2025/1382

18.7.2025 г.

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/1382 НА КОМИСИЯТА

от 15 юли 2025 година

съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета по отношение на адекватното ниво на защита на личните данни от страна на Европейската патентна организация

(нотифицирано под номер C(2025) 4626)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид 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) ([1]), и по специално член 45, параграф 3 от него,

като има предвид, че:

1. ВЪВЕДЕНИЕ

(1) С Регламент (ЕС) 2016/679 се определят правилата за предаването на лични данни от администратори или обработващи лични данни в Съюза на трети държави и международни организации, доколкото това предаване попада в неговото приложно поле. Правилата относно международното предаване на данни са установени в глава V (членове 44—50) от този регламент. Въпреки че потоците от лични данни към и от държави и международни организации извън Европейския съюз са от съществено значение за разширяването на трансграничната търговия и на международното сътрудничество, нивото на защита, което се предоставя за личните данни в Съюза, не трябва да бъде излагано на риск при предаването на тези данни на трети държави и международни организации ([2]).

(2) Съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 Комисията може да реши посредством акт за изпълнение, че дадена трета държава, територия или един или повече конкретни сектори в дадена трета държава, или дадена международна организация осигуряват адекватно ниво на защита. При това условие предаването на лични данни на международна организация може да се извършва, без да е необходимо допълнително разрешение, както е предвидено в член 45, параграф 1 и в съображение 103 от Регламент (ЕС) 2016/679.

(3) Както е посочено в член 45, параграф 2 от Регламент (ЕС) 2016/679, приемането на решение относно адекватното ниво на защита трябва да се основава на цялостен анализ на правния режим на международната организация, който обхваща както правилата, приложими към вносителите на данни, така и ограниченията и гаранциите по отношение на достъпа до лични данни от страна на публичните органи. В своята оценка Комисията трябва да определи дали въпросната международна организация гарантира ниво на защита, равностойно „по същество“ на нивото, гарантирано в рамките на Съюза ([3]). Стандартът, спрямо който се оценява „равностойността по същество“, е определен от законодателството на Съюза, по-специално от Регламент (ЕС) 2016/679, както и от съдебната практика на Съда на Европейския съюз ([4]). „Референтният документ относно адекватното ниво на защита“ на Европейския комитет по защита на данните (ЕКЗД) също е от значение в това отношение, за да се изясни допълнително този стандарт и да се предоставят насоки ([5]).

([1]) ОВ L 119, 4.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Вж. съображение 101 от Регламент (ЕС) 2016/679.
([3]) Вж. съображение 104 от Регламент (ЕС) 2016/679.
([4]) Вж. дело C-311/18, *Facebook Ирландия и Schrems* (*Schrems II*), ECLI:EU:C:2020:559, т. 94.
([5]) Европейски комитет по защита на данните, Референтен документ относно адекватното ниво на защита, WP 254 rev. 01., достъпен на адрес: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Както е пояснено от Съда, от трета държава или международна организация не може да се изисква да осигурява равнище на защита, идентично на гарантираното в правния ред на Съюза ([6]). По-специално средствата, до които въпросната трета държава или международна организация прибягва за защита на личните данни, може да са различни от прилаганите в Съюза, стига те на практика те да се окажат ефективни за осигуряването на адекватно ниво на защита ([7]). Поради това стандартът за адекватно ниво на защита не включва изискване за буквално възпроизвеждане на правилата на Съюза. По-скоро проверката се състои в това дали чрез същността на правата на неприкосновеност на личния живот и гаранциите за защита на данните (включително тяхното ефективно изпълнение, контролиране и прилагане), както и чрез обстоятелствата, свързани с предаването на лични данни, чуждестранната система като цяло осигурява изискваното ниво на защита ([8]).

(5) Комисията анализира правната рамка и практиката на Европейската патентна организация. Въз основа на констатациите, изложени в съображения 7—100, Комисията стига до заключението, че Европейската патентна организация (ЕПО) осигурява адекватно ниво на защита на личните данни, предавани от Съюза на ЕПО, в рамките на приложното поле на Регламент (ЕС) 2016/679.

(6) Съгласно настоящото решение предаването на данни от администратори и обработващи лични данни в Съюза на Европейската патентна организация може да се извършва, без да е необходимо допълнително разрешение. Настоящото решение не засяга прякото прилагане на Регламент (ЕС) 2016/679 спрямо такива образувания, когато условията относно териториалното приложение на посочения регламент, изложени в член 3 от него, са изпълнени.

2. ПРАВИЛА, ПРИЛОЖИМИ КЪМ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

2.1. Организация и задачи на Европейската патентна организация

(7) Европейската патентна организация е междуправителствена организация, създадена на 7 октомври 1977 г. въз основа на Европейската патентна конвенция (ЕПК) от 39 договарящи държави — всички държави, членки на Съюза, и Исландия, Норвегия, Лихтенщайн, Албания, Северна Македония, Монако, Сан Марино, Сърбия, Швейцария, Черна гора, Обединеното кралство и Турция ([9]). Седалището на организацията е в Мюнхен.

(8) Организацията е юридическо лице ([10]) и се състои от два органа ([11]): Европейското патентно ведомство (Ведомството) и Административния съвет. Основната задача на ЕПО е издаването на европейски патенти ([12]) в съответствие с Европейската патентна конвенция, което се извършва от Ведомството под надзора на Административния съвет. Административният съвет се състои от представители на договарящите държави и упражнява законодателни правомощия от името на ЕПО. Той отговаря и за въпросите, свързани с политиката, и контролира дейността на Ведомството ([13]). Ведомството, което действа като изпълнителния орган на ЕПО, се ръководи от председател ([14]), който се отчита пред Административния съвет ([15]). Председателят на Ведомството, наред с другото, изготвя и изпълнява бюджета на Ведомството, назначава и контролира неговия персонал, упражнява дисциплинарна власт над персонала, осигурява функционирането на Ведомството, включително приемането на вътрешни административни инструкции и

([6]) Решение по дело C-362/14, *Schrems* (*Schrems I*), ECLI:EU:C:2015:650, т. 73.
([7]) Решение по дело *Schrems I*, т. 74.
([8]) Решение по дело *Schrems I*, т. 75.
([9]) Това отразява броя на договарящите държави към февруари 2025 г.
([10]) Член 5, параграф 1 от ЕПК.
([11]) Член 4, параграф 2 от ЕПК.
([12]) Във всяка от договарящите държави, за които е издаден, европейският патент по принцип има действието на национален патент, издаден от тази държава, и се подчинява на същите условия като националния патент(вж. член 2, параграф 2 от ЕПК).
([13]) Членове 26 и 33 от ЕПК.
([14]) Председателят на Ведомството се назначава от Административния съвет и представлява ЕПО във външен план (член 5, параграф 3 от ЕПК).
([15]) Член 10, параграф 1 от ЕПК.

