РЕШЕНИЕ (ЕС) 2021/2243 НА КОМИСИЯТА

от 15 декември 2021 година

за определяне на вътрешните правила по отношение на предоставянето на информация на субектите на данни и ограничаването на някои от техните права в контекста на обработването на лични данни за целите на сигурността на информационните и комуникационните системи на Комисията

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 249, параграф 1 от него,

като има предвид, че:

(1) При изпълнението на своите задачи Комисията е длъжна да зачита правата на физическите лица по отношение на обработването на лични данни, признати в член 8, параграф 1 от Хартата на основните права на Европейския съюз и в член 16, параграф 1 от Договора за функционирането на Европейския съюз. Тя трябва също така да зачита правата, предвидени в Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([1]). Същевременно Комисията трябва да управлява инцидентите, свързани с информационната сигурност, в съответствие с правилата, установени в член 15 от Решение (ЕС, Евратом) 2017/46 ([2]).

(2) За да се гарантира информационната сигурност, т.е. опазването на поверителността, целостта и наличността на комуникационните и информационните системи и на обработваните от тях данни, по отношение на лицата, активите и информацията, Комисията, по-специално чрез своята Генерална дирекция „Информатика“, предприе мерки съгласно предвиденото в Решение (ЕС, Евратом) 2017/46 и в Решение C(2017) 8841 final ([3]). Тези мерки включват наблюдение на рисковете за информационната сигурност и на приложените мерки за информационна сигурност, изискване от отговорниците на системи да вземат конкретни мерки за информационна сигурност с оглед на ограничаването на рисковете за информационната сигурност на комуникационните и информационните системи на Комисията и управление на инциденти, свързани с информационната сигурност.

(3) Генерална дирекция „Информатика“ предоставя на Комисията операции и услуги за информационна сигурност и трябва да обработва няколко категории лични данни, за да:

— докладва сигнали и предупреждения във връзка със събития и инциденти, свързани с информационната сигурност;

— реагира и ограничава събития и инциденти, свързани с информационната сигурност;

— улеснява използването на инструменти и операции чрез одити на сигурността, оценки на сигурността и управление на уязвимостите;

— повишава осведомеността на персонала на Комисията в областта на киберсигурността;

— наблюдава, разкрива и предотвратява възникването на събития и инциденти, свързани с информационната сигурност;

— преразглежда профилите на привилегированите потребители.

(4) Инциденти, свързани с информационната сигурност, които биха могли да подкопаят сигурността на информационните и комуникационните системи на Комисията, могат да възникнат при всяка операция по обработване, която осъществява Комисията. Те могат да включват всяка категория лични данни, обработвани от Комисията.

([1]) 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).

([2]) Решение (ЕС, Евратом) 2017/46 на Комисията от 10 януари 2017 г. относно сигурността на комуникационните и информационните системи в Европейската комисия (ОВ L 6, 11.1.2017 г., стр. 40).

([3]) Решение (C(2017) 8841) на Комисията от 13 декември 2017 г. за определяне на правила за прилагане на членове 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 от Решение 2017/46 на Комисията относно сигурността на комуникационните и информационните системи в Комисията.

(5) При определени обстоятелства може да е необходимо правата на субектите на данни съгласно Регламент (ЕС) 2018/1725 да се съгласуват с необходимостта Комисията да извършва ефективно задачите си за гарантиране на информационната сигурност на лицата, активите и информацията в Комисията съгласно Решение (ЕС, Евратом) 2017/46 и при пълно зачитане на основните права и свободи на други субекти на данни. За тази цел с член 25, параграф 1 от Регламент (ЕС) 2018/1725 Комисията бе оправомощена да ограничава прилагането на членове 14—17, 19, 20 и 35 от същия регламент и на принципа на прозрачност, установен в член 4, параграф 1, буква а) от него, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—17, 19 и 20 от посочения регламент.

(6) Настоящото решение следва да се прилага за всички операции по обработване, които осъществява Комисията в качеството си на администратор на лични данни при изпълнението на своите задачи да гарантира информационната сигурност на лицата, активите и информацията в Комисията съгласно Решение (ЕС, Евратом) 2017/46. Поради това то следва да се отнася до субектите на данни от категориите лични данни, обхванати от всички тези операции по обработване, т.е. физическите лица, които взаимодействат с някоя от информационните и комуникационните системи на Комисията.

