ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 14.10.2022 г.
COM(2022) 530 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Първи доклад относно прилагането на Регламента за защита на данните от институциите, органите, службите и агенциите на Европейския съюз (Регламент (ЕС) 2018/1725)

Съдържание

1 Въведение 3

2 Отделни правила за защита на данните за институциите, органите, службите и агенциите на ЕС, съобразени със законодателството на ЕС в областта на защитата на данните 4

3 Прилагане на Регламента за защита на данните от институциите на ЕС в ИОЕС 6

3.1 Ролята на ИОЕС като администратори 6

3.2 Упражняване на правата на субектите на данни 7

3.3 Ограничаване на правата на субектите на данни чрез вътрешни правила 7

3.4 Длъжностни лица по защита на данните 9

3.5 Оценки на въздействието върху защитата на данните 10

3.6 Международно предаване на данни 11

4 Дейност на ЕНОЗД 12

4.1 ЕНОЗД като надзорен орган за защита на данните за ИОЕС 12

4.2 ЕНОЗД като съветник на законодателя на ЕС 14

4.3 Сътрудничество между ЕНОЗД и националните органи за защита на данните 15

4.4 Ресурси на ЕНОЗД 17

5 Използване от Комисията на правомощия за приемане на делегирани актове и актове за изпълнение 18

6 Правила за защита на данните за органите и агенциите, които извършват дейности в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси 18

6.1 Разширяване на прилагането на главата за правоприлагането от Регламента за защита на данните от институциите на ЕС 19

6.2 Разясняване на приложимостта на някои разпоредби на Регламента за защита на данните от институциите на ЕС по отношение на обработването на данни от оперативен характер 21

6.3 Правомощията на ЕНОЗД по отношение на надзора на органите и агенциите на ЕС 21

7 Перспективи 23

ПРИЛОЖЕНИЕ 26

1 Въведение

Регламентът за защита на данните от институциите, органите, службите и агенциите на Европейския съюз[1] („Регламентът за защита на данните от институциите на ЕС“) е основната[2] рамка за защита на данните от институциите, органите, службите и агенциите на ЕС („ИОЕС“), когато обработват лични данни като администратори или обработващи лични данни. Регламентът е стълб на доброто управление и доброто административно поведение на равнище ЕС. Той се прилага от 11 декември 2018 г.[3], когато отмени и замени своя предшественик — Регламент (ЕО) № 45/2001[4].

В настоящото съобщение се представя първият доклад относно прилагането на Регламента за защита на данните от институциите на ЕС в съответствие с член 97 от регламента. В него се прави и преглед на правните актове, приети въз основа на Договорите, които уреждат обработването на лични данни от оперативен характер[5] от органи, служби или агенции на ЕС при извършването на дейности, които попадат в обхвата на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси[6], в съответствие с член 98 от Регламент за защита на данните от институциите на ЕС.

Комисията събра информация за прилагането на Регламента за защита на данните от институциите на ЕС чрез проучване, инициирано през октомври 2021 г., при което ИОЕС бяха поканени да споделят своя опит в прилагането на регламента. Общо 56[7] ИОЕС отговориха, а представените в доклада статистически данни за ИОЕС се основават на тези отговори[8]. До Европейския надзорен орган по защита на данните (ЕНОЗД) в качеството му на надзорен орган беше изпратено отделно искане за предоставяне на информация[9]. Накрая

---

[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 (Текст от значение за ЕИП) (ОВ L 295, 21.11.2018 г., стр. 39—98), http://data.europa.eu/eli/reg/2018/1725/oj

[2] В устройствените актове на някои агенции в областта на правосъдието и вътрешните работи се съдържат специфични правила за защитата на данните, които допълват или се прилагат вместо Регламента за защита на данните от институциите на ЕС, вж. раздел 6.

[3] В съответствие с член 101, параграф 2 от Регламента за защита на данните от институциите на ЕС той се прилага за Евроюст едва от 12 декември 2019 г.

[4] Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1—22), http://data.europa.eu/eli/reg/2001/45/oj

[5] Член 3, параграф 2 от Регламента за защита на данните от институциите на ЕС.

[6] Глава 4 или глава 5 от дял V на трета част от Договора за функционирането на Европейския съюз (ДФЕС).

[7] Проучването беше изпратена до съществуващите по това време ИОЕС (списък: http://publications.europa.eu/code/bg/bg-5000900.htm).

[8] Процентите, посочени в настоящия доклад, са изцяло на базата на ИОЕС, които са отговорили на конкретния въпрос в проучването.

[9] Европейски надзорен орган по защита на данните, Информация, предоставена от Европейския надзорен орган по защита на данните за доклада относно прилагането на Регламент (ЕС) 2018/1725 („Регламента за защита на данните от институциите на ЕС“), 21 декември 2021 г., https://edps.europa.eu/system/files/2022-04/20-12-21-contribution_edps_report_eudpr_en_0.pdf

Комисията също така публикува покана за представяне на мнения[10], с което позволи и на обществеността да представи коментари. В настоящия доклад са разгледани въпросите, повдигнати в малкото коментари, получени в отговор на поканата за представяне на мнения.

В настоящия доклад се представя мястото на Регламента за защита на данните от институциите на ЕС в рамките на законодателството на ЕС в областта на защитата на данните, представя се неговото прилагане от страна на ИОЕС и дейността на ЕНОЗД, и се анализира прилагането на главата, приложима за органите и агенциите на ЕС, които извършват дейности в рамките на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси. Докладът завършва с очертаване на перспективите.

2 Отделни правила за защита на данните за институциите, органите, службите и агенциите на ЕС, съобразени със законодателството на ЕС в областта на защитата на данните

Основните инструменти за защита на данните в ЕС са Общият регламент относно защитата на данните („ОРЗД“)[11], Директивата относно правоприлагането в областта на защитата на данните („ДПЗД“)[12] и Директивата за правото на неприкосновеност на личния живот и електронни комуникации[13]. Те обаче не се прилагат за обработването на лични данни от страна на ИОЕС[14]. Поради това за ИОЕС са необходими отделни, но съгласувани правила за защита на данните. Тези правила са предвидени в Регламента за защита на данните от институциите на ЕС.

За да се осигури последователен подход към защитата на личните данни и тяхното свободно движение в ЕС, Регламентът за защита на данните от институциите на ЕС е приведен, доколкото е възможно, в съответствие с установените в ОРЗД и ДПЗД правила за защита на

[10] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13256-Регламент-относно-защитата-на-данните-от-институциите-органите-службите-и-агенциите-на-ЕС-доклад-относно-прилагането-му_bg

[11] 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—88), http://data.europa.eu/eli/reg/2016/679/oj

[12] 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—131), http://data.europa.eu/eli/dir/2016/680/oj

[13] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (ОВ L 201, 31.7.2002 г., стр. 37—47), https://data.europa.eu/eli/dir/2002/58/oj

[14] Член 2, параграф 3 от ОРЗД, член 2, параграф 3, буква б) от ДПЗД. Директивата за правото на неприкосновеност на личния живот и електронни комуникации сама по себе си не се прилага, но член 37 от Регламента за защита на данните от институциите на ЕС включва задължение ИОЕС да защитават информацията, предавана към, съхранявана в, свързана с, обработвана и събирана от крайните устройства на ползвателите, осъществяващи достъп до техните обществено достъпни уебсайтове и мобилни приложения в съответствие с член 5, параграф 3 от Директива 2002/58/ЕО.

данните, приети за публичния сектор. Когато Регламентът за защита на данните от институциите на ЕС следва същите принципи като ОРЗД, той трябва да се тълкува по същия начин, тъй като следва да се приема за еквивалентен на ОРЗД[15]. Същото може да се приеме и за правилата, съгласувани с ДПЗД.

Регламентът за защита на данните от институциите на ЕС е адаптиран към специфичния контекст на ИОЕС, описан в точките по-долу.