информация за обществеността, и може да представя на Административния съвет всяко предложение за изменение на Конвенцията, за общи правила или за решения, които попадат в рамките на компетентността на Административния съвет ([16]). Ведомството се състои от различни отдели, включително получаващ сектор, правен отдел, експертизен отдел и отдел по възраженията, както и от апелативните състави (наричани също колегии по жалбите — вътрешен независим орган, пред който могат да се обжалват решенията, взети от ЕПО в контекста на процедурата за издаване на патент) ([17]).

(9) При изпълнението на своите задачи ЕПО получава лични данни от редица действащи лица в Съюза. В ЕПО непрекъснато се получават заявки за европейски патенти ([18]), подадени от заявители за патенти или препратени от националните патентни ведомства в държавите членки ([19]). ЕПО също така получава и обработва лични данни в контекста на задачите, които са ѝ възложени съгласно Регламент (ЕС) № 1257/2012 на Европейския парламент и на Съвета ([20]). Тези задачи включват получаване и разглеждане на искания за единно действие на европейски патенти, събиране на годишни такси и регистриране на единно действие ([21]). В този контекст ЕПО получава също така искания относно текущи жалби пред апелативния състав на Ведомството ([22]) от Единния патентен съд (ЕПС), които могат да включват лични данни, необходими за идентифициране на съответния случай ([23]).

(10) По подобен начин ЕПО получава лични данни, съдържащи се в международни заявки за патенти, когато действа съгласно Договора за патентно кооперииране (ДПК) — международен договор, който позволява на заявителите да получават патенти с действие във всички договарящи държави по ДПК ([24]). ЕПО действа като международен орган за търсене съгласно ДПК и в това си качество преглежда патентоспособността на изобретения, оповестени в международни заявки, което помага на заявителите да определят дали да подадат заявка за разглеждане по същество на национално равнище/на равнището на Съюза ([25]).

(11) Освен това ЕПО си сътрудничи тясно с националните патентни ведомства във всички държави членки в рамките на „Европейска патентна мрежа“ и в този контекст обменя лични данни с тях, например при предоставянето на курсове за обучение и ИТ услуги за подпомагане и укрепване на сътрудничеството в рамките на ЕПК. По подобен начин организацията е сключила двустранни споразумения за сътрудничество с държави членки, в рамките на които се извършва обмен на лични данни, например в контекста на създаването на работни групи, командироването и разполагането на технически експерти и др. Тя си сътрудничи тясно и със Службата на Европейския съюз за интелектуална собственост (EUIPO), например като провежда съвместни обучения и прояви за повишаване на осведомеността и като командирова експерти.

([16]) Член 10, параграф 2 от ЕПК.

([17]) Членовете на апелативните състави се назначават от Административния съвет (по предложение на председателя на Ведомството) и работят независимо (член 11, параграф 3 и член 23 от ЕПК).

([18]) Това включва например името, адреса, гражданството и телефонния номер на заявителите; имената и адресите на изобретателите и представителите на патентите; името и финансовата информация на лицето, извършващо плащанията, и др. ЕПО може да получи допълнителни лични данни, ако трета страна повдигне възражение срещу издаването на патента, в който случай с ЕПО може да бъде споделена допълнителна информация, като например съображения, доказателства и писмени становища на третата страна (вж. Правилника за прилагане на ЕПК, например правило 41, параграф 2, правило 143, параграф 1, буква з), правило 92, параграф 2, буква в), правило 19, параграф 1, правило 53, параграф 1 и др.). Вж. също член 9 от Решението на председателя на Ведомството относно процедурата за издаване на патенти.

([19]) Заявка за европейски патент може да бъде подадена в централната служба за индустриална собственост или друг компетентен орган на договаряща държава. След като провери заявката по отношение на сигурността или други национални изисквания, националният орган я препраща на ЕПО.

([20]) Регламент (ЕС) № 1257/2012 на Европейския парламент и на Съвета от 17 декември 2012 г. за осъществяване на засилено сътрудничество в областта на създаването на единна патентна закрила (ОВ L 361, 31.12.2012 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2012/1257/oj).

([21]) Единните патенти с единно действие за всички участващи държави членки се регистрират централно в ЕПО, без да са необходими допълнителни административни стъпки на национално равнище (какъвто е случаят за европейските патенти).

([22]) През декември 2024 г. ЕПО прие правило за независим надзорен механизъм за обработването на лични данни от апелативния състав в качеството му на съдебен орган. Налично на адрес: https://www.epo.org/en/about-us/transparency-portal?search_description=CA%2FD+19%2F24&op=&sort_by=most&items_per_page=10.

([23]) ЕПС е създаден въз основа на Споразумението за Единен патентен съд (ОВ C 175, 20.6.2013 г., стр. 1) и има изключителна компетентност, наред с другото, по отношение на европейските патенти (предмет на преходен период) и европейските патенти с единно действие (например по отношение на искове за действителни или потенциални нарушения и свързани с тях защити, искове за установяване на липса на нарушение, искове за временни и обезпечителни мерки и съдебни разпореждания, искове за отмяна и насрещни искове за отмяна). ЕПС също така има изключителна компетентност по отношение на решенията на ЕПО при изпълнението на нейните задачи в областта на единната патентна закрила.

([24]) За общ преглед на процедурата по ДПК вж. Ръководството на заявителя на ДПК — Въведение в международната фаза, достъпно на адрес https://www.wipo.int/pct/en/guide/index.html, и по-специално глава 3 от него, както и Ръководството за заявители: процедура по ДПК пред ЕПО, 16-то издание, 1 януари 2023 г., на разположение на адрес https://www.epo.org/en/legal/guide-europct/2023/index.html. За категориите лични данни, обработвани от ЕПО в контекста на производства по ДПК, вж. по-специално член 9, букви а), г), з), и), й), л), м), н) и п) от приложението към Решението на председателя на Европейското патентно ведомство от 13 декември 2021 г. относно обработването на лични данни при издаване на патенти и свързани с това производства (ОВ Европейско патентно ведомство 2021, A98).