(7) Личните данни се съхраняват в сигурна електронна среда, за да се предотврати незаконосъобразният достъп на лица извън Комисията. За различните операции по обработване се прилагат различни срокове на съхранение на данните в зависимост от вида на съответните лични данни. Съхранението на преписки от Комисията се урежда с общия за Комисията списък за съхранение на преписки (SEC(2019) 900), регулаторен документ под формата на таблица за съхранението, в който се определят сроковете на съхранение на различните видове преписки на Комисията, за да се ограничи съхраняването на данни до границите на необходимото.

(8) Може да се наложи Комисията да ограничи прилагането на правата на субектите на данни, за да защити вътрешната си сигурност съгласно член 25, параграф 1, буква г) от Регламент (ЕС) 2018/1725 (т.е. да запази поверителността, целостта и наличността на своите комуникационни и информационни системи и на обработваните от тях набори от данни, своите активи и информация). По-специално може да се наложи Комисията да направи това, когато:

— докладва сигнали и предупреждения във връзка със събития и инциденти, свързани с информационната сигурност;

— реагира и ограничава събития и инциденти, свързани с информационната сигурност; улеснява използването на инструменти и операции чрез одити на сигурността, оценки на сигурността и управление на уязвимостите;

— повишава осведомеността на персонала на Комисията в областта на киберсигурността;

— наблюдава, разкрива и предотвратява възникването на събития и инциденти, свързани с информационната сигурност;

— преразглежда профилите на привилегированите потребители.

(9) За целите на управлението на инцидентите, свързани с информационната сигурност, както е посочено в член 15 от Решение (ЕС, Евратом) 2017/46, Генерална дирекция „Информатика“ може да обменя информация с Екипа за реакция при кибератаки на Генерална дирекция „Човешки ресурси и сигурност“.

(10) За да спази членове 14, 15 и 16 от Регламент (ЕС) 2018/1725, Комисията следва да информира всички физически лица за дейностите, които включват обработването на личните им данни и които засягат техните права. Тя следва да направи това по прозрачен и последователен начин, като публикува съобщение за защита на личните данни на уебсайта на Комисията. Когато е уместно, тя следва да прилага допълнителни гаранции, за да информира субектите на данни индивидуално в подходяща форма.

(11) Спазването на членове 14, 15 и 16 от Регламент (ЕС) 2018/1725 би могло да разкрие наличието на мерки, слабости или инциденти, свързани с информационната сигурност, предприети или възникнали по силата на член 15 от Решение (ЕС, Евратом) 2017/46. Разкриването на тези мерки, слабости или инциденти, свързани с информационната сигурност, увеличава риска от заобикаляне на разкритата мярка за информационна сигурност, от злоупотреба с разкритата слабост и от възпрепятстване на текущия анализ на инцидента, свързан с информационната сигурност, поради възможността за случайно или умишлено манипулиране от потребител или злонамерен участник. Това би могло сериозно да накърни способността на Комисията да гарантира своята информационна сигурност и по-специално да управлява ефективно инцидентите, свързани с информационната сигурност, в бъдеще.

(12) Съгласно член 25, параграф 1, буква з) от Регламент (ЕС) 2018/1725 Комисията е оправомощена също така да ограничава прилагането на правата на субектите на данни с цел защита на правата и свободите на други физически лица във връзка с инциденти, свързани с информационната сигурност, които биха могли да застрашат операциите за информационна сигурност.

(13) Възможно е на Комисията да се наложи да ограничи предоставянето на информация на субектите на данни и прилагането на други права на субектите на данни във връзка с лични данни, получени от държави извън ЕС или международни организации, за да изпълни задължението си за сътрудничество с тези държави или организации. Това е част от задължението на Комисията да защитава важна цел от широк обществен интерес на ЕС, както е посочено в член 25, параграф 1, буква в) от Регламент (ЕС) 2018/1725. При някои обстоятелства обаче интересите, произтичащи от основните права на субекта на данните, могат да надделеят над интересите на международното сътрудничество.

(14) Поради това Комисията определи основанията, изброени в член 25, параграф 1, букви в), г) и з) от Регламент (ЕС) 2018/1725, като основания за ограничения, които може да е необходимо да се приложат във връзка с провежданите от Генерална дирекция „Информатика“ операции по обработването на данни, свързани с предоставянето на операции и услуги за информационната сигурност на Комисията.

(15) Всяко ограничение, приложено съгласно настоящото решение, следва да бъде необходимо и пропорционално, като се вземат предвид рисковете по отношение на правата и свободите на субектите на данни.

