РЕШЕНИЕ (ЕС) 2021/1486 НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА

от 7 септември 2021 година за приемане на вътрешни правила относно ограниченията на правата на субектите на данни във връзка със задачите на Европейската централна банка, свързани с пруденциалния надзор над кредитните институции

(ЕЦБ/2021/42)

ИЗПЪЛНИТЕЛНИЯТ СЪВЕТ НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Устава на Европейската система на централните банки и на Европейската централна банка, и по-специално член 11.6 от него,

като взе предвид 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 ([1]), и по-специално член 25 от него,

като има предвид, че:

(1) Европейската централна банка (ЕЦБ) изпълнява задачите си в съответствие с Договорите и Регламент (ЕС) № 1024/2013 на Съвета ([2]).

(2) Съгласно член 45, параграф 3 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета в Решение (ЕС) 2020/655 на Европейската централна банка (ЕЦБ/2020/28) ([3]) се съдържат общите правила за прилагане на Регламент (ЕС) 2018/1725 в ЕЦБ. В частност то съдържа правилата за назначаването и функциите на длъжностното лице по защита на данните (ДЛЗД), включително задачите, задълженията и правомощията му.

(3) При изпълнението на възложените ѝ задачи ЕЦБ и по-специално съответното организационно звено действа като администратор на данни, доколкото определя, самостоятелно или съвместно с други, целите и средствата за обработването на лични данни.

(4) Съгласно член 4, параграф 1 от Регламент (ЕС) № 1024/2013 за целите на надзора и с оглед на гарантирането на сигурността и стабилността на кредитните институции и стабилността на финансовата система ЕЦБ има изключителната компетентност да извършва конкретни задачи във връзка с всички кредитни институции, установени в държавите членки, участващи в единния надзорен механизъм (ЕНМ).

(5) При изпълнението на тези конкретни задачи ЕЦБ обработва няколко категории информация, които може да са свързани с физическо лице, което е идентифицирано или може да бъде идентифицирано, като например данни за установяване на самоличността, данни за връзка, професионални данни, финансови или административни данни, данни, получени от специфични източници, данни за електронни съобщения и данни за електронния трафик, данни от регистрите за съдимост, описание на финансовите и нефинансовите интереси, данни за отношенията на дадено физическо лице или близките му роднини с поднадзорните лица или с членовете на ръководния орган на поднадзорните лица, както и данни, свързани с длъжността, на която е назначено или може да бъде назначено лицето. Личните данни могат също да са част от оценка, включително оценка, извършвана: за целите на лицензирането на кредитна институция, отнемането на лицензa на кредитна институция и процедура за квалифицирано дялово участие; във връзка с правото на установяване за значимо поднадзорно лице; за определяне дали са изпълнени изискванията за надеждност и пригодност; във връзка с политиките за възнагражденията на значимо поднадзорно лице и по отношение на кредитите от такова лице към собствените му висши длъжностни лица и лица, свързани с тези длъжностни лица; и във връзка с твърдения за потенциално неизпълнение на правните актове, посочени в член 4, параграф 3 от Регламент (ЕС) № 1024/2013.

([1]) ОВ L 295, 21.11.2018 г., стр. 39.

([2]) Регламент (ЕС) № 1024/2013 на Съвета от 15 октомври 2013 г. за възлагане на Европейската централна банка на конкретни задачи относно политиките, свързани с пруденциалния надзор над кредитните институции (ОВ L 287, 29.10.2013 г., стр. 63).

([3]) Решение (ЕС) 2020/655 на Европейската централна банка от 5 май 2020 г. за приемане на правила за прилагане във връзка със защитата на данни в Европейската централна банка и за отмяна на Решение ЕЦБ/2007/1 (ОВ L 152, 15.5.2020 г., стр. 13).

(6) При изпълнението на тези конкретни задачите ЕЦБ се стреми да постигне важни цели от общ обществен интерес на Съюза. Поради тази причина изпълнението на тези задачи следва да бъде гарантирано, както е предвидено в Регламент (ЕС) 2018/1725, и по-специално в член 25, параграф 1, букви в) и ж) от него. По-специално при изпълнението на тези задачи ЕЦБ действа в общия обществен интерес на Съюза като публичен орган, на който е възложено да извършва за целите на надзора конкретни задачи във връзка с всички кредитни институции, установени в държавите членки, участващи в ЕНМ. Тези задачи включват функции по наблюдение, проверка или регулиране, свързани с упражняването на правомощия за пруденциален надзор над кредитните институции.

