липса на мониторинг и контрол; — неизправност в процеса: **не**достатъчни/ неясни роли и отговорности; — неизправност в процеса: Неизправност в процеса на управление на риска в областта на ИКТ; — неизправност в процеса: недостатъчно или неуспешни операциите в областта на ИКТ и сигурността на ИКТ;

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	б) недостатъчни/неясни роли и отговорности; в) Неизправност в процеса на управление на риска в областта на ИКТ; г) недостатъчни или неуспешни операции в областта на ИКТ и сигурност на ИКТ; д) недостатъчно или неуспешно управление на проекти в областта на ИКТ; е) неподходящи вътрешни политики, процедури и документация; ж) неподходящо придобиване, разработване или поддържане на системи на ИКТ; з) друго (моля, уточнете). 3. **Срив/неизправност на системата** (ако е избрано, посочете един или повече от следните елементи): а) капацитет и ефективност на хардуера: съществени инциденти с ИКТ, причинени от хардуерни ресурси, които се оказват недостатъчни по отношение на капацитета или ефективността, за да бъдат изпълнени приложимите законодателни изисквания; б) поддръжка на хардуера: съществени инциденти с ИКТ в резултат на неподходяща или недостатъчна поддръжка на хардуерни компоненти, различни от „Остаряване/стареене на хардуера“; в) остаряване/стареене на хардуера: този тип първопричина включва съществени инциденти с ИКТ, които са резултат от остарели или застаряващи хардуерни компоненти; г) съвместимост/конфигурация на софтуера: съществени инциденти с ИКТ, причинени от софтуерни компоненти, които са несъвместими с друг софтуер или системни конфигурации, включително съществени инциденти с ИКТ, произтичащи от софтуерни конфликти, неправилни настройки или неправилно конфигурирани параметри, които оказват влияние върху цялостната функционалност на системата; д) ефективност на софтуера: съществени инциденти с ИКТ, произтичащи от софтуерни компоненти с ниска ефективност или неефективност по причини, различни от посочените в „Съвместимост/конфигурация на софтуера“, включително съществени инциденти с ИКТ, причинени от бавно време за реакция, прекомерно потребление на ресурси или неефективно изпълнение на търсения, които оказват влияние върху ефективността на софтуера или системата;				— неизправност в процеса: недостатъчно или неуспешно управление на проекти в областта на ИКТ; — неизправност в процеса: неподходящи вътрешни политики, процедури и документация; — Неизправност в процеса: неподходящо придобиване, разработване и поддържане на системи на ИКТ; — неизправност в процеса: друго (моля, уточнете); — срив в системата: капацитет и ефективност на хардуера; — срив в системата: поддръжка на хардуера; — срив в системата: остаряване/стареене на хардуера; — срив в системата: съвместимост/конфигурация на софтуера; — срив в системата: ефективност на софтуера; — срив в системата: мрежова конфигурация; — срив в системата: физическо увреждане; — срив в системата: друго (моля, уточнете); — човешка грешка: пропуск; — — човешка грешка: грешка; — човешка грешка: умения и знания; — човешка грешка: недостатъчни човешки ресурси; — човешка грешка: проблеми в комуникацията; — човешка грешка: друго (моля, уточнете); — външно събитие: природни бедствия/форсмажорни обстоятелства; — външно събитие: неизпълнени на трети страни; — външно събитие: друго (моля, уточнете).