(16) Комисията следва да борави с всички ограничения по прозрачен начин и да регистрира всяко прилагане на ограничения в съответния регистър.

(17) Съгласно член 25, параграф 8 от Регламент (ЕС) 2018/1725 администраторите на лични данни могат да отложат, пропуснат или откажат да предоставят информация на субекта на данните относно причините за прилагането на ограничение, ако предоставянето на тази информация би възпрепятствало по някакъв начин ефекта от ограничението. Това се отнася по-специално за ограниченията на задълженията, предвидени в членове 16 и 35 от Регламент (ЕС) 2018/1725. Комисията следва редовно да извършва преглед на наложените ограничения, за да гарантира, че правата на субекта на данни да бъде информиран в съответствие с членове 16 и 35 от Регламент (ЕС) 2018/1725 са ограничени само доколкото тези ограничения са необходими, за да се даде възможност на Комисията да осигури своята информационна сигурност и по-специално да управлява инциденти, свързани с информационната сигурност.

(18) Когато Комисията ограничава прилагането на права на субектите на данни, различни от посочените в членове 16 и 35 от Регламент (ЕС) 2018/1725, администраторът на лични данни следва да преценява за всеки отделен случай дали съобщаването на ограничението би възпрепятствало неговата цел.

(19) Длъжностното лице по защита на данните към Комисията следва да извършва независим преглед на прилагането на ограниченията с цел да се осигури постигането на съответствие с настоящото решение.

(20) За да може Комисията незабавно да ограничи прилагането на определени права и задължения в съответствие с член 25 от Регламент (ЕС) 2018/1725, настоящото решение следва да влезе в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

(21) Европейският надзорен орган по защита на данните издаде становище на 16 септември 2021 г.,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Предмет и обхват

1. С настоящото решение се определят правилата, които Комисията трябва да спазва, когато информира субектите на данни относно обработването на техните лични данни в съответствие с членове 14, 15 и 16 от Регламент (ЕС) 2018/1725 при изпълнение на своите задачи в съответствие с Решение (ЕС, Евратом) 2017/46.

В него се определят също условията, при които Комисията може да ограничи прилагането на членове 4, 14—17, 19, 20 и 35 от Регламент (ЕС) 2018/1725 в съответствие с член 25, параграф 1, букви в), г) и з) от посочения регламент при изпълнение на своите задачи в съответствие с Решение (ЕС, Евратом) 2017/46.

2. Настоящото решение се прилага за обработването на лични данни от Комисията или от нейно име за целите на или във връзка с дейностите, осъществявани за гарантиране на информационната сигурност на лицата, активите и информацията в Комисията съгласно Решение (ЕС, Евратом) 2017/46.

Член 2

Приложими изключения и ограничения

1. Когато Комисията изпълнява задълженията си по отношение на правата на субектите на данни съгласно Регламент (ЕС) 2018/1725, тя преценява дали се прилага някое от изключенията, предвидени в посочения регламент.

2. При спазване на членове 3—7 от настоящото решение, когато упражняването на правата и задълженията, предвидени в членове 14—17, 19, 20 и 35 от Регламент (ЕС) 2018/1725, във връзка с лични данни, обработвани от Комисията, би възпрепятствало целите на предоставяне на операции и услуги за информационната сигурност наред с другото чрез разкриване на инструментите, слабостите и методите за разследване на Комисията или би оказало неблагоприятно въздействие върху правата и свободите и сигурността на други субекти на данни, по-специално при обработването на лични данни с цел:

— докладване на сигнали и предупреждения във връзка със събития и инциденти, свързани с информационната сигурност;

— реагиране и ограничаване на събития и инциденти, свързани с информационната сигурност;

— улесняване на използването на инструменти и операции чрез одити на сигурността, оценки на сигурността и управление на уязвимостите;

— повишаване на осведомеността на персонала на Комисията в областта на киберсигурността;

— наблюдаване, разкриване и предотвратяване на възникването на събития и инциденти, свързани с информационната сигурност;

— преразглеждане на профилите на привилегированите потребители,

Комисията може да ограничи прилагането на:

а) членове 14—17, 19, 20 и 35 от Регламент (ЕС) 2018/1725;

б) принципа на прозрачност, определен в член 4, параграф 1, буква а) от Регламент (ЕС) 2018/1725, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—17, 19 и 20 от Регламент (ЕС) 2018/1725.