([25]) Също така в този случай може да се наложи заявката за патент да бъде прехвърлена от централната служба за индустриална собственост или друг компетентен орган на държава — страна по ДПК, на ЕПО.

(12) Не на последно място ЕПО има договори с няколко доставчици на услуги в Съюза, които действат като обработващи лични данни по смисъла на член 4, точка 8) от Регламент (ЕС) 2016/679 и предават лични данни на ЕПО.

2.2. **Приложима правна рамка и правила за защита на данните**

(13) Първичното законодателство, с което се урежда дейността на ЕПО, е установено с международен договор, а именно с Европейската патентна конвенция, или с Договора за патентно кооперииране, когато ЕПО действа съгласно него. На второ ниво от йерархията на нормите, приложими за ЕПО, са правните актове, приети от Административния съвет или, що се отнася до ДПК, от събранието на ДПК. Вторичното законодателство на ЕПО включва Правилника за прилагане на ЕПК и т.нар. Служебен правилник (с който се уреждат аспекти, свързани със служителите на ЕПО, включително техните права и задължения) ([26]). Правото на защита на личните данни е установено в член 1Б от Служебния правилник ([27]), който съдържа и някои основни разпоредби от рамката на ЕПО за защита на данните, а именно относно приложното поле на тази рамка, защитата на специални категории данни и упражняването на правата от физическите лица. С член 2, параграф 1 и член 32А от Служебния правилник се установяват независими механизми за надзор (длъжностното лице по защита на данните (ДЛЗД) и Комитетът по защита на данните), които да следят спазването на правилата за защита на данните ([28]).

(14) Същите материалноправни изисквания, уреждащи защитата на личните данни, се прилагат и за Административния съвет и Ведомството, както и за всички техни отдели. По-специално обработването на лични данни от Ведомството се урежда от Правилника за прилагане на членове 1Б и 32А от Служебния правилник за щатните служители и другите служители на Европейското патентно ведомство относно защитата на личните данни (Правилник за защита на данните (ПЗД), който е приет от Административния съвет ([29]). Обработването на лични данни от Административния съвет е предмет на Правилника за защита на данните на Административния съвет, който прилага ПЗД *mutatis mutandis* ([30]). Когато настоящото решение се позовава на ПЗД, позоваванията включват съответните изисквания, които се прилагат за Административния съвет, неговия секретариат и неговите комитети. Структурата и съдържанието на ПЗД са тясно съгласувани с рамката на Съюза за защита на данните ([31]). По-специално ПЗД има много общо с Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([32]), с който се определят изисквания за защита на данните за институциите и органите на Съюза, и поради това е добре пригоден към специфичната структура и характеристики на международните организации, като същевременно отразява в голяма степен Регламент (ЕС) 2016/679.

([26]) Член 33 от ЕПК.

([27]) Вж. по-конкретно член 1Б, параграф 1 от Служебния правилник, в който се предвижда, че „Ведомството се стреми да гарантира спазване на основните права на неприкосновеност на личния живот и на защита на личните данни на всички лица, чиито данни се обработват от Ведомството, както и отчетност в това отношение“. Вж. също член 1, параграф 1 от ПЗД, в който се обяснява, че ПЗД осигурява правната рамка, необходима, за да се гарантира, че се спазват „основните права на физическите лица на неприкосновеност на личния живот и защита на личните данни, обработвани от Ведомството“.

([28]) Вж. също членове 47 и 48 от ПЗД.

([29]) Правилник за защита на данните (от стр. 495), на разположение на адрес https://report-archive.epo.org/files/babylon/service_regulations_en.pdf. ПЗД се прилага и за апелативните състави на Ведомството, с изключение на процедурата за обжалване пред Комитета по защита на данните, която не се прилага за обработването на лични данни от съставите при изпълнение на съдебните им функции (член 2, параграф 6 от ПЗД). За тези дейности ПЗД изисква от съставите да създадат отделен независим механизъм за разглеждане.

([30]) Правилник на Административния съвет за защита на данните, достъпен на адрес https://link.epo.org/ac-document/CA/D%202/23%20-%20En.pdf. Единственият аспект, по който Правилникът за защита на данните на Административния съвет се различава от ПЗД, са адаптациите, свързани със специфичната структура на Административния съвет, т.е. позоваванията на председателя на Административния съвет, които заменят позоваванията на председателя на Ведомството. Освен това за т.нар. специален комитет към Административния съвет са приети отделни правила — Правилник за защита на данните на специалния комитет. Този комитет се състои от договарящите държави на ЕПО и потребителски организации и е създаден с член 9, параграф 2 от Регламент (ЕС) № 1257/2012 и член 145 от ЕПК, за да упражнява надзор върху дейностите на Ведомството в контекста на единната патентна процедура. Правилникът за защита на данните на специалния комитет прилага Правилника за защита на данните на Административния съвет (който на свой ред прилага ПЗД) при обработването на лични данни от специалния комитет (вж. https://link.epo.org/web/about-us/governance/SC_D_1_23_en.pdf). Отново Правилникът за защита на данните на специалния комитет се различава от правилниците на Административния съвет и Ведомството само по отношение на позоваванията на председателя на специалния комитет (вместо на председателя на Административния съвет или на председателя на Ведомството).

([31]) Правилник за защита на данните на ЕПО: https://www.epo.org/en/about-us/office/data-protection-and-privacy.

([32]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(15) Що се отнася до обработването на данни от Ведомството, неговият председател е издал допълнителни правно обвързващи инструменти, като например циркулярни писма, решения и вътрешни административни инструкции ([33]). По-специално ПЗД се допълва от Решение на председателя на Ведомството от 13 декември 2021 г. относно обработването на лични данни в рамките на процедури за предоставяне на патенти и свързани с тях производства (Решение *PGP*) ([34]); Решение от 7 декември 2022 г. относно обработването на лични данни в производства, свързани с европейски патенти с единно действие (Решение UP) ([35]); Решение от 17 ноември 2022 г. относно държави и образувания, за които се счита, че осигуряват адекватна защита на личните данни ([36]); Решение от 2 май 2024 г. за определяне на оперативните звена на Ведомството, действащи като администратори на данни с делегирани правомощия ([37]); и Циркулярно писмо № 420 за прилагане на член 25 от ПЗД относно ограниченията на правата на субектите на данни (Циркулярно писмо 420) ([38]). Специално за обработването на данни в контекста на производства по издаване на патенти е важно да се отбележи, че изискванията за обработването на лични данни, предвидени пряко в ЕПК и ДПК, имат предимство пред ПЗД. Взаимодействието между ЕПК и ДПК, от една страна, и ПЗД, от друга страна, е изяснено в Решението *PGP* ([39]) и Решението UP. Специфичните изисквания за защита на данните, произтичащи пряко от ЕПК и ДПК, са оценени в съображения 55—59. ПЗД и допълващите го инструменти са правно обвързващи и приложими и физическите лица могат да се позоват на тях пред независими механизми за правна защита, както е описано в съображения 89—96.