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	е) мрежова конфигурация: съществени инциденти с ИКТ, произтичащи от неправилни или неправилно конфигурирани мрежови настройки или инфраструктура, включително съществени инциденти с ИКТ, причинени от грешки в мрежовата конфигурация, проблеми с маршрутизацията, неправилна конфигурация на защитната стена или други проблеми, свързани с мрежата, които засягат свързаността или комуникацията; ж) физическо увреждане: съществени инциденти с ИКТ, причинени от физическо увреждане на инфраструктурата на ИКТ, които водят до сривове в системата; з) друго (моля, уточнете). 4. **Човешка грешка** (ако е избрано, посочете един или повече от следните елементи): а) пропуск (непреднамерен); б) грешка; в) умения и знания: съществени инциденти с ИКТ, произтичащи от липса на експертен опит или умения за работа със системи или процеси на ИКТ, които могат да бъдат причинени от неподходящо обучение, недостатъчни знания или пропуски в уменията, необходими за изпълнение на конкретни задачи или справяне с технически предизвикателства; г) недостатъчни човешки ресурси: съществени инциденти с ИКТ, причинени от липса на необходимите ресурси, включително хардуер, софтуер, инфраструктура или персонал, и включващи ситуации, при които недостатъчните ресурси водят до оперативна неефективност, сривове в системата или невъзможност да се отговори на изискванията на стопанската дейност; д) проблеми в комуникацията; е) друго (моля, уточнете). 5. **Външно събитие** (ако е избрано, посочете един или повече от следните елементи): а) природни бедствия/форсмажорни обстоятелства; б) неизпълнение на трети страни;				

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	в) друго (моля, уточнете). Финансовите субекти следва да имат предвид, че при повтарящи се съществени инциденти с ИКТ се взема под внимание конкретната очевидна първопричина за инцидента, а не широките категории, включени в това поле.				
4.3. Допълнителна класификация на първопричините за инцидента	Допълнителна класификация на първопричините за съществения инцидент с ИКТ в рамките на вида инцидент, включително следните допълнителни категории за класифициране, свързани с подробните категории, които се докладват в полето за данни 4.2. Полето е задължително за окончателния доклад, ако в полето за данни 4.2 са докладвани специфични категории, които изискват допълнителна степен на подробност. 2(а) **Недостатъчен мониторинг или липса на мониторинг и контрол:** а) мониторинг на спазването на политиката; б) мониторинг на трети страни доставчици на услуги; в) мониторинг и проверка на отстраняването на уязвимите места; г) управление на самоличността и достъпа; д) криптиране и криптография; е) водене на регистри. 2(в) **Неизправност в процеса на управление на риска в областта на ИКТ:** а) неуспешно определяне на точните равнища на допустим риск; б) недостатъчни оценки на уязвимите места и заплахите; в) неподходящи мерки за третиране на риска; г) лошо управление на остатъчните рискове в областта на ИКТ. 2(г) **Недостатъчно или неуспешни операции в областта на ИКТ и сигурността на ИКТ:** а) управление на уязвими места и коригирането; б) управление на промените; в) управление на капацитета и ефективността; г) управление на активи в областта на ИКТ и класификация на информацията;	Не	Не	Да	Избор (от няколко възможности): — мониторинг на спазването на политиката; — мониторинг на трети страни доставчици на услуги; — мониторинг и проверка на отстраняването на уязвимите места; — управление на самоличността и достъпа; — криптиране и криптография; — водене на регистри; — неуспешно определяне на точните равнища на допустим риск; — недостатъчни оценки на уязвимите места и заплахите; — неподходящи мерки за третиране на риска; — лошо управление на остатъчните рискове в областта на ИКТ; — управление на уязвими места и софтуерни корекции; — управление на промените; — управление на капацитета и ефективността; — управление на активи в областта на ИКТ и класификация на информацията; — създаване на резервни копия и възстановяване; — обработване на грешки; — неподходящо придобиване, разработване и поддържане на системи на ИКТ; — недостатъчно или неуспешно изпитване на софтуера