Комисията може да направи това в съответствие с член 25, параграф 1, букви в), г) и з) от Регламент (ЕС) 2018/1725.

3. При спазване на разпоредбите на членове 3—7 Комисията може да ограничи правата и задълженията, посочени в параграф 2 от настоящия член:

а) когато упражняването на тези права и задължения по отношение на личните данни, получени от друга институция, орган, агенция или служба на ЕС, може да бъде ограничено от тази друга институция, орган, агенция или служба на ЕС въз основа на правните актове, предвидени в член 25 от Регламент (ЕС) 2018/1725, или в съответствие с глава IX от същия регламент, с Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета ([4]) или с Регламент (ЕС) 2017/1939 на Съвета ([5]);

б) когато упражняването на тези права и задължения по отношение на личните данни, получени от компетентния орган на държава членка, може да бъде ограничено от компетентните органи на тази държава членка въз основа на законодателните мерки, посочени в член 23 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([6]), 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 ([7]);

([4]) Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и за замяна и отмяна на решения 2009/371/ПВР, 2009/934/ПВР, 2009/935/ПВР, 2009/936/ПВР и 2009/968/ПВР на Съвета (ОВ L 135, 24.5.2016 г., стр. 53).

([5]) Регламент (ЕС) 2017/1939 на Съвета от 12 октомври 2017 г. за установяване на засилено сътрудничество за създаване на Европейска прокуратура (ОВ L 283, 31.10.2017 г., стр. 1).

([6]) 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).

([7]) 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).

в) когато упражняването на тези права и задължения би възпрепятствало сътрудничеството на Комисията с държави извън ЕС или международни организации във връзка с общи заплахи за киберсигурността.

Преди да наложи ограничения при обстоятелствата, посочени в първа алинея, букви а) и б), Комисията се консултира със съответните институции, органи, агенции, служби на ЕС или органи на държавите членки относно потенциалните основания за налагане на ограничения, както и относно необходимостта и пропорционалността на съответните ограничения, освен ако това не би възпрепятствало дейностите на Комисията и освен ако за Комисията не е ясно, че прилагането на ограничение е предвидено в някой от актовете, посочени в тези букви, или че тази консултация би възпрепятствала целите на нейните дейности съгласно Решение (ЕС, Евратом) 2017/46.

Първа алинея, буква в) не се прилага, когато интересите или основните права и свободи на субекта на данните надделяват над интереса на Комисията да си сътрудничи с държави извън ЕС или с международни организации.

4. Параграфи 1, 2 и 3 не засягат прилагането на други решения на Комисията за определяне на вътрешни правила, уреждащи предоставянето на информация на субектите на данни и ограничаването на прилагането някои права съгласно член 25 от Регламент (ЕС) 2018/1725.

5. Всяко ограничение на правата и задълженията, посочено в параграф 2, е необходимо и пропорционално на рисковете за правата и свободите на субектите на данни.

6. Преди прилагане на ограничения се извършва проверка за необходимостта и пропорционалността за всеки отделен случай и ограниченията са в границите само на строго необходимото за постигане на набелязаната цел.

Член 3

Предоставяне на информация на субектите на данни

1. Комисията публикува на своя уебсайт съобщение за защита на личните данни, с което информира всички субекти на данни за своите дейности, които включват обработване на личните им данни за целите на изпълнението на задачите ѝ съгласно Решение (ЕС, Евратом) 2017/46, включително описание на категориите лични данни. Когато е възможно това да се направи, без да се застрашава информационната сигурност, Комисията гарантира, че субектите на данни са информирани индивидуално в подходяща форма.

2. Когато Комисията ограничава изцяло или частично предоставянето на информация на субектите на данни, чиито лични данни обработва за целите на изпълнението на задачите ѝ съгласно Решение (ЕС, Евратом) 2017/46, тя записва и регистрира причините за ограничаването в съответствие с член 6 от настоящото решение.

Член 4

Право на достъп на субекта на данни, право на изтриване и право на ограничаване на обработването

1. Когато Комисията ограничава изцяло или частично правото на субектите на данни на достъп до лични данни, правото на изтриване или правото на ограничаване на обработването, както са посочени в членове 17, 19 и 20 от Регламент (ЕС) 2018/1725, в отговора си на искането за достъп, изтриване или ограничаване на обработването тя информира засегнатия субект на данни:

а) за приложеното ограничение и основните причини за него;

б) за това как да подаде жалба до Европейския надзорен орган по защита на данните или да потърси защита по съдебен ред пред Съда на Европейския съюз.