(7) В този контекст е целесъобразно да се уточнят основанията, на които ЕЦБ може да ограничи правата на субектите на данни във връзка с данните, получени при изпълнението на надзорните ѝ задачи съгласно Регламент (ЕС) № 1024/2013.

(8) В съответствие с член 25, параграф 1 от Регламент (ЕС) 2018/1725 ограниченията на прилагането на членове 14—22, 35 и 36, както и на член 4, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—22 от същия регламент, следва да бъдат определени във вътрешни правила или правни актове, приети въз основа на Договорите. Поради това ЕЦБ следва да определи правилата, съгласно които може да ограничава правата на субектите на данни при изпълнението на надзорните си задачи.

(9) Макар че с настоящото решение се определят правилата, съгласно които ЕЦБ може да ограничава правата на субектите на данни при изпълнението на надзорните си задачи, Изпълнителният съвет възнамерява да приеме отделно решение за приемане на вътрешни правила относно ограничаването на тези права, когато ЕЦБ обработва лични данни във връзка с вътрешната си дейност.

(10) ЕЦБ може да прилага изключения в съответствие с Регламент (ЕС) 2018/1725, което обезсмисля необходимостта от прилагането на ограничения, включително по-специално предвидените в член 15, параграф 4, член 16, параграф 5, член 19, параграф 3 и член 35, параграф 3 от посочения регламент. За обработването на данни за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели ЕЦБ може да прилага изключението, посочено в член 16, параграф 5, буква б) или в член 19, параграф 3, буква г) от Регламент (ЕС) 2018/1725.

(11) Упражняването на правата на субектите на данни, уредени в членове 17, 18, 20, 21, 22 и 23 от Регламент (ЕС) 2018/1725, може да направи невъзможно или сериозно да затрудни постигането на конкретни целите на обработването, включително целите на архивирането в обществен интерес, целите на научните или историческите изследвания и статистическите цели. Поради това с настоящото решение следва да се предвиди дерогация от тези права съгласно член 25, параграфи 3 и 4 от Регламент (ЕС) 2018/1725, като се предвидят подходящи гаранции.

(12) ЕЦБ следва да обоснове защо подобни ограничения на правата на субектите на данни са строго необходими и пропорционални в едно демократично общество, за да се гарантират преследваните цели при упражняването на правомощията ѝ и свързаните с тях функции, както и как ЕЦБ зачита същността на основните права и свободи, като същевременно налага такива ограничения.

(13) В тази рамка ЕЦБ е задължена да зачита във възможно най-голяма степен предвидените в Регламент (ЕС) 2018/1725 основни права на субектите на данни, по-специално правата, свързани с правото на предоставяне на информация, достъп и коригиране, правото на изтриване, ограничаване на обработването, правото на съобщаване на субекта на данните за нарушение на сигурността на личните данни или поверителността на съобщенията.

(14) ЕЦБ обаче може да бъде задължена да ограничи информацията, предоставяна на субектите на данни, и техните права, за да защити изпълнението на надзорните си задачи, по-специално собствените си разследвания и процедури, разследванията и процедурите на други публични органи и основните права и свободи на други лица, свързани с нейните разследвания или други процедури.

(15) ЕЦБ следва да отмени ограничението, което вече е било наложено, доколкото то вече не е необходимо.

(16) ДЛЗД на ЕЦБ следва да преразгледа прилагането на ограниченията, за да гарантира спазването на настоящото решение и на Регламент (ЕС) 2018/1725.

(17) В съответствие с член 41, параграф 2 от Регламент (ЕС) 2018/1725 беше проведена консултация с Европейския надзорен орган по защита на данните, който прие становище на 12 март 2021 г.,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Предмет и приложно поле

1. С настоящото решение се определят правилата, свързани с ограничаването на правата на субектите на данни от ЕЦБ, когато тя извършва дейностите по обработване на лични данни, вписани в централния регистър, при изпълнението на надзорните си задачи съгласно Регламент (ЕС) № 1024/2013.