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
		д) създаване на резервни копия и възстановяване; е) обработване на грешки. 2(ж) **неподходящо придобиване, разработване и поддържане на системи на ИКТ:** а) неподходящо придобиване, разработване и поддържане на системи на ИКТ; б) недостатъчно изпитване на софтуера или неуспешно изпитване на софтуера.				
4.4.	Други видове първопричини	Финансовите субекти, които са избрали „друг“ вид първопричина в полето за данни 4.2., посочват други видове първопричини	Не	Не	Да, ако в полето за данни 4.2. е избран „друг“ вид първопричини	Буквено-цифрово
4.5.	Информация за първопричините за инцидента	Описание на последователността на събитията, довели до съществения инцидент с ИКТ, и описание на начина, по който съществения инцидент с ИКТ има подобна очевидна първопричина, ако този инцидент е класифициран като повтарящ се инцидент, включително кратко описание на всички основни причини и фактори, допринесли за възникването на съществения инцидент с ИКТ. Когато е имало злонамерени действия, описание на начина на извършване на злонамереното действие, включително използваните тактики, техники и процедури, както и на входящия вектор на съществения инцидент с ИКТ, включително описание на разследванията и анализите, довели до установяване на първопричините, ако е приложимо.	Не	Не	Да	Буквено-цифрово
4.6.	Разрешаване на инцидента	Допълнителна информация относно предприетите/планираните действия/мерки за трайно разрешаване на съществения инцидент с ИКТ и за предотвратяване на повторното му възникване. Извлечени поуки от съществения инцидент с ИКТ.	Не	Не	Да	Буквено-цифрово

Поле за данни		Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
		Описанието съдържа следните точки: 1. **Описание на действията за разрешаване на инцидента** а) предприети действия за трайното разрешаване на съществения инцидент с ИКТ (с изключение на всички временни действия); б) за всяко предприето действие се посочва потенциалното участие на трета страна доставчик и на финансовия субект; в) посочва се дали процедурите са били адаптирани след съществен инцидент с ИКТ; г) посочва се всеки допълнителен контрол, който е бил въведен или който е планиран, със съответните срокове за изпълнение. Потенциални проблеми, установени по отношение на надеждността на засегнатите информационни системи/или по отношение на въведените процедури или контрол, ако е приложимо. Финансовите субекти ясно посочват как предвидените коригиращи действия ще бъдат насочени към установените първопричини и кога се очаква същественият инцидент с ИКТ да бъде трайно разрешен. 2. **Извлечени поуки** Финансовите субекти описват констатациите от прегледа след инцидента.				
4.7.	Дата и час на отстраняване на първопричината за инцидента	Дата и час на отстраняване на първопричината за инцидента.	Не	Не	Да	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДД Тчч:мм:сс)
4.8.	Дата и час на разрешаване на инцидента	Дата и час на разрешаване на инцидента.	Не	Не	Да	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДД Тчч:мм:сс)

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
4.9. Информация за това дали датата на трайното разрешаване на инцидентите се различава от първоначално планираната дата на изпълнение	Описание на причината, поради която датата на трайното разрешаване на съществените инциденти с ИКТ е различна от първоначално планираната дата на изпълнение, когато е приложимо.	Не	Не	Да	Буквено-цифрово
4.10. Оценка на риска за критичните функции за целите на разрешаването	Оценка на това дали съществуващият инцидент с ИКТ представлява риск за критичните функции по смисъла на член 2, параграф 1, точка 35 от Директива 2014/59/ЕС на Европейския парламент и на Съвета ([2]). Субектите, посочени в член 1, параграф 1 от Директива 2014/59/ЕС, посочват дали инцидентът представлява риск за критичните функции по смисъла на член 2, параграф 1, точка 35 от Директива 2014/59/ЕС, както са докладвани в образец Z07.01 от Регламент за изпълнение (ЕС) 2018/1624 на Комисията ([3]) и онагледени за конкретния субект в образец Z07.02.	Не	Не	Да, ако инцидентът представлява риск за критичните функции на финансовите субекти съгласно член 2, параграф 1, точка 35 от Директива 2014/59/ЕС.	Буквено-цифрово
4.11. Информация от значение за органите за преструктуриране	Описание на това дали съществуващият инцидент с ИКТ е повлиял на възможността за преструктуриране на субекта или групата и ако е повлиял, по какъв начин. Субектите, посочени в член 1, параграф 1 от Директива 2014/59/ЕС, предоставят информация за това дали съществуващият инцидент с ИКТ е повлиял на възможността за преструктуриране на субекта или групата и ако е повлиял, по какъв начин. Тези субекти посочват също така дали съществуващият инцидент с ИКТ засяга платежоспособността или ликвидността на финансовия субект и потенциалната количествена оценка на въздействието. Тези субекти предоставят също така информация за въздействието върху оперативната непрекъснатост, въздействието върху възможността за преструктуриране на субекта, всяко допълнително въздействие върху разходите и загубите от съществения инцидент с ИКТ, включително върху капиталовото състояние на финансовия субект, и дали договорните споразумения относно използването на услуги в областта на ИКТ все още са стабилни и напълно приложими в случай на преструктуриране на субекта.	Не	Не	Да, ако инцидентът е повлиял на възможността за преструктуриране на субекта или групата.	Буквено-цифрово