- Тъй като приложното му поле са изключително ИОЕС като публични органи, няколко разпоредби от ОРЗД, които се отнасят единствено за частния сектор, са пропуснати. Например в Регламента за защита на данните от институциите на ЕС не съществува възможността за обработване въз основа на правното основание „законни интереси“ на администратора[16].
- Няколко правомощия на Комисията да приема актове за изпълнение или делегирани актове не са повторени като такива, а вместо това Регламентът за защита на данните от институциите на ЕС препраща към ОРЗД или ДПЗД. Например в Регламента за защита на данните от институциите на ЕС не се съдържа механизъм за приемане на решения относно адекватното ниво на защита за международно предаване на данни, но ИОЕС могат да се позовават и на решенията относно адекватното ниво на защита, приети по силата на ОРЗД или ДПЗД.
- С Регламента за защита на данните от институциите на ЕС също така пряко се създава ЕНОЗД, като се определят неговите задачи, правомощия и процедури за назначаване. Съгласно ОРЗД и ДПЗД съответните надзорни органи се създават по силата на националното законодателство в съответствие с изискванията на тези два акта.
- Главата от Регламента за защита на данните от институциите на ЕС, приложима за органите и агенциите на ЕС в областта на наказателното правоприлагане[17], е функционално еквивалентна на ДПЗД по отношение на тези органи и агенции. Като пряко приложим регламент обаче той е формулиран по различен начин. В него са предвидени общи правила, които при необходимост се допълват от конкретни разпоредби в учредителните актове на органите и агенциите, развиващи дейност в тази област. В него е предвиден персонализиран режим за обработване на лични данни от оперативен характер, като се взема предвид специфичното естество на този сектор, например правилата за информиране на субектите на данни, с които се гарантира, че разследването е защитено.

[15] Вж. съображение 5 от Регламента за защита на данните от институциите на ЕС.

[16] Това отразява ситуацията при неговия предшественик, Регламент (ЕО) № 45/2001, в който също не се съдържаше основанието „законен интерес“. В съображение 22, второ изречение от Регламента за защита на данните от институциите на ЕС се пояснява, че „обработването на лични данни за изпълнението на задачи от обществен интерес от страна на институции и органи на Съюза включва обработването на лични данни, които са необходими за управлението и функционирането [им]“, което означава, че такива операции по обработване, например за осигуряване на контрол на физическия достъп до помещенията на ИОЕС, също са обхванати.

[17] Глава IX относно обработването на лични данни от оперативен характер от органи, служби и агенции на ЕС при извършване на дейности, които попадат в обхвата на трета част, дял V, глава 4 или глава 5 от ДФЕС.

3 Прилагане на Регламента за защита на данните от институциите на ЕС в ИОЕС

3.1 Ролята на ИОЕС като администратори

Отзивите на ИОЕС като цяло показват, че първите години от прилагането на Регламента за защита на данните от институциите на ЕС са допринесли успешно за укрепването на тяхната обща култура за защита на данните. В това отношение 94 % от ИОЕС заявяват, че с влизането в сила на Регламента за защита на данните от институциите на ЕС до известна степен или в голяма степен се е повишила осведомеността на тяхната организация относно правилата за защита на данните. Като цяло ИОЕС посочват, че Регламентът за защита на данните от институциите на ЕС е оказал положително въздействие върху техните политики за защита на данните, а служителите на ИОЕС са по-запознати с отчетността на своите организации като администратори, както и с изискванията за обработването на лични данни.

ИОЕС посочват извършването на оценки на въздействието върху защитата на данните, установяването и управлението на нарушения на сигурността на данните, както и защитата на данните на етапа на проектирането и по подразбиране като основни последици от Регламента за защита на данните от институциите на ЕС в сравнение с отменения Регламент (ЕО) № 45/2001. С Регламента за защита на данните от институциите на ЕС възможността за съвместно администриране — няколко организации, определящи заедно целите и средствата за обработване на лични данни — става по-видима, по същия начин както при ОРЗД. ЕНОЗД предостави насоки[18] по тази тема, а Комисията разработи вътрешни образци на договорености за съвместно администриране.

Макар и допълнителните изисквания за отчетност, необходими за доказване на спазването на Регламента за защита на данните от институциите на ЕС от страна на ИОЕС, като цяло да бяха приветствани, някои ИОЕС отбелязват, че правилата на регламента са довели до увеличаване на работното натоварване. Те също така посочват, че в Регламента за защита на данните от институциите на ЕС се съдържат сравнително сложни правила, което означава, че ИОЕС се нуждаят от повече експертен опит, включително сред техните длъжностни лица по защита на данните (ДЛЗД), както и в мрежите от координатори за защита на данните (КЗД) в тези ИОЕС, които разполагат с такива мрежи.

Всички ИОЕС, с изключение на две от тях, съхраняват данните си за операциите по обработване в централен регистър. Макар и това да не е конкретно изискване съгласно Регламента за защита на данните от институциите на ЕС, то е добра практика, която се препоръчва и от ЕНОЗД[19]. Освен това 72 % от ИОЕС са преобразували в записи всички свои

[18] Понятията „администратор“, „обработващ лични данни“ и „съвместно администриране“ съгласно Регламент (ЕС) 2018/1725, https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint

[19] Отчетност на място: Насоки относно документирането на действия по обработване за институциите, органите и агенциите на ЕС — част I: Записи и оценка на праговете, стр. 7, https://edps.europa.eu/sites/default/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf

уведомления до ДЛЗД съгласно предишния регламент[20]. Тези, които все още не са изпълнили тази задача, следва да прегледат и актуализират документацията си за операциите по обработване, за да се уверят, че тя е пълна и актуална.

3.2 Упражняване на правата на субектите на данни

С Регламента за защита на данните от институциите на ЕС на субектите на данни се предоставя широк набор от права във връзка с обработването на личните им данни, в съответствие с ОРЗД. Като администратори ИОЕС имат конкретно задължение да улеснят упражняването на тези права[21]. В резултат на това 96 % от ИОЕС посочват, че са извършили дейности за повишаване на осведомеността, като например актуализиране на обществено достъпната информация за операциите по обработване, информационните съобщения или ръководствата за субектите на данни.

Редица ИОЕС, като например Комисията, Европейската централна банка и Европейската служба за външна дейност, отчитат ясно изразено увеличение на постъпилите искания от физически лица между 2018 г. и 2021 г.[22] За други обаче, като Съда на Европейския съюз, Европейския икономически и социален комитет и Агенцията на Европейския съюз в областта на убежището, броят е стабилен или варира без ясна тенденция. Все още не е възможно да се установи ясна тенденция в броя на исканията от субекти на данни след влизането в сила на Регламента за защита на данните от институциите на ЕС, като се има предвид, че начинът на регистриране на различните видове искания варира в различните ИОЕС.

3.3 Ограничаване на правата на субектите на данни чрез вътрешни правила

Подобно на ОРЗД, в Регламента за защита на данните от институциите на ЕС[23] е предвидена възможност за ограничаване на някои от правата на субектите на данни. Това може да се направи със законодателни актове и чрез вътрешни правила[24]. Към такива вътрешни правила се прилагат строги критерии. Те трябва да са ясни и точни и прилагането им следва да бъде предвидимо за лицата, които са техни адресати. Правилата трябва да бъдат публикувани в Официален вестник и да отговарят на изискванията, посочени в Хартата на основните права и Европейската конвенция за защита на правата на човека и основните свободи[25].

[20] Член 25 от Регламент (ЕО) № 45/2001.
[21] Член 14 от Регламента за защита на данните от институциите на ЕС.
[22] Това включва общите искания за информация и исканията за упражняване на правата на субектите на данни съгласно глава II от Регламента за защита на данните от институциите на ЕС, като например правото на достъп до личните им данни, съхранявани от ИОЕС.
[23] Член 25 от Регламента за защита на данните от институциите на ЕС.
[24] Това съответства на възможностите за ограничаване на правата на субектите на данни на национално равнище в някои държави членки, напр. чрез министерски постановления.
[25] Член 25, параграф 5 и съображение 24 от Регламента за защита на данните от институциите на ЕС.

Ограниченията, основани на вътрешни правила, могат да се отнасят само до дейността на ИОЕС. Те трябва да зачитат основните права, да представляват необходими и пропорционални мерки в едно демократично общество и да са насочени към гарантиране на някоя от конкретно посочените в Регламента за защита на данните от институциите на ЕС цели[26]. Всеки субект на данни, чиито права са били ограничени, има право да подаде жалба до ЕНОЗД[27].

Преобладаващото мнозинство (84 %) от ИОЕС са приели вътрешни правила. Тези правила например са въведени, за да се позволи отлагане на предоставянето на информация на засегнато лице при вътрешно административно разследване[28]. В други случаи целта на тези правила е да се осигури продължаващо ефективно сътрудничество с държавите членки в областите, в които дейността на ИОЕС зависи от информация, получена от компетентните органи на държавите членки. Например вътрешните правила, приети от Комисията за обработване на лични данни в рамките на нейните дейности в областта на конкуренцията, борбата с измамите и вътрешния одит, включват възможността за въвеждане на ограничения върху правата на субектите на данни, когато личните данни се получават от компетентните органи на държавите членки[29]. С тези правила се определя възможността за налагане на подобни ограничения, когато националните органи са наложили ограничения въз основа на законодателна мярка, възможна съгласно ОРЗД[30] или ДПЗД[31].