(16) Правилата, предвидени в правните инструменти, посочени в съображение 15, са допълнително приведени в действие в инструменти, издадени от длъжностното лице по защита на данните (ДЛЗД) (вж. съображения 83—88) ([40]), които се прилагат за Административния съвет и Ведомството, както и за всички техни отдели ([41]).

2.3. **Материално и персонално приложно поле на Правилата за защита на данните**

(17) Съгласно ПЗД и Служебния правилник ([42]) всички служители на ЕПО са длъжни да спазват ПЗД при обработването на лични данни. Материалното и персоналното приложно поле на ПЗД се определят от понятията „лични данни“, „обработване“, „администратор“, „администратор с делегирани правомощия“ и „обработващ лични данни“, определени в тях.

2.3.1. ***Определение за лични данни и обработване***

(18) Определенията за „лични данни“ и „обработване“ в ПЗД са идентични на определенията в Регламент (ЕС) 2016/679 ([43]). ПЗД се прилага за всяко обработване на лични данни от ЕПО, независимо дали това обработване се отнася до лични данни на собствените ѝ служители или до данни на други лица ([44]). Данните, които са били

([33]) Член 10 от ЕПК. Вж. също член 1, параграф 2, буква а) от ПЗД.

([34]) https://www.epo.org/en/legal/official-journal/2021/12/a98.html. Подобно решение е прието по отношение на обработването на данни в производства по обжалване пред апелативните състави от председателя на апелативните състави, а именно решението от 14 юли 2023 г. относно обработването на лични данни в производства по обжалване пред апелативните състави, достъпно на адрес https://www.epo.org/en/legal/official-journal/2023/07/a73.html.

([35]) Решение от 7 декември 2022 г. относно обработването на лични данни в производства, свързани с европейски патенти с единно действие, достъпно на адрес https://www.epo.org/en/legal/official-journal/2022/12/a112.html.

([36]) https://epo.org/en/legal/official-journal/2022/12/a111.html. Изменено с Решение от 11 май 2023 г. (ОВ Европейско патентно ведомство 2023, A57), достъпно на адрес https://www.epo.org/en/legal/official-journal/2023/06/a57.html.

([37]) https://link.epo.org/web/en-decision-of-the-president-on-delegated-controllers.pdf. Посоченото решение се актуализира най-малко веднъж годишно.

([38]) Циркулярно писмо 420 за прилагане на член 25 от Правилата за защита на данните, достъпно на адрес https://link.epo.org/web/circular_420_en.pdf.

([39]) Що се отнася до обработването на лични данни от апелативните състави в производства по обжалване, това взаимодействие е изяснено в решението на председателя на апелативните състави относно обработването на лични данни в производства по обжалване пред апелативните състави.

([40]) Вж. например позоваването на оперативни документи, издадени от ДЛЗД, в член 1, параграф 2, буква в) от ПЗД, които са одобрени от председателя на Ведомството и по този начин са станали обвързващи.

([41]) Вж. член 1, параграф 6 и член 12, параграф 5 от Правилника за защита на данните на Административния съвет.

([42]) Член 2, параграф 2 от ПЗД и член 1 от Служебния правилник.

([43]) Член 3, параграф 1, букви а) и б) от ПЗД и член 4, параграфи 1 и 2 от ОРЗД.

([44]) Член 1Б, параграф 2 от Служебния правилник и член 2, параграфи 2 и 3 от ПЗД. Вж. също определението за „субект на данни“ (член 3, параграф 1, буква ц) от ПЗД): „всяко физическо лице, което е идентифицирано или може да бъде идентифицирано, независимо дали това лице е служител на Ведомството или не“. За да се определи дали дадено лице може да бъде идентифицирано, трябва да се вземат предвид всички средства, като например подбирането на лица за извършване на проверка, с които е най-вероятно да си послужи администраторът или друго лице, за да идентифицира пряко или непряко даденото физическо лице.

подложени на псевдонимизация ([45]), също се считат за лични данни, докато данните на починали лица или юридически лица или анонимната информация ([46]) не се третират като лични данни съгласно ПЗД ([47]).

(19) ПЗД се прилага за обработването на лични данни от ЕПО изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част или са предназначени да бъдат част от регистър с лични данни ([48]).

2.3.2. *Администратор, администратор с делегирани правомощия и обработващ лични данни*

(20) Съгласно ПЗД „администратор“ означава „образувание, а именно Европейското патентно ведомство, което самостоятелно или съвместно с други определя целите и средствата за обработването на лични данни“ ([49]). По принцип председателят на Ведомството действа като администратор за операциите по обработване на данни, извършвани от Ведомството ([50]). Същото се отнася и за Административния съвет (чийто председател действа като администратор), апелативните състави, действащи в качеството си на съдебни органи (чиито председател действа като администратор ([51])) и специалния комитет (чийто председател действа като администратор ([52])). Администраторът може да делегира това правомощие на оперативните звена, представлявани от служител на висша ръководна длъжност ([53]). В такива случаи оперативните звена действат като „администратори с делегирани правомощия“ ([54]), които определят целта (например причината, обосновката и бизнес нуждите) и средствата за операцията по обработване и гарантират, че всички операции по обработване, включващи лични данни, са в съответствие с правилата на ПЗД ([55]). В такива случаи администраторът продължава да носи отговорност за обработването на лични данни. В ПЗД се предвижда и сценарий на „съвместно администриране“, при който администраторът определя целта и средствата за обработването заедно с един или повече администратори извън ЕПО ([56]).

([45]) „Псевдонимизация“ означава обработване на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тази информация се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано. Вж. член 3, параграф 1, буква д) от ПЗД.