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
4.12. Прагове на същественост за критерия за класифициране „Икономическо въздействие“	Подробна информация за праговете, които евентуално е достигнал съществения инцидент с ИКТ по отношение на критерия „Икономическо въздействие“, посочен в член 7 и член 14 от Делегиран регламент (ЕС) 2024/1772.	Не	Не	Да	Буквено-цифрово
4.13. Размер на брутните преки и непреки разходи и загуби	Общ размер на брутните преки и непреки разходи и загуби, понесени от финансовия субект в резултат на съществения инцидент с ИКТ, включително: а) размера на иззетите средства или финансови активи, за които финансовият субект носи отговорност; б) размера на разходите за замяна или преместване на софтуер, хардуер или инфраструктура; в) размера на разходите за персонал, включително разходите, свързани със замяна или преместване на персонал, наемане на допълнителен персонал, възнаграждение за извънреден труд и възстановяване на загубени или нарушени умения на персонала; г) размера на таксите поради неспазване на договорни задължения; д) размера на разходите за правна защита и обезщетение на клиенти; е) размера на загубите поради пропуснати приходи; ж) размера на разходите, свързани с вътрешна и външна комуникация; з) размера на консултантските разходи, включително разходите, свързани с правни консултации, криминалистични анализи и услуги за възстановяване; и) размера на други разходи и загуби, включително: i) преки такси, включително такси за обезценка и сетълмент, в отчета за приходите и разходите и обезценявания поради съществения инцидент с ИКТ; ii) провизии или резерви, отчетени в отчета за приходите и разходите, срещу вероятни загуби, свързани със съществения инцидент с ИКТ;	Не	Не	Да	Парична стойност

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	iii) предстоящи загуби, под формата на загуби, произтичащи от съществения инцидент с ИКТ, които временно са осчетоводени в преходни или временни сметки и все още не са отразени в отчета за приходите и разходите, но които се планира да бъдат включени в рамките на период от време, съизмерим с размера и продължителността на предстоящите загуби; iv) съществени несъбрани приходи, свързани с договорни задължения с трети лица, включително решението да се предостави обезщетение на клиент след съществения инцидент с ИКТ под формата на отказ от коригиране на приходите или намаляване на договорните такси за определен бъдещ период от време, вместо да се предостави възстановяване на разходи или директно плащане; v) загуби от несвоевременност, когато те обхващат повече от една финансова счетоводна година и водят до правен риск. При своята оценка финансовите субекти вземат предвид член 7, параграфи 1 и 2 от Делегиран регламент (ЕС) 2024/1772. Финансовите субекти не включват в тази стойност финансови възстановявания от какъвто и да е вид. Финансовите субекти докладват паричната сума като положителна стойност. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, финансовите субекти вземат предвид общия размер на разходите и загубите за всички финансови субекти. Финансовите субекти докладват данните в единици с минимална точност до хиляди единици.				
4.14. Размер на финансовите възстановявания	Общ размер на финансовите възстановявания. Финансовите възстановявания се отнасят до първоначалната загуба, причинена от инцидента, независимо от момента, в който финансовите възстановявания са получени под формата на финансови средства или икономически ползи.	Не	Не	Да	Парична стойност Финансовите субекти докладват данните в единици с минимална точност до хиляди единици