Когато ИОЕС са приели вътрешни правила, с които се позволява ограничаване на правата на субектите на данни, тези правила обикновено се прилагат за всеки отделен случай, както се изисква съгласно съответните им вътрешни правила. Въпреки това 69 % от ИОЕС с въведени правила по член 25 съобщават, че все още не са ги използвали. Тези, които са ги използвали, съобщават за по-малко от 10 случая на ограничения, с изключение на Европейския парламент и Комисията. В дейностите на Европейската служба за борба с измамите все по-често възниква необходимостта от ограничения, и по-специално за отлагане на предоставянето на информация на субектите на данни относно обработването на техните лични данни, когато разследването е все още в начален етап, за да не се попречи на събирането на доказателства. Европейската служба за борба с измамите е приложила и няколко ограничения по отношение на исканията на субекти на данни за достъп до собствените им лични данни, които са били отхвърлени единствено с цел защита на правата

[26] Член 25, параграф 1 от Регламента за защита на данните от институциите на ЕС.
[27] Член 25, параграф 6 от Регламента за защита на данните от институциите на ЕС.
[28] Вж. например Решение № 59/2021 на генералния секретар на Съвета на Европейския съюз за определяне на правила за изпълнение във връзка с прилагането на Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета и ограничаването на правата на субектите на данни за целите на административни разследвания, дисциплинарни и съдебни производства 2022/C 25/02 (ОВ C 25, 18.1.2022 г., стр. 2—7).
[29] Решение (ЕС) 2018/1961 на Комисията (ОВ L 315, 12.12.2018 г., стр. 35); Решение (ЕС) 2018/1962 на Комисията (ОВ L 315, 12.12.2018 г., стр. 41); Решение (ЕС) 2018/1927 на Комисията (ОВ L 313, 10.12.2018 г., стр. 39).
[30] Член 23 от ОРЗД.
[31] Член 13, параграф 3, член 15 или член 16 от ДПЗД.

и свободите на други лица[32], например когато разкриването на данните би изложило информатора на риск от ответни действия с цел отмъщение.

Съгласно вътрешните правила на ИОЕС от тях обикновено се изисква да информират своите ДЛЗД за всички прилагани ограничения и да предоставят на ДЗЛД достъп до регистъра и всички документи относно тези ограничения[33].

3.4 Длъжностни лица по защита на данните

Задължението за назначаване на ДЛЗД във всички ИОЕС вече беше заложено в предишния Регламент (ЕО) № 45/2001. В Регламента за защита на данните от институциите на ЕС тази роля е по-ясно изразена, като е въведен принципът на отчетност. Това означава, че администраторът отговаря за спазването на правилата за защита на данните и трябва да може да го докаже.

ДЛЗД в 46 % от ИОЕС се подпомагат от мрежи от КЗД или сходни структури[34]. По-големите ИОЕС е по-вероятно да разполагат с такива мрежи (напр. Европейският парламент, Генералният секретариат на Съвета, Комисията и Европейската служба за външна дейност [ЕСВД]). ЕСВД също така организира и поддържа мрежа от кореспонденти за защита на данните в делегациите на ЕС.

Редица ИОЕС отбелязват увеличаването на отговорностите и работното натоварване на техните ДЛЗД (а оттам и на КЗД). Те признават необходимостта от предоставяне на повече ресурси на ДЛЗД (и КЗД), за да се гарантира, че те могат да прилагат ефективно политиките за защита на данните на своите ИОЕС. Споменава се и необходимостта да се гарантира независимостта на ДЛЗД.

В този контекст са налице две тенденции: От една страна, в Регламента за защита на данните от институциите на ЕС се поставя по-голям акцент върху отчетността на администратора, например чрез премахване на процедурата за предварителна проверка, която съществуваше съгласно предишния Регламент (ЕО) № 45/2001, като по този начин се намалява административната тежест. От друга страна, администраторите изискват повече насоки от ДЛЗД/КЗД за това как най-добре да спазват Регламента за защита на данните от институциите на ЕС. Във връзка с това е отбелязано, че мрежата от ДЛЗД на ИОЕС осигурява важен форум за обсъждане и изясняване на някои правни и технически аспекти, специфични за обработването на данни от страна на ИОЕС. Тази мрежа предоставя платформа за обмен на информация между ДЛЗД и ЕНОЗД, както и между самите ДЛЗД. Тя осъществява сътрудничество постоянно и обикновено заседава два пъти годишно.

---

[32] Вж. член 2, параграф 2 от Решение 2018/1962 на Комисията относно защитата на трети лица, както е посочено в член 25, параграф 1, буква з) от Регламента за защита на данните от институциите на ЕС.

[33] Това се препоръчва и в издадените от ЕНОЗД насоки относно член 25 от Регламента за защита на данните от институциите на ЕС, които са достъпни на адрес: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidance-art-25-regulation-20181725_en

[34] Например Европейската комисия разполага с длъжностно лице по защита на данните към Генералния секретариат, което се подпомага от координатори за защита на данните във всяка генерална дирекция.

Над половината (54 %) от ИОЕС са отделили повече ресурси за своите ДЛЗД и функциите за защита на данните като цяло. Повечето (84 %) ИОЕС са адаптирали вътрешните си процеси, за да гарантират, че служителите им информират и се консултират с ДЛЗД за новите операции по обработване на лични данни. Обикновено това се прави чрез включване на ДЛЗД например в процесите на управление на промените или в управителните съвети на проектите.

3.5 Оценки на въздействието върху защитата на данните

Най-голям брой оценки на въздействието върху защитата на данните (ОВЗД) са извършени от Европейската централна банка, Европейската инвестиционна банка и Комисията. В сравнение с предишната система за „предварителна проверка“[35] съгласно Регламент (ЕО) № 45/2001, броят на отнасяните към ЕНОЗД случаи е намалял значително. Това беше очакваната последица от тази промяна и тя доведе до намаляване на броя на консултациите с ЕНОЗД по отношение на административните операции по обработване, като например оценяването на персонала.

В таблица 1 от приложението е представен преглед на ОВЗД, извършени от ИОЕС в периода между 2019 г. и 2021 г.

Почти всички (94 %) ИОЕС са съгласни, че критериите съгласно Регламента за защита на данните от институциите на ЕС[36] за това кога трябва да извършват ОВЗД адекватно обхващат високорисковите операции по обработване. Тези, които не са съгласни, подчертават необходимостта ЕНОЗД да вземе предвид технологичното развитие при тълкуването на тези критерии. Например облачните изчисления вече не са „нова“ технология и това следва да се има предвид, когато се преценява дали трябва да се извършват ОВЗД. ИОЕС, които повдигнаха този въпрос, смятат, че самият правен текст обикновено е достатъчно ясен и че това е въпрос на тълкуване от страна на ЕНОЗД.

В Регламента за защита на данните от институциите на ЕС не се съдържа конкретно задължение за публикуване на резултатите от ОВЗД. Мнозинството (84 %) от ИОЕС не публикуват извършените от тях ОВЗД, докато 14 % ги публикуват частично или като резюме, след заличаване на информацията, която би могла да компрометира приетите мерки за сигурност. Само една ИОЕС посочва, че публикува изцяло своите ОВЗД. Публикуването на ОВЗД, като при необходимост се заличава информацията, която би изложила на риск сигурността на операциите по обработване, подобрява прозрачността по отношение на

[35] Член 27 от Регламент (ЕО) № 45/2001. В рамките на тази система операциите по обработване, напр. тези, които включват обработване на лични данни, свързани със здравословно състояние и с подозрения за престъпления, нарушения, присъди или мерки за сигурност, или предназначени за оценка на лични аспекти, свързани със субекта на данни, включително неговите способности, ефективност и поведение, трябваше да бъдат „предварително проверени“ от ЕНОЗД. Това доведе до голям брой уведомления (и съответни становища на ЕНОЗД) за много сходни операции по обработване, напр. процедурите за подбор и оценка на персонала попадат в обхвата на тази разпоредба.

[36] Член 39 от Регламента за защита на данните от институциите на ЕС.

спазването на правилата на Регламента за защита на данните от институциите на ЕС от страна на ИОЕС и е добра практика, която се препоръчва от ЕНОЗД[37].

3.6 Международно предаване на данни

Почти всички (91 %) ИОЕС съобщават, че дейността им включва международно предаване на лични данни. Това включва предаване на данни на държави извън ЕС/ЕИП, както и на международни организации. Няколко ИОЕС обаче споменават, че такова предаване е рядкост или засяга само ограничено количество лични данни. Що се отнася до използваните инструменти за предаване на данни, ИОЕС се позовават предимно на решения относно адекватното ниво на защита (приети съгласно ОРЗД[38] или ДПЗД[39]) и договорни инструменти, например за предаване на данни на частни дружества. За предаването на данни на публични органи се използват и други инструменти, като например правно обвързващи споразумения и административни договорености. Освен това 51 % от ИОЕС споменават, че извършват ограничени, отделни случаи на предаване на данни, например за организиране на обучение, въз основа на законовите основания за предаването на данни („дерогации“)[40].