([46]) Анонимна информация е информация, която не е свързана с идентифицирано физическо лице или лице, което може да бъде идентифицирано, или с лични данни, анонимизирани по такъв начин, че субектът на данните (повече) не може да бъде идентифициран. Вж. член 3, параграф 1, буква с) от ПЗД. Съгласно член 13, параграф 1 от ПЗД администраторът не е длъжен да поддържа, придобива или обработва допълнителна информация за идентифициране на физическо лице единствено с цел спазване на ПЗД, когато целите, за които се обработват данните, (повече) не изискват идентифициране на физическо лице.

([47]) Член 2, параграф 4 от ПЗД. По отношение на обработването на лични данни за целите на архивирането (при законното упражняване на официалните правомощия на ЕПО), за целите на научни или исторически изследвания или за статистически цели, ПЗД изисква да са въведени технически и организационни мерки, наред с другото за да се гарантира спазването на принципа на свеждане на данните до минимум, а когато целта на обработването може да бъде постигната по този начин, данните да се обработват по начин, който повече не позволява идентифицирането на физическото лице (член 14 от ПЗД).

([48]) Член 1Б, параграф 3 от Служебния правилник и член 2, параграф 1 от ПЗД. „Регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип; вж. член 3, параграф 1, буква е) от ПЗД.

([49]) Член 3, параграф 1, буква ж) от ПЗД. Когато в настоящото решение се използва терминът „администратор“, това се отнася или до самата ЕПО, или до администраторите с делегирани правомощия.

([50]) Член 10, параграф 2 от ЕПК и член 28, параграф 1 от ПЗД.

([51]) Член 28, параграф 2 от ПЗД. Това произтича по-специално от делегирането на правомощия от председателя на Ведомството, вж. https://www.epo.org/en/legal/official-journal/2021/etc/se1/p175.html. За други дейности (когато съставите не действат в качеството си на съдебни органи) председателят на апелативните състави действа като администратор с делегирани правомощия от председателя на Ведомството.

([52]) Вж. член 1, параграфи 4 и 5 от ПЗД на Административния съвет и член 13а, параграф 2 от Процедурния правилник на специалния комитет.

([53]) Член 28, параграф 3 от ПЗД.

([54]) Вж. член 3, параграф 1, буква з) от ПЗД. Лицето, представляващо оперативния отдел, трябва да бъде служител на висша ръководна длъжност, обикновено поне директор. Списъкът на администраторите с делегирани правомощия се оповестява публично (вж. например https://link.epo.org/web/en-decision-of-the-president-on-delegated-controllers.pdf и https://link.epo.org/web/decision_of_the_president_of_the_boards_of_appeal_appointing_a_delegated_controller_en.pdf) и се актуализира редовно.

([55]) Когато в настоящото решение се използва терминът „администратор“, това включва съответните администратори с делегирани правомощия.

([56]) В този случай в член 29 от ПЗД се изисква администраторът (с делегирани правомощия) да определи по прозрачен начин съответните отговорности на двете страни за спазване на техните задължения за защита на данните, по-специално по отношение на упражняването на правата на физическите лица и задълженията за прозрачност.

(21) Определението за „обработващ лични данни“ в ПЗД е идентично на определението в член 4, параграф 8 от Регламент (ЕС) 2016/679: „физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора“ ([57]). Администраторът има право да използва само обработващи лични данни, които предоставят достатъчни гаранции, че ще бъдат приложени подходящи технически и организационни мерки, за да се гарантира, че обработването отговаря на изискванията на ПЗД ([58]). Отношенията между администратора и обработващия лични данни трябва да се уреждат с договор или правен акт, който е обвързващ за обработващия лични данни и, наред с другото, определя предмета, продължителността, естеството и целта на обработването ([59]). Обработващият лични данни има право да обработва данните само въз основа на документирани инструкции на администратора. Обработващият лични данни е длъжен да съдейства на администратора при изпълнението на задълженията му съгласно ПЗД. На обработващия лични данни се забранява да ангажира подизпълнители като обработващи лични данни без предварителното разрешение на администратора ([60]). Администраторите с делегирани правомощия имат на разположение стандартно споразумение за обработване на данни ([61]). Освен това, ако обработващият лични данни се намира в трета държава, всяко споделяне на лични данни с този обработващ лични данни трябва също да отговаря на изискванията на ПЗД за международно предаване на данни, както е описано в съображения 68—73 от настоящото решение ([62]).

2.4. **Гаранции, права и задължения**

2.4.1. ***Законосъобразност и добросъвестност на обработването***

(22) Личните данни следва да се обработват законосъобразно и добросъвестно.

(23) Тези общи принципи са установени в член 4, параграф 2, буква а) от ПЗД по начин, който може да се счита за идентичен на член 5, параграф 1, буква а) от Регламент (ЕС) 2016/679.

(24) Принципът на законосъобразност е доразвит в член 5 от ПЗД, в който се изброяват правните основания за обработване на лични данни. Тези правни основания са а) необходимостта от изпълнение на дадена задача при упражняването на официалните дейности на ЕПО ([63]) или при законното упражняване на официалните правомощия, предоставени на администратора, което включва обработването, необходимо за управлението и функционирането на Ведомството ([64]); б) необходимостта от спазване на правно задължение, което се прилага спрямо администратора (например да публикува информация, посочена в заявка за патент, в Европейския патентен регистър) ([65]); в) необходимостта от изпълнение на договор, по който субектът на данните е страна, или от предприемане на стъпки по искане на субекта на данните преди сключването на договор; г) съгласието на субекта на данните; или д) необходимостта да бъдат защитени жизненоважните интереси на субекта на данни или на друго физическо лице.

([57]) Член 3, параграф 1, буква й) от ПЗД.

([58]) Член 30, параграф 1 от ПЗД.

([59]) Член 30, параграф 3 от ПЗД.

([60]) Член 30, параграфи 2 и 3 от ПЗД. Обработващият лични данни, ангажиращ обработващ лични данни като подизпълнител (по договор), е длъжен да наложи на подизпълнителя същите задължения за защита на данните като задълженията, предвидени в договора между администратора и обработващия лични данни (член 30, параграф 4 от ПЗД).

([61]) Приложение Д към общите условия на договора за ЕПО, https://link.epo.org/web/general_conditions_of_contract_en.pdf.

([62]) Член 8, параграфи 1, 2 и 5 във връзка с член 9, параграф 1 от ПЗД.