2. Правата на субектите на данни, които могат да бъдат ограничавани, са уредени в следните членове от Регламент (ЕС) 2018/1725:

а) член 14 (прозрачна информация, комуникация и условия за упражняването на правата на субекта на данните);

б) член 15 (информация, която се предоставя, когато от субекта на данните се събират лични данни);

в) член 16 (информация, която се предоставя, когато личните данни не са получени от субекта на данните);

г) член 17 (право на достъп на субекта на данните);

д) член 18 (право на коригиране);

е) член 19 (право на изтриване – „право да бъдеш забравен“);

ж) член 20 (право на ограничаване на обработването);

з) член 21 (задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването);

и) член 22 (право на преносимост на данните);

й) член 35 (съобщаване на субекта на данните за нарушение на сигурността на личните данни);

к) член 36 (поверителност на електронните съобщения);

л) член 4, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—22 от Регламент (ЕС) 2018/1725.

Член 2

Определения

За целите на настоящото решение се прилагат следните определения:

1) „обработване“ означава обработване съгласно определението в член 3, точка 3 от Регламент (ЕС) 2018/1725;

2) „лични данни“ означава лични данни съгласно определението в член 3, точка 1 от Регламент (ЕС) 2018/1725;

3) „субект на данни“ означава физическо лице, което е идентифицирано или може да бъде идентифицирано; физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождението, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, икономическата, културната или социалната идентичност на това физическо лице;

4) „централен регистър“ означава публично достъпното хранилище на всички дейности по обработване на лични данни, извършени в ЕЦБ, поддържано от ДЛЗД на ЕЦБ и предвидено в член 9 от Решение (ЕС) 2020/655 (ЕЦБ/2020/28);

5) „администратор“ означава ЕЦБ и по-специално компетентното организационно звено на ЕЦБ, което самостоятелно или съвместно с други, определя целите и средствата на обработването на лични данни и отговаря за операцията по обработването;

6) „институции и органи на Съюза“ означава институции и органи на Съюза съгласно определението в член 3, точка 10 от Регламент (ЕС) 2018/1725.

Член 3

Прилагане на ограниченията

1. Администраторът може да ограничи правата, посочени в член 1, параграф 2, за да гарантира интересите и целите, посочени в член 25, параграф 1 от Регламент (ЕС) 2018/1725, по-специално когато упражняването на тези права би застрашило или би засегнало неблагоприятно:

а) изпълнението на надзорните задачи на ЕЦБ съгласно Регламент (ЕС) № 1024/2013, включително правилното функциониране на системата за надзор;

б) сигурността и стабилността на кредитните институции и стабилността на финансовата система в рамките на Съюза и на всяка държава членка;

в) ефективността на съобщаването за нарушения съгласно член 23 от Регламент (ЕС) № 1024/2013;

2. За да гарантира интересите и целите, посочени в член 25, параграф 1 от Регламент (ЕС) 2018/1725, администраторът може да ограничи правата, посочени в член 1, параграф 2, по отношение на личните данни, получени от други институции и органи на Съюза, от компетентните органи на държавите членки или на трети държави или от международни организации, в следните случаи:

а) когато упражняването на тези права може да бъде ограничено от други институции и органи на Съюза, от които са получени личните данни, или въз основа на други актове, предвидени в член 25 от Регламент (ЕС) 2018/1725, или в съответствие с глава IX от Регламент (ЕС) 2018/1725, или в съответствие с учредителните актове на други институции и органи на Съюза;

б) когато упражняването на тези права може да бъде ограничено от компетентните органи на държавите членки, от които са получени личните данни, въз основа на актовете, посочени в член 23 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([4]), или съгласно националните мерки за транспониране на член 13, параграф 3, член 15, параграф 3 или член 16, параграф 3 от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета ([5]);

в) когато упражняването на тези права би могло да застраши или да засегне неблагоприятно сътрудничеството на ЕЦБ с трети държави или международни организации, от които е получена информацията, при изпълнението на нейните задачи, освен ако интересите или основните права и свободи на субектите на данни надделяват над интереса на ЕЦБ от сътрудничество.

([4]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

([5]) Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

3. Преди да приложи ограничение в случаите, посочени в параграф 2, букви а) и б), администраторът:

а) се осведомява за договореностите, сключени със съответните институции и органи на Съюза или с компетентните органи на държавите членки; и

б) провежда консултации със съответните институции и органи на Съюза или с компетентните органи на държавите членки, освен ако за него е ясно, че прилагането на това ограничение е предвидено в някой от актовете или мерките, посочени в параграф 2, букви а) и б).