На практика предаването на данни обикновено не се извършва пряко от ИОЕС, а от техните обработващи лични данни (които не са ИОЕС), действащи от тяхно име. Поради това Комисията обърна специално внимание на този сценарий в стандартните договорни клаузи, приети съгласно ОРЗД през юни 2021 г.[41], за да помогне на администраторите и обработващите лични данни да спазват изискванията както на ОРЗД, така и на Регламента за защита на данните от институциите на ЕС. По-специално обработващите лични данни в Европейското икономическо пространство (ЕИП) разполагат с възможността да включат тези стандартни договорни клаузи за международно предаване на данни в договорите със своите обработващи лични данни подизпълнители в трети държави[42]. По този начин се гарантира спазването на правилата на Регламента за защита на данните от институциите на ЕС[43] относно включването на обработващи лични данни подизпълнители от името на ИОЕС, стига задълженията за защита на данните да са съгласувани в договорите между: i) ИОЕС и обработващия лични данни; и ii) обработващия лични данни и неговия обработващ лични данни подизпълнител[44]. По-специално ИОЕС могат да осигурят такова съгласуване,

---

[37] Макар че съгласно Регламента за защита на данните от институциите на ЕС публикуването на (обобщени) доклади за ОВЗД не е задължение, това е добра практика, която се препоръчва от ЕНОЗД, вж. Отчетност на място, част II, стр. 18/19, https://edps.europa.eu/node/4582_en

[38] Член 45, параграф 3 от ОРЗД.

[39] Член 36, параграф 3 от ДПЗД.

[40] Член 50 от Регламента за защита на данните от институциите на ЕС.

[41] Решение за изпълнение (ЕС) 2021/914 на Комисията от 4 юни 2021 г. относно стандартни договорни клаузи за предаването на лични данни на трети държави съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета.

[42] С помощта на „Модул 3“ от стандартните договорни клаузи.

[43] Член 29, параграф 4 от Регламента за защита на данните от институциите на ЕС.

[44] Вж. съображение 8 от Решение за изпълнение (ЕС) 2021/914 на Комисията и бележка под линия 1 от приложението към това решение.

като използват приети от Комисията стандартни договорни клаузи за отношенията между администраторите и обработващите лични данни[45].

За да предостави допълнителни инструменти, с които да се осигурят подходящи гаранции за прякото предаване на данни от ИОЕС на трети държави (т.е. без участието на обработващ лични данни от ЕС/ЕИП), в момента Комисията разработва стандартни договорни клаузи съгласно член 48, параграф 2, буква б) от Регламента за защита на данните от институциите на ЕС. Тези клаузи ще бъдат приведени, доколкото е възможно, в съответствие със съществуващите клаузи, приети съгласно ОРЗД.

И накрая, с оглед на специфичните въпроси, възникващи при предаването на лични данни на международни организации (например поради статута на международните организации и приложимите привилегии и имунитети), Комисията работи съвместно с ДЛЗД на ИОЕС за разработване на специфични инструменти (напр. административни договорености), които са адаптирани за такова предаване.

4 Дейност на ЕНОЗД

4.1 ЕНОЗД като надзорен орган за защита на данните за ИОЕС

ЕНОЗД е независимият надзорен орган за защита на данните за ИОЕС[46], който отразява ролята на националните надзорни органи за защита на данните, създадени в държавите членки съгласно ОРЗД и ДПЗД.

В таблица 2 от приложението е представен преглед на надзорните дейности на ЕНОЗД в периода между 2018 г. и 2021 г. От влизането в сила на Регламента за защита на данните от институциите на ЕС на 11 декември 2018 г.[47] данните за 2018 г. представляват референтен брой за сравнение със ситуацията по време на предишния Регламент (ЕО) № 45/2001.

[45] Решение за изпълнение (ЕС) 2021/915 на Комисията от 4 юни 2021 г. относно стандартни договорни клаузи между администратори и обработващи лични данни съгласно член 28, параграф 7 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета и член 29, параграф 7 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета.

[46] С изключение на Съда на Европейския съюз при изпълнение на съдебните му функции, вж. член 57, параграф 1, буква а) и съображение 74 от Регламента за защита на данните от институциите на ЕС. В тези случаи надзорът се осъществява по специални механизми, създадени с Решение на Съда на Европейския съюз от 1 октомври 2019 г. за въвеждане на вътрешен механизъм за контрол на обработването на лични данни в рамките на съдебните функции на Съда (ОВ C 383, 2019 г., стр. 2) и с Решение на Общия съд от 16 октомври 2019 г. за въвеждане на вътрешен механизъм за контрол на обработването на лични данни в рамките на съдебните функции на Общия съд (ОВ C 383, 2019 г., стр. 4). Освен това все още съществува Съвместният надзорен орган за Митническата информационна система, създаден съгласно Решение 2009/917/ПВР на Съвета.

[47] Изключение в тази връзка е Евроюст, за който Регламентът за защита на данните от институциите на ЕС се прилага от 12 декември 2019 г., вж. член 101, параграф 2 от Регламента за защита на данните от институциите на ЕС.

ЕНОЗД отбелязва изместване към основната дейност на ИОЕС в предмета на консултациите, получени от тях след започването на прилагането на Регламента за защита на данните от институциите на ЕС. Това означава изместване към въпроси, свързани с обработването на лични данни за изпълнението на задачите, възложени на ИОЕС в обществен интерес, и отдалечаване от „административните“ теми, като например управление на персонала.

Броят на недопустимите жалби, постъпили в ЕНОЗД, се е увеличил между 2019 г. и 2021 г.[48] Повечето жалби, които са счетени за недопустими, са насочени срещу администратори в държави членки, които са под надзора не на ЕНОЗД, а на своите национални органи за защита на данните. Броят им през 2018 г. е бил по-висок най-вероятно защото тогава започна да се прилага ОРЗД. Това доведе до повишаване на осведомеността на населението относно правилата за защита на данните, но и до увеличаване на броя на недопустимите жалби. ЕНОЗД може също така да приключи разглеждането на допустими жалби при уреждане на спора по взаимно съгласие.

По отношение на проверките и одитите през 2019 г. е отчетено увеличение в сравнение с референтния брой за 2018 г., последвано от спад през 2020 г. и 2021 г. Това може да се обясни с пандемията от COVID-19, която доведе до затруднения при проверките на място и замяната им с дистанционни одити. ЕНОЗД извършва оценка на рисковете, за да реши кои ИОЕС да инспектира. Взема се предвид например броят на предоставените консултации, особено когато като част от основната дейност на ИОЕС се обработват специални категории данни. ЕНОЗД може също така да реши да проведе разследвания по своя инициатива, напр. относно използването на доставчици на компютърни услуги „в облак“ от страна на ИОЕС.

По отношение на нарушенията на сигурността на данните ЕНОЗД докладва, че в повечето случаи основната причина е човешка грешка, следвана от технически грешки и външни атаки[49].

ЕНОЗД е използвал повечето от правомощията си съгласно Регламента за защита на данните от институциите на ЕС, включително например налагането на временни забрани за извършване на операции по обработване на данни[50]. Досега не е използвал новото си правомощие да налага административни имуществени санкции, което е крайна мярка съгласно Регламента за защита на данните от институциите на ЕС[51].

---

[48] Вж. таблица 2 в приложението.

[49] За 2020 г. (последната година, за която са налични пълни статистически данни): 52 % от нарушенията на сигурността на данните са причинени от човешка грешка; 21 % — от техническа грешка; 17 % — от външна атака; а останалите се дължат на други причини, например злоупотреба с привилегировани акаунти.

[50] Например относно операциите по обработване за наблюдение на социалните медии от тогавашната Европейска служба за подкрепа в областта на убежището (EASO): https://edps.europa.eu/sites/default/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf В отговор на това тогавашната EASO спря въпросните операции по обработване.

[51] Съгласно ОРЗД при нарушение може директно да се налагат имуществени санкции, напр. когато администраторът не информира надлежно субектите на данни относно обработването на техните лични данни

В информацията, предоставена от ЕНОЗД за настоящия доклад, органът също така сочи, че е инвестирал в дейности за повишаване на осведомеността, например за обучение, като през 2019 г., след влизането в сила на Регламента за защита на данните от институциите на ЕС, участниците са достигнали пик от над 4 600. Макар броят на участниците през 2020 г. и 2021 г. да е спаднал спрямо този пик, той все още е значително по-висок от референтния брой от 1 000 участници през 2018 г.