Поле за данни	Описание	Задължително за първоначалното уведомление	Задължително за неокончателния доклад	Задължително за окончателния доклад	Вид на полето
	Финансовите субекти докладват паричната сума като положителна стойност. В случай на предоставяне на обобщена информация, както е посочено в член 7 от настоящия регламент, финансовите субекти вземат предвид общия размер на финансовите възстановявания за всички финансови субекти.				
4.15. Информация за това дали несъществените инциденти са били повтарящи се	Информация за това дали повече от един несъществен инцидент с ИКТ е бил повтарящ се и дали заедно се считат за съществен инцидент по смисъла на член 8, параграф 2 от Делегиран регламент (ЕС) 2024/1772. Финансовите субекти посочват дали несъществените инциденти с ИКТ са били повтарящи се и дали заедно се считат за един съществен инцидент с ИКТ. Финансовите субекти посочват и броя на случаите на тези несъществени инциденти с ИКТ.	Не	Не	Да, ако същественият инцидент се състои от повече от един несъществен повтарящ се инцидент.	Буквено-цифрово
4.16. Дата и час на възникване на повтарящи се инциденти	Когато финансовите субекти докладват за повтарящи се съществени инциденти с ИКТ, датата и часът на възникване на първия инцидент с ИКТ.	Не	Не	Да, за повтарящи се инциденти	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДД Тчч:мм:сс)

(1) 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).

(2) Директива 2014/59/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. за създаване на рамка за възстановяване и преструктуриране на кредитни институции и инвестиционни посредници и за изменение на Директива 82/891/ЕИО на Съвета и директиви 2001/24/ЕО, 2002/47/ЕО, 2004/25/ЕО, 2005/56/ЕО, 2007/36/ЕО, 2011/35/ЕС, 2012/30/ЕС и 2013/36/ЕС и на регламенти (ЕС) № 1093/2010 и (ЕС) № 648/2012 на Европейския парламент и на Съвета (ОВ L 173, 12.6.2014 г., стр. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

(3) Регламент за изпълнение (ЕС) 2018/1624 на Комисията от 23 октомври 2018 г. за определяне на технически стандарти за изпълнение по отношение на процедурите, стандартните формуляри и образците за предоставянето на информация за целите на плановете за преструктуриране на кредитни институции и инвестиционни посредници в съответствие с Директива 2014/59/ЕС на Европейския парламент и на Съвета и за отмяна на Регламент за изпълнение (ЕС) 2016/1066 на Комисията (ОВ L 277, 7.11.2018 г., стр. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ПРИЛОЖЕНИЕ III

Образци за уведомяване за значителни киберзаплахи

Номер на полето	Поле за данни	
1	Наименование на субекта, който подава уведомлението	
2	Идентификационен код на субекта, който подава уведомлението	
3	Вид на финансовия субект, който подава уведомлението	
4	Наименование на финансовия субект	
5	ИКПС на финансовия субект	
6	Име на основното лице за контакт	
7	Адрес на електронната поща на основното лице за контакт	
8	Телефон на основното лице за контакт	
9	Име на второ лице за контакт	
10	Адрес на електронната поща на второто лице за контакт	
11	Телефон на второто лице за контакт	
12	Дата и час на откриване на киберзаплахата	
13	Описание на значителната киберзаплаха	
14	Информация за потенциалното въздействие	
15	Критерии за класифициране на потенциални инциденти	
16	Състояние на киберзаплахата	
17	Предприети действия за предотвратяване на реализацията	
18	Уведомяване на други заинтересовани страни	
19	Показатели за компрометиране на системите	
20	Друга полезна информация	