4. Администраторът може да прилага ограничение само когато въз основа на оценка на всеки отделен случай стигне до заключението, че ограничението:

а) е необходимо и пропорционално, като се вземат предвид рисковете за правата и свободите на субекта на данните; и

б) е съобразено със същността на основните права и свободи в едно демократично общество.

5. Администраторът документира своята оценка във вътрешна бележка за оценка, която включва правното основание, причините за ограничението, ограничените права на субектите на данните, засегнатите субекти на данни, необходимостта и пропорционалността на ограничението и вероятната продължителност на ограничението.

6. Решението на администратора за ограничаване на правата на субект на данни съгласно настоящото решение се взема на равнището на съответния ръководител или заместник-ръководител на структурното звено, в чиято сфера на дейност се извършва основната операция по обработване, включваща личните данни.

Член 4

Дерогации

1. За обработването на данни за целите на научни или исторически изследвания или за статистически цели администраторът може да прилага дерогации в съответствие с член 25, параграф 3 от Регламент (ЕС) 2018/1725. За тази цел администраторът може да прилага дерогация от правата, посочени в членове 17, 18, 20 и 23 от Регламент (ЕС) 2018/1725, в съответствие с условията, предвидени в член 25, параграф 3 от същия регламент.

2. За обработването на данни за целите на архивирането в обществен интерес, администраторът може да прилага дерогации в съответствие с член 25, параграф 4 от Регламент (ЕС) 2018/1725. За тази цел администраторът може да прилага дерогация от правата, посочени в членове 17, 18, 20, 21, 22 и 23 от Регламент (ЕС) 2018/1725, в съответствие с условията, предвидени в член 25, параграф 4 от същия регламент.

3. За тези дерогации се прилагат подходящи гаранции в съответствие с член 13 от Регламент (ЕС) 2018/1725 и член 8 от настоящото решение.

Член 5

Предоставяне на обща информация относно ограниченията

Администраторът предоставя обща информация относно потенциалното ограничаване на правата на субектите на данни, както следва:

а) администраторът посочва правата, които могат да бъдат ограничени, причините за ограничението и потенциалната му продължителност;

б) администраторът включва информацията, посочена в буква а), в своите съобщения за защита на данните, декларации за поверителност и регистри на дейностите по обработване, предвидени в член 31 от Регламент (ЕС) 2018/1725.

Член 6

Ограничаване на правото на достъп на субектите на данни, правото на коригиране, правото на изтриване или правото на ограничаване на обработването

1. Когато администраторът ограничава изцяло или частично правото на достъп, правото на коригиране, правото на изтриване или правото на ограничаване на обработването, посочени съответно в член 17, член 18, член 19, параграф 1 и член 20, параграф 1 от Регламент (ЕС) 2018/1725, в срока, посочен в член 11, параграф 5 от Решение (ЕС) 2020/655 (ЕЦБ/2020/28), той информира съответния субект на данни в своя писмен отговор на искането му за наложеното ограничение, за основните мотиви за ограничението и за възможността да подаде жалба до Европейския надзорен орган по защита на данните или да потърси съдебна защита пред Съда на Европейския съюз.

2. Администраторът съхранява вътрешната бележка за оценката, посочена в член 3, параграф 5, и когато е приложимо, документите, съдържащи основните фактически и правни елементи, и ги предоставя на Европейския надзорен орган по защита на данните при поискване.

3. Администраторът може да отложи, пропусне или откаже предоставянето на информация за мотивите за ограничението, посочени в параграф 1, ако предоставянето на тази информация би възпрепятствало постигането на целта на ограничението. Веднага след като установи, че предоставянето на информацията вече не възпрепятства постигането на целта на ограничението, администраторът предоставя тази информация на субекта на данните.

Член 7

Продължителност на ограниченията

1. Администраторът отменя ограничението веднага щом обосновалите го обстоятелства престанат да са налице.

2. Когато отмени ограничение съгласно параграф 1, администраторът незабавно:

а) доколкото все още не е направил това, информира субекта на данните за основните причини, на които се основава прилагането на ограничение;

б) информира субекта на данните за правото му да подаде жалба до Европейския надзорен орган по защита на данните или да потърси съдебна защита пред Съда на Европейския съюз;

в) предоставя на субекта на данните правото, което е било предмет на отменения ограничение;

3. На всеки шест месеца администраторът прави преоценка на необходимостта от поддържането на ограничение, наложено съгласно настоящото решение, и документира повторната си оценка във вътрешна бележка за оценка.