ИОЕС дават до голяма степен положителна обратна връзка за взаимодействието с ЕНОЗД и получените от него насоки, като 86 % от тях посочват, че отговорите винаги или предимно са били лесни за разбиране. ИОЕС също така оценяват увеличените контакти на ЕНОЗД с мрежата от ДЛЗД.

Въпреки това някои ИОЕС отбелязват, че съветите на ЕНОЗД понякога пристигат с твърде голямо закъснение[52]. Те подчертават значението на продължаващата подкрепа и съвети от страна на ЕНОЗД и призовават за своевременни и практически насоки по определени въпроси, свързани със защитата на данните. Тези въпроси включват прилагането на основан на риска подход за администраторите, международното предаване и взаимоотношенията между администраторите (включително съвместни администратори) и техните обработващи лични данни.

4.2 ЕНОЗД като съветник на законодателя на ЕС

Комисията провежда официални консултации[53] с ЕНОЗД, в частност по законодателни предложения с въздействие върху обработването на лични данни, след приемането им от колегиума[54]. ЕНОЗД отговаря на тези консултации със становища или коментари[55]. ЕНОЗД също така издава становища по собствена инициатива, като например предварителното си становище относно европейското пространство на здравни данни[56]. Когато дадено предложение е от особено значение за защитата на данните, Комисията може да се консултира и с Европейския комитет по защита на данните (ЕКЗД). В такъв случай ЕНОЗД

(членове 12—14 от ОРЗД). Съгласно Регламента за защита на данните от институциите на ЕС ЕНОЗД може да налага имуществени санкции само за неизпълнение на разпореждане, напр. за отстраняване на неизпълнение на задължението за надлежно информиране на субектите на данни съгласно членове 14—16 от Регламента за защита на данните от институциите на ЕС.

[52] 67 % от ИОЕС заявяват, че са получили съветите на ЕНОЗД своевременно или предимно своевременно, докато 33 % са неутрални или заявяват, че (в повечето случаи) съветът е пристигал с голямо закъснение.

[53] Член 42 от Регламента за защита на данните от институциите на ЕС.

[54] По отношение на актовете за изпълнение и делегираните актове официалната консултация може да се проведе успоредно с периода за събиране на отзиви от широката общественост относно проектите на актове за изпълнение и делегирани актове.

[55] Съгласно член 218 от ДФЕС ЕНОЗД нарича отговорите по законодателни предложения и препоръки „становища“. Отговорите, отнасящи се до актове за изпълнение или делегирани актове, се наричат „коментари“, вж. също Решение на Европейския надзорен орган по защита на данните от 15 май 2020 г. за приемане на Процедурен правилник на ЕНОЗД (ОВ L 204, 26.6.2020 г., стр. 49), http://data.europa.eu/eli/proc_rules/2020/626/oj

[56] Предварително становище 8/2020 на ЕНОЗД относно европейското пространство на здравни данни, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en

и ЕКЗД следва да издадат съвместно становище[57], за да гарантират, че законодателят на ЕС получава съгласувани съвети.

Комисията също така провежда неофициални консултации с ЕНОЗД, преди колегиумът да приеме актове, които са обект на изискванията за провеждане на консултация. В отговор на такива консултации ЕНОЗД предоставя на Комисията неофициални коментари. Тази възможност спомага да се гарантира, че актовете на Комисията са в пълно съответствие с правилата за защита на данните преди тяхното приемане. Неофициалните консултации се използват особено по отношение на актове, които са чувствителни или имат по-значително въздействие върху защитата на данните.

Дейността на ЕНОЗД като съветник на законодателя на ЕС зависи от броя на новите предложения, изготвени от Комисията. След по-малкия брой през последната година на отиващата си Комисия, значителното увеличение на официалните коментари през 2021 г. се дължи на увеличения брой законодателни предложения и на усилията на Комисията да осигури последователно изпълнение на задължението за провеждане на консултация с ЕНОЗД[58]. Това включва актове за изпълнение и делегирани актове, включващи обработване на лични данни. След влизането в сила на Регламента за защита на данните от институциите на ЕС Генералният секретариат на Комисията изготви процедури и повиши осведомеността на службите относно изискването за провеждане на консултация с ЕНОЗД. Това доведе до по-систематично провеждане на консултации, включително по отношение на актове за изпълнение и делегирани актове. За целите на планирането ЕНОЗД и службите на Комисията провеждат годишни срещи, на които се обсъждат предстоящата работна програма и предложенията, за които се изисква консултация.

4.3 Сътрудничество между ЕНОЗД и националните органи за защита на данните

ЕНОЗД е член на ЕКЗД и му предоставя секретариат. Той също така си сътрудничи по други начини с националните надзорни органи при изпълнението на съответните им задачи[59]. Примерите включват отнасяне на жалби до компетентния надзорен орган за защита на данните или случаи, свързани с външни доставчици на услуги, които се използват както от ИОЕС, така и от администратори при спазване на ОРЗД. ЕНОЗД също така взема активно участие в работата на ЕКЗД, като поема функции, например като водещ докладчик или съдокладчик за насоките, или допринася по друг начин за работата му.

По отношение на няколко широкомащабни информационни системи и агенции, създадени по силата на правото на ЕС, от ЕНОЗД и националните надзорни органи, всеки от които действа в рамките на съответните си отговорности, се изисква да си сътрудничат активно,

[57] Член 42, параграф 2 от Регламента за защита на данните от институциите на ЕС.
[58] Член 42 от Регламента за защита на данните от институциите на ЕС.
[59] В съответствие с член 61 от Регламента за защита на данните от институциите на ЕС ЕНОЗД си сътрудничи и със Съвместния надзорен орган, създаден съгласно член 25 от Решение 2009/917/ПВР на Съвета.

за да се осигури координиран надзор[60]. В миналото учредителните актове на всяка система или агенция включваха конкретни разпоредби за тази цел. С Регламента за защита на данните от институциите на ЕС[61] се създава хармонизирана система за тази координация на надзора, към която може да препращат и други актове. Това е направено по отношение на Информационната система за вътрешния пазар[62], ECRIS-TCN[63], Евроюст[64], а съвсем наскоро и за Европол[65]. В други системи все още са налице координационни групи за надзор с подробни правила в учредителните им актове или подробни позовавания на заседанията като част от ЕКЗД[66].

---

[60] Примери за това са Шенгенската информационна система, Визовата информационна система и Евродак. Вж. Регламент (ЕС) 2018/1862 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси, за изменение и отмяна на Решение 2007/533/ПВР на Съвета и за отмяна на Регламент (ЕО) № 1986/2006 на Европейския парламент и на Съвета и Решение 2010/261/ЕС на Комисията (ОВ L 312, 7.12.2018 г., стр. 56—106); Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. относно Визовата информационна система (ВИС) и обмена на данни между държави членки относно визите за краткосрочно пребиваване (ОВ L 218, 13.8.2008 г., стр. 60—81); и Регламент (ЕС) № 603/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. за създаване на система Евродак за сравняване на дактилоскопични отпечатъци с оглед ефективното прилагане на Регламент (ЕС) № 604/2013 за установяване на критерии и механизми за определяне на държавата членка, компетентна за разглеждането на молба за международна закрила, която е подадена в една от държавите членки от гражданин на трета държава или от лице без гражданство и за искане на сравнения с данните в Евродак от правоприлагащите органи на държавите членки и Европол за целите на правоприлагането и за изменение на Регламент (ЕС) № 1077/2011 за създаване на Европейска агенция за оперативното управление на широкомащабни информационни системи в областта на свободата, сигурността и правосъдието (ОВ L 180, 29.6.2013 г., стр. 1—30).

[61] Член 62 от Регламента за защита на данните от институциите на ЕС.

[62] Регламент (ЕС) 2018/1724 на Европейския парламент и на Съвета от 2 октомври 2018 г. за създаване на единна цифрова платформа за предоставяне на достъп до информация, до процедури и до услуги за оказване на помощ и решаване на проблеми и за изменение на Регламент (ЕС) № 1024/2012 (ОВ L 295, 21.11.2018 г., стр. 1—38).

[63] Регламент (ЕС) 2019/816 на Европейския парламент и на Съвета от 17 април 2019 г. за създаване на централизирана система за установяване на държавите членки, разполагащи с информация за присъди срещу граждани на трети държави и лица без гражданство (ECRIS-TCN), с цел допълване на Европейската информационна система за съдимост и за изменение на Регламент (ЕС) 2018/1726 (ОВ L 135, 22.5.2019 г., стр. 1—26).