ПРИЛОЖЕНИЕ IV

РЕЧНИК НА ДАННИТЕ И ИНСТРУКЦИИ ЗА УВЕДОМЯВАНЕ ЗА ЗНАЧИТЕЛНИ КИБЕРЗАПЛАХИ

Поле за данни	Описание	Задължително поле	Вид на полето
1. Наименование на субекта, който подава уведомлението	Пълно наименование на фирмата на субекта, който подава уведомлението.	Да	Буквено-цифрово
2. Идентификационен код на субекта, който подава уведомлението	Идентификационен код на субекта, който подава уведомлението. Когато финансовите субекти подават уведомлението/доклада, идентификационният код е идентификационният код на правния субект (ИКПС), който представлява уникален код от 20 буквено-цифрови знака въз основа на ISO 17442-1:2020. Когато трета страна доставчик подава доклад за финансов субект, тя може да използва идентификационен код, както е посочено в техническите стандарти за изпълнение, приети съгласно член 28, параграф 9 от Регламент (ЕС) 2022/2554.	Да	Буквено-цифрово
3. Вид на финансовия субект, който подава доклада	Вид на субекта, посочен в член 2, параграф 1, букви а)—у) от Регламент (ЕС) 2022/2554, който подава доклада.	Да, ако докладът не е предоставен директно от засегнатия финансов субект.	Избор (може да изберете повече от един елемент) — кредитна институция; — платежна институция; — освободена платежна институция; — доставчик на услуги по предоставяне на информация за сметка; — институция за електронни пари; — освободена институция за електронни пари; — инвестиционен посредник; — доставчик на услуги за криптоактиви; — емитент на токени, обезпечени с активи; — централен депозитар на ценни книжа; — централен контрагент; — място на търговия; — регистър на трансакции; — лице, управляващо алтернативен инвестиционен фонд; — управляващо дружество; — доставчик на услуги за докладване на данни;

Поле за данни		Описание	Задължително поле	Вид на полето
				— застрахователно и презастрахователно предприятие; — застрахователен посредник, презастрахователен посредник и посредник, предлагащ застрахователни продукти като допълнителна дейност; — институция за професионално пенсионно осигуряване; — агенция за кредитен рейтинг; — администратор на критични бенчмаркове; — доставчик на услуги за колективно финансиране; — регистър на секюритизации.
4.	Наименование на финансовия субект	Пълно наименование на фирмата на финансовия субект, който уведомява за значителната киберзаплаха.	Да, ако финансовият субект е различен от субекта, който подава уведомлението.	Буквено-цифрово
5.	ИКПС на финансовия субект	Идентификационен код на правния субект (ИКПС) на финансовия субект, който уведомява за значителната киберзаплаха, определен в съответствие с Международната организация по стандартизация.	Да, ако финансовият субект, който уведомява за значителната киберзаплаха, е различен от субекта, който подава доклада.	Уникален 20-буквено-цифров код въз основа на ISO 17442-1:2020.
6.	Име на основното лице за контакт	Име и фамилия на основното лице за контакт на финансовия субект.	Да	Буквено-цифрово
7.	Адрес на електронната поща на основното лице за контакт	Адрес на електронната поща на основното лице за контакт, който може да бъде използван от компетентния орган за последваща комуникация.	Да	Буквено-цифрово
8.	Телефон на основното лице за контакт	Телефонният номер на основното лице за контакт, който може да бъде използван от компетентния орган за последваща комуникация. Телефонният номер се съобщава с всички международни префикси (напр. +33XXXXXXXXX)	Да	Буквено-цифрово
9.	Име на второ лице за контакт	Име и фамилия на второто лице за контакт на финансовия субект или на субект, който подава уведомлението от името на финансовия субект, ако има такъв.	Да, ако са налични името и фамилията на второто лице за контакт на финансовия субект или на субекта, който подава уведомлението от името на финансовия субект	Буквено-цифрово