([63]) Това се отнася до задачите, изпълнявани съгласно ЕПК и ДПК или правилата, приети на тази основа (например Служебния правилник), които са необходими за изпълнението на задачите на ЕПО в процедурата за издаване на патенти. Вж. също параграф 5, точка 1) от приложението към Решението *PGP* и съответните разпоредби на ЕПК, като например части IV и V от нея. За изпълнението на задачите на ЕПО в контекста на процедурата за издаване на патенти ЕПО обработва лични данни при обработването на заявки и патенти; провеждането на процедури по възражение; комуникациите със страните по процедурите (и когато е приложимо, с трети страни); поддържането на Европейския патентен регистър; изготвянето на доклади и статистически данни и обмена на данни с договарящите държави и Световната организация за интелектуална собственост (параграф 6 от приложението към Решението *PGP*).

([64]) Това обхваща задачите, възложени на председателя на Ведомството, за да се гарантира ефективното функциониране и управление на Ведомството. Вж. например член 10 от ЕПК, в който се описват задачите на председателя на Ведомството по отношение на персонала, (достъпа до) сградите и управлението на оборудването. Този подход е в съответствие с член 5, параграф 1, буква а) и съображение 22 от Регламент (ЕС) 2018/1725. По подобен начин това се отнася до задачите на Административния съвет по ЕПК, например за установяване на правила относно пенсиите и финансовите разпоредби, вж. член 33 от ЕПК, правило 9, точка 2), правило 12, буква в) и правило 122, точка 4) от Правилника за прилагане на ЕПК. Що се отнася до специалния комитет, това се отнася до надзорните задачи съгласно член 145 от ЕПК. Що се отнася до апелативните състави, това се отнася например до тяхната компетентност да разглеждат жалби срещу решения на други части на Ведомството, вж. член 21, параграф 1 от ЕПК.

([65]) Вж. например правило 20 от Правилника за прилагане на ЕПК.

(25) Съгласието е определено в ПЗД по същия начин, както в Регламент (ЕС) 2016/679, а именно като „всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени“ ([66]). Администраторът е този, който трябва да докаже, че субектът на данните е дал съгласието си ([67]). Когато се прави оценка дали съгласието е било свободно изразено, следва да се отчита дали изпълнението на даден договор е поставено в зависимост от съгласието за обработване на данни, което не е необходимо за изпълнението на този договор ([68]). Съгласието не може да се разглежда като свободно дадено, ако субектът на данни няма истински и свободен избор и не е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него ([69]). Нещо повече, за да бъде съгласието информирано, в ПЗД се изисква субектът на данни да знае поне самоличността на администратора и целите на обработването, за които са предназначени личните данни ([70]). Не на последно място субектът на данни има право да оттегли съгласието си по всяко време ([71]).

2.4.2. *Обработване на специални категории данни*

(26) Когато се обработват „специални категории данни“, следва да има специфични гаранции.

(27) ПЗД съдържа специални правила по отношение на обработването на специални категории лични данни ([72]), които са определени по същия начин, както в Регламент (ЕС) 2016/679, а именно като „лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни ([73]) или биометрични данни ([74]) за целите единствено на идентифицирането на физическо лице, както и данни за здравословното състояние ([75]) или данни за сексуалния живот или сексуалната ориентация на физическото лице“ ([76]). Съгласно ПЗД обработването на специални категории данни по принцип е забранено, освен ако не важи специално изключение ([77]).

(28) Специфичните изключения, изброени в член 11, параграф 2 от ПЗД, са подобни на тези в член 9, параграфи 2 и 3 от Регламент (ЕС) 2016/679, с няколко адаптации към правната рамка, в която функционира ЕПО. Обработването на специални категории лични данни е разрешено само при конкретни и ограничени обстоятелства ([78]), т.е. когато 1) субектът на данните е дал изрично съгласие за това; 2) обработването е необходимо, за да бъдат защитени жизненоважните интереси на дадено лице (когато субектът на данните е физически или юридически неспособен да

([66]) Член 3, параграф 1, буква м) от ПЗД. Вж. също член 7, параграф 2 от ПЗД.
([67]) Член 7, параграф 1 от ПЗД.
([68]) Член 7, параграфи 1, 5, 6 и 7 от ПЗД.
([69]) Член 7, параграф 4 от ПЗД.
([70]) Член 7, параграф 4 от ПЗД.
([71]) Член 7, параграф 5 от ПЗД.
([72]) Вж. например член 11 от ПЗД.
([73]) „Генетични данни“ означава лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравословното състояние на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице; вж. член 3, параграф 1, буква о) от ПЗД.
([74]) „Биометрични данни“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни; вж. член 3, параграф 1, буква п) от ПЗД.
([75]) „Данни за здравословното състояние“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние; вж. член 3, параграф 1, буква р) от ПЗД.
([76]) Член 11, параграф 1 от ПЗД.
([77]) Член 11, параграфи 1 и 2 от ПЗД.
([78]) ПЗД също така позволява обработването на специални категории данни при специфични сценарии, които засягат предимно персонала на ЕПО и следователно имат по-малко значение за данните, предавани въз основа на настоящото решение. По-конкретно, специални категории данни могат да бъдат обработвани, когато това е разрешено от правно обвързваща разпоредба, приложима за Европейската патентна организация (например ЕПК и актовете, приети от Административния съвет и председателя на Ведомството, вж. член 3, параграф 1, буква ш) от ПЗД), която предвижда подходящи гаранции за основните права и интереси на субекта на данните (член 11, параграф 2, буква б) от ПЗД) и е необходима за целите на изпълнението на задълженията и упражняването на специфичните права на администратора или на субекта на данните в областта на трудовото и социалноосигурителното право. По подобен начин обработването може да се извърши, когато е необходимо, от съображения за обществен интерес в областта на общественото здраве, като например защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи, на основание на националното право, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна (вж. член 11, параграф 2, буква ж) от ПЗД). И накрая, обработването може да е необходимо за профилактичната или трудовата медицина, оценката на работоспособността на работника или служителя, медицинската диагноза, предоставянето на здравни или социални грижи или лечение, управлението на системите и услугите за здравни или социални грижи или за медицинските прегледи и становища, когато тези данни се обработват от медицински специалист, обвързан от задължението за професионална тайна, или от друго лице, което има равностойно задължение за опазване на тайна (член 11, параграф 3 от ПЗД).