[64] Член 42, параграф 2 от Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно Агенцията на Европейския съюз за сътрудничество в областта на наказателното правосъдие (Евроюст) и за замяна и отмяна на Решение 2002/187/ПВР на Съвета (ОВ L 295, 21.11.2018 г., стр. 138—183).

[65] Вж. промените в член 44, параграф 2 от Регламента за Европол, въведени с Регламент (ЕС) 2022/991 на Европейския парламент и на Съвета от 8 юни 2022 г. за изменение на Регламент (ЕС) 2016/794 по отношение на сътрудничеството на Европол с частноправни субекти, обработването на лични данни от Европол в подкрепа на наказателни разследвания и ролята на Европол в областта на научните изследвания и иновациите (ОВ L 169, 27.6.2022 г., стр. 1—42).

[66] Член 57 от Регламент (ЕС) 2018/1861 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на граничните проверки, за изменение на Конвенцията за прилагане на Споразумението от Шенген и за изменение и отмяна на Регламент (ЕО) № 1987/2006 (ОВ L 312, 7.12.2018 г., стр. 14—55) и член 71 от Регламент (ЕС) 2018/1862 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси, за изменение и

ЕНОЗД допринася и за механизма за оценка по Шенген, създаден съгласно Регламент (ЕС) № 1053/2013 на Съвета[67]. Съгласно посочения регламент Комисията може да покани ЕНОЗД да определи наблюдател, който да вземе участие в проверка на място, обхващаща област от неговата компетентност, т.е. оценки на защитата на данните[68]. Това съответства на възможността Европейската агенция за гранична и брегова охрана (Frontex) и Европол да определят наблюдатели съответно за оценки на управлението на границите и на полицейското сътрудничество. Според Комисията експертният опит на наблюдателите на ЕНОЗД е ценен актив за оценките на защитата на данните.

4.4 Ресурси на ЕНОЗД

През отчетния период[69] броят на служителите на ЕНОЗД (включително в секретариата на ЕКЗД)[70]) нарасна постепенно, което отразява общата тенденция при националните надзорни органи за защита на данните. С течение на времето дейността на секретариата на ЕКЗД се увеличи, като нараства броят на насоките, препоръките, становищата и другите документи на ЕКЗД, за които секретариатът допринася. Осигуряването на достатъчно ресурси за секретариата на ЕКЗД е от съществено значение с оглед на по-значителната роля, която се очаква да има той за ефективното прилагане на ОРЗД. Това се отнася по-специално до целта на ЕКЗД да развие по-тясно сътрудничество в областта на стратегическата работа и да използва нови инструменти в подкрепа на сътрудничеството между органите за защита на данните[71]. По-специално наличието на силен и добре обезпечен с ресурси секретариат, който да подпомага работата на ЕКЗД, е от решаващо значение, за да се гарантира, че ЕКЗД може да изпълнява работата си според изискванията, особено в контекста на механизма за съгласуваност[72], чието използване се очаква да продължи да нараства.

В предоставената от него информация за настоящия доклад ЕНОЗД по-специално счита, че ако му бъдат възложени допълнителни задачи, например като орган за надзор на пазара съгласно законодателното предложение за изкуствения интелект[73], следва да му бъдат предоставени съответни допълнителни ресурси.

отмяна на Решение 2007/533/ПВР на Съвета и за отмяна на Регламент (ЕО) № 1986/2006 на Европейския парламент и на Съвета и Решение 2010/261/ЕС на Комисията (ОВ L 312, 7.12.2018 г., стр. 56—106).

[67] Регламент (ЕС) № 1053/2013 на Съвета от 7 октомври 2013 г. за създаването на механизъм за оценка и наблюдение с цел проверка на прилагането на достиженията на правото от Шенген и за отмяна на решението на изпълнителния комитет от 16 септември 1998 г. за оценка и прилагане на Споразумението от Шенген (ОВ L 295, 6.11.2013 г., стр. 27—37).

[68] Член 10, параграф 5 от Регламент (ЕС) № 1053/2013 на Съвета от 7 октомври 2013 г.

[69] Вж. таблица 4 в приложението.

[70] Член 57, параграф 1, буква л) от Регламента за защита на данните от институциите на ЕС.

[71] Изявление на ЕКЗД относно по-тясното сътрудничество по стратегически досиета, 29 април 2022 г.: Органите за защита на данните взеха решение за по-тясно сътрудничество по стратегически досиета | Европейски комитет по защита на данните (europa.eu).

[72] Глава VII от ОРЗД.

[73] COM/2021/206 final.

5 Използване от Комисията на правомощия за приемане на делегирани актове и актове за изпълнение

В Регламента за защита на данните от институциите на ЕС се съдържат няколко правомощия за Комисията да приема актове за изпълнение и да установява стандартни клаузи, както и препратки към правомощията по ОРЗД[74].

В Регламента за защита на данните от институциите на ЕС[75] се съдържат разпоредби, с които тя се оправомощава да установява стандартни договорни клаузи за защитата на данните за договорите между администратори и обработващи лични данни, съответстващи на правомощията по ОРЗД[76]. Комисията се възползва от това правомощие и през юни 2021 г.[77] прие стандартни договорни клаузи, уреждащи отношенията между администраторите и обработващите лични данни, които обхващат както ОРЗД, така и Регламента за защита на данните от институциите на ЕС. С тези клаузи на администраторите се предоставят лесни за използване инструменти за ефективно управление на взаимоотношенията с техните обработващи лични данни.

С Регламента за защита на данните от институциите на ЕС[78] също така се оправомощава Комисията да приема стандартни договорни клаузи за защита на данните за осигуряване на подходящи гаранции за предаването на лични данни извън ЕС/ЕИП. В момента Комисията подготвя такива клаузи.

6 Правила за защита на данните за органите и агенциите, които извършват дейности в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси

В глава IX от Регламента за защита на данните от институциите на ЕС се съдържат правила за ИОЕС, които обработват лични данни от оперативен характер при извършването на дейности, попадащи в обхвата на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси („глава за правоприлагането“). Тя има за цел да се намали фрагментирането:

- между режимите за защита на данните, приложими към обработването на данни от оперативен характер от агенциите на ЕС в тази област;

[74] Вж. член 47 от Регламента за защита на данните от институциите на ЕС, с който се дава възможност на ИОЕС да се позовават на решения относно адекватното ниво за защита, приети съгласно ОРЗД и ДПЗД, и член 14, параграф 8 от Регламента за защита на данните от институциите на ЕС относно делегираните актове за икони съгласно член 12, параграф 8 от ОРЗД.

[75] Член 29, параграф 7 от Регламента за защита на данните от институциите на ЕС.

[76] Член 28, параграф 7 от ОРЗД.

[77] Решение за изпълнение (ЕС) 2021/915 на Комисията от 4 юни 2021 г. относно стандартни договорни клаузи между администратори и обработващи лични данни съгласно член 28, параграф 7 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета и член 29, параграф 7 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета (текст от значение за ЕИП) (ОВ L 199, 7.6.2021 г., стр. 18—30), https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32021D0915

[78] Член 48, параграф 2, буква б) от Регламента за защита на данните от институциите на ЕС.

- с режима за защита на данните, приложим към националните дейности по наказателно правоприлагане съгласно ДПЗД.

За тази цел в главата за правоприлагането от Регламента за защита на данните от институциите на ЕС е предвиден набор от хоризонтални правила, основани на ДПЗД. При необходимост тези правила могат да бъдат допълнени със специални правила в учредителните актове на агенциите в зависимост от съответните им мандати и от специфичното естество на техните задачи и операции по обработване на данни.

В Регламента за защита на данните от институциите на ЕС се посочва необходимостта да се осигури единна и съгласувана защита на физическите лица при обработването на техните лични данни[79]. За тази цел в него изрично се посочва целта за разширяване на прилагането на главата за правоприлагането от Регламента за защита на данните от институциите на ЕС, така че да обхваща агенциите, които към момента на приемането на регламента са имали отделни рамки за защита на данните в своите устройствени актове, а именно Европол и Европейската прокуратура. В него се споменава и евентуалното изменение на главата за правоприлагането, ако е необходимо.