Поле за данни		Описание	Задължително поле	Вид на полето
10.	Адрес на електронната поща на второто лице за контакт	Адрес на електронната поща на второто лице за контакт или функционален адрес на електронната поща на екипа, който може да бъде използван от компетентния орган за последваща комуникация, ако има такъв.	Да, ако е наличен адрес на електронната поща на второто лице за контакт или функционален адрес на електронната поща на екипа, който може да бъде използван от компетентния орган за последваща комуникация	Буквено-цифрово
11.	Телефон на второто лице за контакт	Телефонният номер на второто лице за контакт, който може да бъде използван от компетентния орган за последваща комуникация, ако има такъв. Телефонният номер се съобщава с всички международни префикси (напр. +33XXXXXXXXX).	Да, ако е наличен телефонният номер на второто лице за контакт, който може да бъде използван от компетентния орган за последваща комуникация	Буквено-цифрово
12.	Дата и час на откриване на киберзаплахата	Дата и час на узнаване от страна на финансовия субект за значителната киберзаплаха.	Да	Стандарт ISO 8601 UTC (ГГГГ-ММ-ДД Тчч: мм:сс)
13.	Описание на значителната киберзаплаха	Описание на най-съществените аспекти на значителната киберзаплаха. Финансовите субекти предоставят: а) общ преглед на най-съществените аспекти на значителната киберзаплаха; б) свързаните рискове, произтичащи от нея, включително потенциални уязвими места на системите на финансовия субект, които може да бъдат използвани; в) информация за вероятността за реализиране на значителната киберзаплаха; както и г) информация за източника на информация относно киберзаплахата.	Да	Буквено-цифрово
14.	Информация за потенциалното въздействие	Информация за потенциалното въздействие на киберзаплахата върху финансовия субект, неговите клиенти или финансови контрагенти, ако киберзаплахата се е реализирала	Да	Буквено-цифрово
15.	Критерии за класифициране на потенциални инциденти	критериите за класифициране, които биха могли да доведат до докладване на съществен инцидент, ако киберзаплахата се е реализирала.	Да	Избор (от няколко възможности): — засегнати клиенти, финансови контрагенти и трансакции; — въздействие върху репутацията; — продължителност и прекъсване на услугата; — географски обхват; — загуби на данни; — засегнати критични услуги; — икономическо въздействие.

Поле за данни		Описание	Задължително поле	Вид на полето
16.	Състояние на киберзаплахата	Информация за състоянието на киберзаплахата за финансовия субект и дали са настъпили промени в нейната активност. Когато киберзаплахата е спряла да комуникира с информационните системи на финансовия субект, състоянието ѝ може да бъде отбелязано като неактивно. Ако финансовият субект разполага с информация, че заплахата продължава да е активна срещу други страни или финансовата система като цяло, състоянието се отбелязва като активно.	Да	Избор: — активно; — неактивно.
17.	Предприети действия за предотвратяване на реализацията	Информация на високо равнище за действията, предприети от финансовия субект за предотвратяване на реализирането на значителните киберзаплахи, ако е приложимо.	Да	Буквено-цифрово
18.	Уведомяване на други заинтересовани страни	Информация за уведомяване на други финансови субекти или органи за киберзаплахата.	Да, ако други финансови субекти или органи са били уведомени за киберзаплахата)	Буквено-цифрово
19.	Показатели за компрометиране на системите	Информация, свързана със значителната киберзаплаха, която може да помогне за идентифициране на злонамерена дейност в мрежата или информационната система (показатели за застрашена сигурност), когато е приложимо. Предоставените от финансовия субект показатели за застрашена сигурност може да включват, наред с другото, следните категории данни: а) IP адреси; б) URL адреси; в) домейни; г) хешове на файлове; д) данни за зловреден софтуер (име на зловредния софтуер, имена на файлове и тяхното местоположение, специфични ключове в регистъра, свързани с дейността на зловредния софтуер); е) данни за мрежовата активност (портове, протоколи, адреси, препратки, потребителски агенти, заглавия, специфични регистри или характерни модели в мрежовия трафик); ж) данни за съобщения на електронната поща (подател, получател, тема, заглавие, съдържание); з) DNS заявки и конфигурации на регистъра; и) дейности, свързани с потребителски профили (влизане в системата, дейности, свързани с привилегировани потребителски профили, ескалация на привилегии); й) трафик на базата данни (четене/запис), заявки към същия файл. Този вид информация може да включва данни, свързани с показатели, описващи модели в мрежовия трафик, съответстващи на известни атаки/съобщения от бот мрежи, IP адреси на машини, заразени със зловреден софтуер (ботове), данни, свързани със сървъри за управление и контрол, използвани от зловреден софтуер (обикновено домейни или IP адреси), и URL адреси, свързани с наблюдавани фишинг сайтове или уебсайтове, които хостват зловреден софтуер или комплекти с експлойти.	Да, ако е налична информация за показатели за компрометиране на системите, свързани с киберзаплахата)	Буквено-цифрово
20.	Друга полезна информация	Всяка друга полезна информация за значителната киберзаплаха	Да, ако е приложимо и ако има друга налична информация, която не е включена в образеца.	Буквено-цифрово