даде своето изрично съгласие); 3) личните данни явно са направени обществено достояние от субекта на данни; 4) обработването е необходимо за конкретна цел, свързана с упражняването на официалните дейности на ЕПО или при упражняването на легитимно правомощие, предоставено на администратора ([79]); или 5) обработването е необходимо за установяването, упражняването или защитата на правни претенции.

(29) В допълнение към специалните категории лични данни, посочени в съображение 27, в ПЗД се изисква и специална защита за обработването на лични данни, свързани с наказателни присъди и нарушения, т.е. като се разрешава такова обработване само след предварителна консултация с Комитета по защита на данните или когато обработването се изисква от правно обвързващ инструмент, който предвижда подходящи гаранции за правата и свободите на физическите лица ([80]).

2.4.3. *Ограничение в рамките на целта*

(30) Личните данни следва да се обработват с конкретна цел и впоследствие да се използват само дотолкова, доколкото употребата им не е несъвместима с целта на обработването.

(31) Този принцип е гарантиран в член 4, параграф 2, буква б) от ПЗД, съгласно който личните данни трябва да се „събират за конкретни, изрично указани и законни цели и да не се обработват допълнително по начин, който е несъвместим с тези цели“.

(32) Подобно на Регламент (ЕС) 2016/679, ПЗД позволява по-нататъшно обработване (независимо от съвместимостта на целта на по-нататъшното обработване с първоначалната цел) въз основа на изричното съгласие на субекта на данните или въз основа на приложимите правни разпоредби на ЕПО ([81]). Във втория случай в ПЗД се изисква обработването да бъде необходима и пропорционална мярка, с която да се защити цел от широк обществен интерес ([82]).

(33) Когато по-нататъшното обработване не е базирано на тези две основания, в ПЗД е предвидено при оценката на съвместимостта на целта на по-нататъшното обработване с целта, за която личните данни са били първоначално събрани, да бъдат взети предвид редица фактори ([83]). Този подход и факторите, изброени в ПЗД, са идентични с посочените в член 6, параграф 4 от Регламент (ЕС) 2016/679 и член 6 от Регламент (ЕС) 2018/1725 ([84]).

2.4.4. *Точност и свеждане до минимум на данните, ограничаване на съхранението и сигурност на данните*

(34) Личните данни следва да бъдат точни и при необходимост да се актуализират. Те следва също така да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват, и по принцип да се съхраняват не по-дълго от необходимото за целите, за които се обработват.

(35) Тези принципи са установени в член 4, параграф 2, буква в), г) и д) от ПЗД по същия начин, както в Регламент (ЕС) 2016/679.

([79]) Например в контекста на жалби срещу издаден патент чувствителни данни могат да бъдат включени в свидетелски показания или представени доказателства. Обработването съгласно тази разпоредба може да се извършва и ако това е съществено необходимо за управлението и функционирането на Ведомството и за задълженията, произтичащи от задължението на ЕПО за сътрудничество с договарящите държави (например необходимостта от обработка на здравна информация на персонала или посетителите в съответствие с изискванията, наложени от органите в областта на общественото здраве на приемащата държава от ЕПО). Във всеки случай правният инструмент, на който се основава обработването, трябва да бъде пропорционален на преследваната цел, да зачита същността на правото на защита на данните и да предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните (член 11, параграф 2, буква е) от ПЗД).

([80]) Член 12 от ПЗД. Един възможен сценарий, при който такива данни ще бъдат обработени, е дисциплинарно производство срещу представители по индустриална собственост пред дисциплинарната комисия на ЕПО (вж. например т. A.7 от приложението към Решението *PGP*).

([81]) Член 6, параграф 2 от ПЗД.

([82]) Например сигурността на организацията; предотвратяването, разследването, разкриването и съдебното преследване на престъпления; правата и свободите на другите, и др. (вж. член 25, параграф 1 от ПЗД).

([83]) Член 6, параграф 3 от ПЗД.

([84]) По-специално всяка връзка между целта на събирането и целта на предвиденото по-нататъшно обработване; контекста, в който са били събрани данните; естеството на данните; и възможните последици от по-нататъшното обработване за физическите лица (вж. член 6, параграф 3 от ПЗД).

(36) Личните данни също трябва да се обработват по начин, който гарантира тяхната сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане. За тази цел стопанските субекти трябва да предприемат подходящи технически или организационни мерки за защита на личните данни от възможни заплахи. Тези мерки трябва да се оценяват, като се вземат предвид достиженията на техническия прогрес и съответните разходи.

(37) Сигурността на данните е залегнала в правната рамка на ЕПО чрез принципа на цялостност и поверителност, установен в член 4, параграф 2, буква е) и член 33 от ПЗД, по почти същия начин като в Регламент (ЕС) 2016/679. По-специално в ПЗД се изисква да се гарантира ниво на сигурност, съответстващо на риска, чрез подходящи технически и организационни мерки, като се вземат предвид достиженията на съвременните технологии, разходите за изпълнение и естеството, обхватът, контекстът и целите на обработването, както и различната вероятност и тежест на всички рискове за правата и свободите на физическите лица.

(38) Освен това в ПЗД се съдържат специфични изисквания относно разглеждането и уведомяването за нарушение на сигурността на данните ([85]). Най-напред администраторът е длъжен да уведоми ДЛЗД за нарушение на сигурността на данните без ненужно забавяне (и когато е осъществимо, не по-късно от 72 часа, след като е узнал за него), освен ако има малка вероятност нарушението да доведе до риск за правата и свободите на физическите лица ([86]). По подобен начин обработващият лични данни е длъжен да уведоми администратора за нарушение без ненужно забавяне ([87]). В уведомлението трябва по-конкретно да се опише естеството на нарушението, вероятните последици от него и мерките, които са предприети или се предлага да бъдат предприети за справяне с нарушението ([88]). Когато има вероятност нарушението на сигурността на данните да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, трябва да съобщи за нарушението на субекта на данните ([89]). В съобщението до субекта на данните трябва да се опише естеството на нарушението на сигурността на личните данни на ясен и прост език ([90]), като съобщението не е необходимо, ако администраторът е предприел последващи мерки, които гарантират, че високият риск за правата и свободите на субектите на данни вече не съществува ([91]).

2.4.5. ***Прозрачност***

(39) Субектите на данни следва да бъдат информирани за основните характеристики на обработването на техните лични данни.