Член 8

Гаранции

ЕЦБ прилага организационни и технически гаранции, както е посочено в приложението, за предотвратяване на злоупотреби и на неправомерен достъп или прехвърляне.

Член 9

Преглед от длъжностното лице по защита на данните

1. Когато администраторът ограничава прилагането на правата на субекта на данни, през цялото време той трябва да работи с ДЛЗД. По-специално се прилага следното:

а) администраторът се консултира без ненужна забава с ДЛЗД;

б) по искане на ДЛЗД администраторът му предоставя достъп до всички документи, съдържащи основните фактически и правни елементи, включително вътрешната бележка за оценка, посочена в член 3, параграф 5;

в) администраторът документира как е участвало ДЛЗД, включително относимата информация, която е била обменена, по-специално датата на първата консултация, посочена в буква а);

г) ДЛЗД може да поиска от администратора да преразгледа ограничението;

д) администраторът информира в писмен вид ДЛЗД за резултата от поискания преглед без ненужно забавяне и при всички случаи преди прилагането на ограничението.

2. Администраторът уведомява ДЛЗД, когато ограничението бъде отменено.

Член 10

Влизане в сила

Настоящото решение влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

Съставено във Франкфурт на Майн на 7 септември 2021 година.

Председател на ЕЦБ
Christine LAGARDE

ПРИЛОЖЕНИЕ

Организационните и технически гаранции в ЕЦБ за предотвратяване на злоупотреби и на неправомерен достъп или прехвърляне включват:

а) по отношение на лицата:

i) всички лица, които имат достъп до непублична информация на ЕЦБ, носят отговорност за познаването и прилагането на политиката и правилата на ЕЦБ за управлението и поверителността на информацията;

ii) процедура за разрешение на достъпа, която гарантира, че само проверени и упълномощени лица имат достъп до помещенията на ЕЦБ и до нейната непублична информация;

iii) информационно-технологични мерки, информационни мерки и мерки за повишаване на осведомеността за физическата сигурност;

iv) обучения, които се провеждат редовно за членовете на персонала и външните доставчици на услуги;

v) по отношение на членовете на персонала на ЕЦБ се прилагат строги правила за професионална тайна, определени в Условията за работа и Правилата за персонала на ЕЦБ, чието нарушаване води до дисциплинарни санкции

vi) правила и задължения, уреждащи достъпа на външни доставчици на услуги или изпълнители на договори до непублична информация на ЕЦБ, които са определени в договорни споразумения;

vii) контрол на достъпа, включително зониране за сигурност, които се прилагат, като се гарантира, че достъпът на лица до непублична информация на ЕЦБ е разрешен и ограничен въз основа на оперативните нужди и изискванията за сигурност;

б) по отношение на процесите:

i) наличие на процеси за осигуряване на контролирано внедряване, експлоатация и поддръжка на ИТ приложенията, които подпомагат дейността на ЕЦБ;

ii) използване на ИТ приложения за дейността на ЕЦБ, които отговарят на стандартите за сигурност на ЕЦБ;

iii) наличие на всеобхватна програма за физическа сигурност, чрез която постоянно оценяват заплахите за сигурността и която включва мерки за физическа сигурност, за да се гарантира адекватно ниво на защита;

в) по отношение на технологиите:

i) всички електронни данни се съхраняват в ИТ приложения, отговарящи на стандартите за сигурност на ЕЦБ, и по този начин са защитени срещу неразрешен достъп или промяна;

ii) ИТ приложенията се внедряват, експлоатират и поддържат при ниво на сигурност, съответстващо на изискванията за поверителност, цялост и наличност на ИТ приложенията, които се основават на анализи на въздействието върху дейността;

iii) нивото на сигурност на ИТ приложенията редовно се проверява чрез технически и нетехнически оценки на сигурността;

iv) достъпът до непублична информация на ЕЦБ се предоставя в съответствие с принципа „необходимост да се знае“, а привилегированият достъп е строго ограничен и строго контролиран;

v) осъществяване на контрол за откриване и проследяване на действителни и потенциални нарушения на сигурността.