6.1 Разширяване на прилагането на главата за правоприлагането от Регламента за защита на данните от институциите на ЕС

Към момента на изготвяне на настоящия доклад главата за правоприлагането от Регламента за защита на данните от институциите на ЕС се прилага за обработването на лични данни от оперативен характер от:

- Евроюст[80] — допълнено от специфични правила, съдържащи се в Регламента за Евроюст;
- Европол[81] — допълнено от специфични правила, съдържащи се в Регламента за Европол, който е изменен[82] след влизането в сила на Регламента за защита на данните от институциите на ЕС;

[79] Член 98, параграф 2 от Регламента за защита на данните от институциите на ЕС.
[80] Член 26 от Регламент (ЕС) 2018/1727 на Европейския парламент и на Съвета от 14 ноември 2018 г. относно Агенцията на Европейския съюз за сътрудничество в областта на наказателното правосъдие (Евроюст) и за замяна и отмяна на Решение 2002/187/ПВР на Съвета (ОВ L 295, 21.11.2018 г., стр. 138—183).
[81] Член 28 от изменения 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.
[82] Регламент (ЕС) 2022/991 на Европейския парламент и на Съвета от 8 юни 2022 г. за изменение на Регламент (ЕС) 2016/794 по отношение на сътрудничеството на Европол с частноправни субекти, обработването на лични данни от Европол в подкрепа на наказателни разследвания и ролята на Европол в областта на научните изследвания и иновациите (ОВ L 169, 27.6.2022 г., стр. 1—42).

- Европейската агенция за гранична и брегова охрана — за малката част от нейните дейности, които са част от наказателното правоприлагане[83].

Въпреки това главата за правоприлагането от Регламента за защита на данните от институциите на ЕС все още не се прилага за Европейската прокуратура, чийто учредителен регламент беше приет преди него. В Регламента за Европейската прокуратура е предвиден самостоятелен режим за обработване на данни от оперативен характер. Последиците от това са две: Първо, някои от разпоредбите в Регламента за Европейската прокуратура се различават по същество от главата за правоприлагането от Регламента за защита на данните от институциите на ЕС, като например обработването на „ограничени“ лични данни[84]. Второ, някои от разпоредбите на Регламента за Европейската прокуратура, макар и сходни по същество, са формулирани по различен начин от главата за правоприлагането от Регламента за защита на данните от институциите на ЕС, което може да доведе до различни тълкувания.

С оглед на съгласуваността и в съответствие с общата цел за свеждане до минимум на фрагментирането на правилата за защита на данните, по отношение на Европейската прокуратура следва да се възприеме подход, подобен на този, приет за Евроюст и Европол. Целта е да се гарантира прякото прилагане на главата за правоприлагането от Регламента за защита на данните от институциите на ЕС по отношение на Европейската прокуратура, като в Регламента за Европейската прокуратура се запазят само необходимите уточнения. В същото време, предвид факта, че Европейската прокуратура функционира само от една година, в краткосрочен план все още е необходимо да се събере повече информация за практическото прилагане на режима за защита на данните на Европейската прокуратура. Това ще позволи точното определяне на тези уточнения с оглед на естеството на Европейската прокуратура като независимата прокурорска служба на ЕС[85].

[83] Вж. член 10, параграф 1, буква р) и член 90 от Регламент (ЕС) 2019/1896 на Европейския парламент и на Съвета от 13 ноември 2019 г. за европейската гранична и брегова охрана и за отмяна на регламенти (ЕС) № 1052/2013 и (ЕС) 2016/1624 (ОВ L 295, 14.11.2019 г., стр. 1—131), https://eur-lex.europa.eu/eli/reg/2019/1896/oj

[84] Съгласно член 61, параграф 4 от Регламента за Европейската прокуратура е позволено обработването на „ограничени“ данни „освен за съхранение, единствено с цел защита на правата на субекта на данните или на друго физическо или юридическо лице, което е страна по производство, образувано от Европейската прокуратура, или за целите [на доказване]“. Съответният член 82, параграф 3 от Регламента за защита на данните от институциите на ЕС гласи, че „ограничените данни се обработват единствено с оглед на целта, поради която тяхното изтриване е било възпрепятствано“, което включва запазването на данните за доказателство, но не се отнася до защитата на правата на субекта на данни или други лица.

[85] Придобитият с Евроюст и Европол опит не може да се пренесе пряко в Европейската прокуратура, тъй като мандатът на прокуратурата не е да подкрепя и засилва сътрудничеството между националните органи, а да разследва и преследва престъпления, засягащи финансовите интереси на ЕС.

6.2 Разясняване на приложимостта на някои разпоредби на Регламента за защита на данните от институциите на ЕС по отношение на обработването на данни от оперативен характер

В Регламента за защита на данните от институциите на ЕС[86] се посочва, че „само член 3 [определения] и глава IX [глава за правоприлагането] от настоящия регламент се прилагат за обработването на лични данни от оперативен характер“.

В главата за правоприлагането се съдържат материалноправни разпоредби, които съответстват на повечето разпоредби от глави II—V от Регламента за защита на данните от институциите на ЕС (общи принципи, права на субектите на данни, някои задължения на администраторите и обработващите лични данни, международно предаване на данни), с някои разлики, за да се отчете специфичният характер на правоприлагането (напр. правила за информиране на субектите на данни и за правото им на достъп до техните данни).

Важно е да се уточни, че с изменението на Регламента за защита на данните от институциите на ЕС в главата за правоприлагането са установени конкретни правила само за съответните разпоредби на други глави от регламента, които имат директен еквивалент в главата за правоприлагането. По този начин, ако законодателят не включи конкретни правила в акта за създаване на дадена агенция, за обработването на данни от оперативен характер се прилагат разпоредбите на глави, различни от главата за правоприлагането, които нямат директен еквивалент в последната[87].

Това изменение би подобрило правната сигурност и би осигурило цялостна рамка (напр. относно длъжността ДЛЗД, сътрудничеството с националните надзорни органи за защита на данните), включително за всички бъдещи агенции в тази област[88]. С наличието на такава цялостна рамка биха намалели и рисковете от фрагментиране.

6.3 Правомощията на ЕНОЗД по отношение на надзора на органите и агенциите на ЕС

Понастоящем в регламентите за създаване на Европейската прокуратура, Евроюст и Европол се съдържат конкретни разпоредби относно правомощията на ЕНОЗД[89].

---

[86] Член 2, параграф 2 от Регламента за защита на данните от институциите на ЕС.

[87] Напр. по отношение на задължението на администраторите да си сътрудничат съгласно член 32 от Регламента за защита на данните от институциите на ЕС, правилата относно длъжностните лица по защита на данните в членове 43—45 от Регламента за защита на данните от институциите на ЕС, член 31 относно воденето на регистри на дейностите по обработване и относно сътрудничеството с други надзорни органи съгласно член 61 от Регламента за защита на данните от институциите на ЕС.

[88] Все пак трябва да бъде установена специфичната правна рамка на тези агенции в съответствие с изискванията съгласно Регламента за защита на данните от институциите на ЕС, напр. член 72 относно определянето на срокове на съхранение. Но няма да е необходимо да се уреждат правата на субектите на данни или правомощията на ЕНОЗД, освен ако законодателят изрично не реши да се отклони от подхода на Регламента за защита на данните от институциите на ЕС.

[89] Член 85 от Регламента за Европейската прокуратура, член 40 от Регламента за Евроюст и член 43 от Регламента за Европол.

С актуализирания Регламент за Европол на ЕНОЗД се предоставят правомощия, които са съгласувани с тези по член 58 от Регламента за защита на данните от институциите на ЕС[90]. Такъв е по-специално случаят с правомощието за налагане на административни имуществени санкции и правомощието да се разпореди на администратора или обработващия лични данни да съобразят операциите по обработване на данни и, ако е целесъобразно, това да стане по указан начин и в определен срок.

В случая с Европейската прокуратура обаче правомощията на ЕНОЗД са формулирани по различен начин от този в Регламента за защита на данните от институциите на ЕС. ЕНОЗД не разполага с двете правомощия, посочени по-горе[91].

В Регламента за Frontex, за малката част от дейностите на Frontex, които са предмет на главата за правоприлагането[92], не се съдържат конкретни разпоредби относно правомощията на ЕНОЗД, което води до неясноти относно тези правомощия.

Предоставянето на ЕНОЗД на пълния набор от правомощия, посочени в член 58 от Регламента за защита на данните от институциите на ЕС, може да бъде постигнато, като се следват двете стъпки по-долу.

1. Пояснява, че съгласно Регламента за защита на данните от институциите на ЕС на ЕНОЗД по подразбиране се възлага надзорът на главата за правоприлагането и правомощията, предоставени му съгласно член 58 от регламента[93]. Това налага изменение на Регламента за защита на данните от институциите на ЕС, както е предложено в предишния раздел.
   С това също така биха се запълнили пропуските в Регламента за Frontex.