2. Комисията може да отложи, пропусне или откаже предоставянето на информация относно причините за ограничението, посочено в параграф 1, доколкото това би възпрепятствало постигането на целта на ограничението.

3. Комисията записва и регистрира причините за ограничението в съответствие с член 6.

4. Когато правото на достъп е изцяло или частично ограничено, субектите на данни могат да упражняват правото си на достъп, като се свържат с Европейския надзорен орган по защита на данните в съответствие с член 25, параграфи 6, 7 и 8 от Регламент (ЕС) 2018/1725.

Член 5

Съобщаване на субектите на данни за нарушения на сигурността на личните данни

Когато Комисията ограничава съобщаването за нарушение на сигурността на личните данни на субекта на данните, както е посочено в член 35 от Регламент (ЕС) 2018/1725, тя записва и регистрира причините за ограничението в съответствие с член 6 от настоящото решение. Комисията съобщава на Европейския надзорен орган по защита на данните за записа в момента на уведомлението за нарушение на сигурността на личните данни.

Член 6

Записване и регистриране на ограниченията

1. Комисията записва причините за всички ограничения, прилагани в съответствие с настоящото решение, като включва позоваване на правното(ите) основание(я), приложено(и) за ограничението, и оценка на необходимостта от ограничението и неговата пропорционалност и взема предвид съответните елементи, посочени в член 25, параграф 2 от Регламент (ЕС) 2018/1725.

2. В записа се посочва по какъв начин упражняването на дадено право от страна на субекта на данни би възпрепятствало целите на предоставянето на операции и услуги за информационната сигурност на Комисията съгласно Решение (ЕС, Евратом) 2017/46 или целите на ограниченията, прилагани в съответствие с член 2, параграфи 2 или 3 от настоящото решение, или как би оказало неблагоприятно въздействие върху правата и свободите на други субекти на данни.

3. Комисията регистрира тези записи и всички документи, съдържащи съответните фактически и правни елементи. При поискване те се предоставят на Европейския надзорен орган по защита на данните.

Член 7

Продължителност на ограниченията

1. Ограниченията, посочени в членове 3, 4 и 5, продължават да се прилагат дотогава, докато причините за тях продължават да са валидни.

2. Когато причините за ограничение, посочено в членове 3, 4 и 5, вече не са валидни, Комисията:

а) премахва ограничението;

б) информира субекта на данни за основните причини за ограничението;

в) информира субекта на данни за това как да подаде жалба до Европейския надзорен орган по защита на данните по всяко време или да потърси защита по съдебен ред пред Съда на Европейския съюз.

Член 8

Гаранции и срокове на съхранение

1. Комисията преразглежда прилагането на ограниченията, посочени в членове 3, 4 и 5, шест месеца след приемането им, както и при приключването на индивидуалната операция за информационна сигурност. След това Комисията преразглежда и преценява ежегодно необходимостта от запазването на дадено ограничение.

Прегледът включва оценка на необходимостта от ограничението и неговата пропорционалност, като се вземат предвид съответните елементи, посочени в член 25, параграф 2 от Регламент (ЕС) 2018/1725.

2. Комисията е приела технически и организационни мерки за предотвратяване на случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни, като например управление на правата за достъп, политика за архивиране и всякакви други мерки в съответствие с Решение (ЕС, Евратом) 2017/46.

3. Комисията записва приложимите срокове на съхранение в съответствие с общия за Комисията списък за съхранение на преписки и съобщава на субектите на данни съответните срокове на съхранение за тези дейности по обработване в своето съобщение за защита на личните данни.

Член 9

Преглед от длъжностното лице по защита на данните към Комисията

1. Длъжностното лице по защита на данните към Комисията се уведомява без ненужно забавяне, когато правата на субектите на данни се ограничават в съответствие с настоящото решение. При поискване на длъжностното лице по защита на данните се предоставя достъп до записа и документите, съдържащи съответните фактически и правни елементи.

2. Длъжностното лице по защита на данните може да поиска преразглеждане на ограниченията и се уведомява за резултата от поисканото преразглеждане.

3. Комисията документира участието на длъжностното лице по защита на данните, когато правата на субектите на данни се ограничават в съответствие с настоящото решение.

Член 10

Влизане в сила

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

Съставено в Брюксел на 15 декември 2021 година.

За Комисията
Председател
Ursula VON DER LEYEN