2. С премахването на разпоредбите относно правомощията на ЕНОЗД от учредителните актове на агенциите и органите пълният обхват на правомощията на ЕНОЗД съгласно изменения Регламент за защита на данните от институциите на ЕС ще се прилага пряко за Евроюст и Европейската прокуратура. Целта е те да бъдат приведени в съответствие във възможно най-голяма степен, за да се намали фрагментирането на правилата за защита на данните.

[90] Някои от задачите на ЕНОЗД, които не са от значение за Европол, напр. одобряването на стандартни договорни клаузи, не се повтарят.
[91] Съгласно член 85, параграф 3, буква б) от Регламента за Европейската прокуратура и член 40, параграф 3, буква б) от Регламента за Евроюст в случай на предполагаемо нарушение на разпоредбите, уреждащи обработването на лични данни от оперативен характер, ЕНОЗД може единствено да сезира Европейската прокуратура или Евроюст, и когато е уместно, да отправя предложения за отстраняване на това нарушение и за подобряване на защитата на субектите на данни.
[92] Вж. член 10, параграф 1, буква р) и член 90 от Регламента за Frontex.
[93] С член 1, параграф 3 от Регламента за защита на данните от институциите на ЕС на ЕНОЗД се възлага задачата да „следи за прилагането на разпоредбите на настоящия регламент по отношение на всички операции по обработване на лични данни, извършвани от институция или орган на Съюза“. Въпреки че тази разпоредба може да се тълкува като приложима и за дейностите, попадащи в главата за правоприлагането, би било полезно тя да бъде изрично формулирана, за да се гарантира правната сигурност.

7 Перспективи

Като цяло Регламентът за защита на данните от институциите на ЕС функционира добре и е подходящ за целта. На този етап Комисията няма да предлага изменения на онези части, които са еквивалентни на съответните правила в ОРЗД, като по този начин ще запази възможно най-тясно съответствие между Регламента за защита на данните от институциите на ЕС и ОРЗД[94]. Евентуалните изменения, разгледани в настоящия доклад, се отнасят до други части, а именно връзката на главата за правоприлагането от Регламента за защита на данните от институциите на ЕС с другите разпоредби на настоящия регламент.

През пролетта на 2022 г. Комисията предложи правила за укрепване на информационната сигурност в ИОЕС[95], които ще имат положително въздействие върху информационната сигурност, включително върху защитата на личните данни. Целта на това предложение е да се подобри допълнително устойчивостта и способността на ИОЕС да реагират на инциденти, когато са изправени пред киберзаплахи.

Комисията ще предприеме и стъпките, изложени в точките по-долу:

- при актуализирането на актовете за създаване на широкомащабни информационни системи, които продължават да съдържат подробни правила за модела за координация на надзора, да гарантира, че моделът за координация на надзора по Регламента за защита на данните от институциите на ЕС[96] ще се прилага за рационализиране на процедурите;
- да разгледа възможността за изменения на Регламента за защита на данните от институциите на ЕС с цел:
    - подобряване на правната сигурност и допълване на рамката за обработване на данни от оперативен характер, като в член 2, параграф 2 се поясни, че общите разпоредби на Регламента за защита на данните от институциите на ЕС се прилагат и за обработването на лични данни от оперативен характер, освен ако в главата за правоприлагането не се съдържат конкретни разпоредби (например относно правото на достъп). Това също така би осигурило готова рамка за всички бъдещи агенции в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество;
    - гарантиране на участието на ЕНОЗД като наблюдател във всички оценки на защитата на данните съгласно механизма за оценка по Шенген;
- впоследствие да разгледа възможността за изменение на регламентите за Европейската прокуратура и Евроюст в рамките на едно бъдещо преразглеждане с цел да се гарантира пълното прилагане на правилата за обработване на лични данни от оперативен характер в изменения Регламент за защита на данните от институциите на ЕС, като вземе предвид

[94] Ако ОРЗД бъде изменен на по-късен етап, Комисията ще разгледа необходимите изменения на Регламента за защита на данните от институциите на ЕС, за да запази съгласуваността на двата текста.
[95] Предложение за регламент на Европейския парламент и на Съвета за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза, COM(2022) 122 final.
[96] Член 62 от Регламента за защита на данните от институциите на ЕС.

специфичното естество на тези органи. Това също така ще доведе до хармонизиране на правомощията на ЕНОЗД спрямо тези органи и агенции с тези, с които разполага спрямо другите ИОЕС;

- да предложи стандартни договорни клаузи за международно предаване на лични данни[97] за ИОЕС;
- да продължи тясното сътрудничество с ЕНОЗД (и с ЕКЗД, когато е уместно) с цел да се гарантира своевременна и целева консултация по новите предложения[98], както и да продължи да провежда неофициални консултации с ЕНОЗД по важни текстове преди тяхното приемане.

[97] Съгласно член 48, параграф 2, буква б) от Регламента за защита на данните от институциите на ЕС.
[98] В съответствие с член 42 от Регламента за защита на данните от институциите на ЕС.

ЕНОЗД се приканва:

- да предостави допълнителни и своевременни практически насоки на ИОЕС, включително относно международното предаване на данни;
- да продължи да повишава осведомеността на администраторите и обработващите лични данни относно техните задължения съгласно Регламента за защита на данните от институциите на ЕС, както и да съветва ДЛЗД;
- да засили усилията за ефективно прилагане на Регламента за защита на данните от институциите на ЕС с цел да се гарантира пълната защита на субектите на данни.

Институциите, органите, службите и агенциите на ЕС се приканват:

- да продължат и при необходимост да засилят усилията за повишаване на осведомеността с цел да се гарантира достатъчно ниво на вътрешен експертен опит относно правилата на Регламента за защита на данните от институциите на ЕС;
- да разгледат възможността за публикуване на ОВЗД, като при необходимост изключват информацията, която би могла да компрометира приетите мерки за сигурност;
- да се уверят, че ДЛЗД (както и КЗД) разполагат с достатъчно ресурси и позиция в рамките на ИОЕС, които им позволяват да изпълняват задачите си ефективно и независимо;
- да приключат с преобразуването на оставащите уведомления по предишния регламент за защита на данните в регистри за защита на данните.

ПРИЛОЖЕНИЕ

Таблица 1 — Оценки на въздействието върху защитата на данните и предварителни консултации, проведени от ИОЕС

	2019 г.	2020 г.	2021 г.
Приет остатъчен риск	30	50	77
Предварителни консултации с ЕНОЗД	3	3	5
Изоставени проекти	2	2	0

Таблица 2 — Надзорна дейност на ЕНОЗД

	2018 г.	2019 г.	2020 г.	2021 г.
Консултации	50[99]	75	59	52
Предварителни консултации	0	0	1	4
Разрешения за предаване	0	1	0	4
Постъпили допустими жалби	58	59	43	44[100]
Решения[101] по допустими жалби	23	48	35	22
Постъпили недопустими жалби	240	151	203	269
Извършени проверки/одити	5	9	4	4
Проведени официални разследвания	0	4	1	2
Постъпили уведомления за нарушения на сигурността на данните	7	95	121	82[102]

[99] Две от които след влизането в сила на Регламента за защита на данните от институциите на ЕС.
[100] До 15 ноември 2021 г.
[101] Включително случаи, прекратени по взаимно съгласие, насочване към ДЛЗД и други начини за прекратяване.
[102] До средата на ноември 2021 г.

Таблица 3 — Консултативна дейност на ЕНОЗД

	2018 г.	2019 г.	2020 г.	2021 г.
Коментари	13	3	19	72
Становища	7	6	8	12
Становища по собствена инициатива	1	1	2	0
Съвместни становища с ЕКЗД	0	1	0	5
Неофициални коментари	33[103]	16	13	25

Таблица 4 — Ресурси на ЕНОЗД

	2018 г.	2019 г.	2020 г.	2021 г.	2022 г. (прогнозно)
Общ брой служители на ЕНОЗД (включително в секретариата на ЕКЗД)	98	100	118	126	139
Служители на ЕНОЗД в секретариата на ЕКЗД	19	22	27	34	38
Бюджет[104]	13 539 302 EUR (изпълнени)	15 301 687 EUR (изпълнени)	14 211 719 EUR (изпълнени)	16 761 285 EUR (изпълнени)	20 202 000 EUR (проект)

[103] Съгласно предишния Регламент (ЕО) № 45/2001 ЕНОЗД отчиташе консултациите по делегирани актове/актове за изпълнение като „неофициални“ коментари. Известна част от коментарите, включени към неофициалните коментари за 2018 г., биха били отчетени като „официални коментари“ през следващите години.

[104] Тези числа са актуализирани в сравнение с числата, представени от ЕНОЗД за настоящия доклад.