(40) В съответствие с ПЗД администраторът е длъжен в момента на получаване на личните данни да предостави на физическите лица информация за своята самоличност и координати за връзка (както и координатите за връзка на ДЛЗД), за целта на обработването и за правното основание за него, за получателите или категориите получатели, за факта, че възнамерява да предаде данните извън ЕПО, както и за приложимите права и възможността за получаване на правна защита ([92]). Същото се отнася и за случаите, в които личните данни се обработват за цел, различна от тази, за която са били събрани ([93]). И двете задължения се прилагат само доколкото съответното лице все още не разполага с тази информация ([94]).

(41) Същата информация трябва да бъде предоставяна на субектите на данни, когато личните данни не се събират пряко от тях, заедно с допълнителна информация относно източника на личните данни и засегнатите категории данни ([95]). Тази информация трябва да бъде предоставена в разумен срок след получаването на данните (но най-късно в срок до един месец), като се отчитат конкретните обстоятелства, при които личните данни се обработват ([96]). В случай че лични данни трябва да се използват за комуникация със субекта на данните, същата информация следва да бъде предоставена най-късно в момента на първата комуникация с физическото лице ([97]). Информацията, посочена в съображение 40, трябва също така да бъде предоставена преди всяко по-нататъшно обработване или, ако се предвижда разкриване на

([85]) „Нарушение на сигурността на данните“ означава „нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин“; вж. член 3, параграф 1, буква н) от ПЗД.
([86]) Член 34, параграф 1 от ПЗД.
([87]) Член 34, параграф 2 от ПЗД.
([88]) Член 34, параграфи 1 и 3 от ПЗД.
([89]) Член 34, параграф 6 от ПЗД.
([90]) Член 34, параграф 6 от ПЗД.
([91]) Член 34, параграф 8 от ПЗД.
([92]) Член 16, параграфи 1 и 2 от ПЗД.
([93]) Член 16, параграф 3 от ПЗД.
([94]) Член 16, параграф 4 от ПЗД.
([95]) Член 17, параграфи 1 и 2 от ПЗД.
([96]) Член 17, параграф 3, буква а) от ПЗД.
([97]) Член 17, параграф 3, буква б) от ПЗД.

друг получател, най-късно когато личните данни се разкриват на трета страна ([98]). Това задължение не важи в редица случаи, а именно когато субектът на данни вече разполага със съответната информация; когато тази информация трябва да остане поверителна поради задължение за професионална тайна, уредено въз основа на ЕПК и/или други правни разпоредби, приложими за ЕПО ([99]); когато предоставянето на тази информация се окаже невъзможно или би изисквало непропорционално големи усилия, по-специално за обработване с цел архивиране, научни или исторически изследвания или статистически данни, доколкото това би направило невъзможно или сериозно би възпрепятствало постигането на целите на обработването; или когато получаването или разкриването на тази информация е изрично предвидено в ЕПК или в други приложими правни разпоредби, които предвиждат подходящи мерки за защита на законните интереси на субекта на данните ([100]).

2.4.6. ***Индивидуални права***

(42) Субектите на данни следва да имат определени права, които могат да бъдат противопоставени на администратора или на обработващия лични данни, по-специално правото на достъп до данните, правото на коригиране, правото на възражение срещу тяхното обработване и правото данните да бъдат заличени. В същото време тези права може да бъдат обект на ограничения, доколкото ограниченията са необходими и пропорционални с цел да се гарантират важни цели от широк обществен интерес.

2.4.6.1. *Права, предоставени от ПЗД*

(43) В член 1Б, параграф 4 от Служебния правилник е установена необходимостта от улесняване на упражняването на индивидуалните права. За по-нататъшното изпълнение на това изискване, ПЗД предоставя на физическите лица същите права като предвидените в Регламент (ЕС) 2016/679, а именно право на достъп (член 18 от ПЗД), право на коригиране (член 19 от ПЗД), право на изтриване (член 20 от ПЗД), право на ограничаване на обработването (член 21 от ПЗД), право на преносимост на данните (член 22 от ПЗД), право на възражение (член 23 от ПЗД) и право да не подлежат на автоматизирано вземане на решения (член 24 от ПЗД).

(44) В ПЗД се определят и общи разпоредби за обработването на искания за упражняване на права от физически лица, като от администратора се изисква да общува със субектите на данни на ясен и прост език и в сбита, прозрачна, разбираема и леснодостъпна форма (писмено или по друг начин) ([101]). Администраторът трябва да предостави на физическите лица информация относно мерките, предприети в отговор на искане, без ненужно забавяне и при всички случаи в срок от един месец от получаването на искането (който може да бъде удължен с още два месеца, когато това е необходимо с оглед на сложността и броя на исканията) ([102]). Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може да откаже да предприеме действия по искането ([103]). Когато администраторът не предприеме действия по дадено искане, той трябва да информира физическото лице за това и да предостави информация относно възможността за търсене на правна защита ([104]).

([98]) Член 17, параграф 3, буква в) и член 17, параграф 4 от ПЗД. Съгласно определението в член 3, параграф 1, буква л) от ПЗД "трета страна" означава всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различни от съответното физическо лице, администратора, обработващия данните и лицата, които, бидейки под прякото ръководство на администратора или обработващия данните, имат право да обработват данните.

([99]) Член 17, параграф 4 от ПЗД. Подобни изисквания за поверителност се прилагат например в контекста на обработването на лични данни на персонала от медицинската служба на ЕПО (в който случай съответните практикуващи специалисти могат да бъдат задължени да пазят професионална тайна, вж. например член 11, параграф 3 от ПЗД и Правилника за прилагане на членове 83а, 84 и 84а от Служебния правилник, параграф Д) или в контекста на процедури за наемане на работа (раздел 6 от приложение II — Състезателни процедури за постове, за които председателят на Ведомството изпълнява ролята на орган по назначаването).

([100]) Т.е. когато ЕПК или приети въз основа на нея правни инструменти уреждат конкретно информацията, която трябва да бъде разкрита на физически лица или на обществеността, вж. по-подробно раздел 1.4.6.7 по-долу.

([101]) Член 15, параграф 1 от ПЗД.

([102]) Член 15, параграф 2 от ПЗД.

([103]) Член 15, параграф 4 от ПЗД. Освен това в член 13, параграф 2 от ПЗД се пояснява, че ако администраторът може да докаже, че не е в състояние да идентифицира субекта на данните, разпоредбите относно индивидуалните права не се прилагат (освен ако субектът на данни предостави допълнителна информация, позволяваща неговото идентифициране).

([104]) Член 15, параграф 3 от ПЗД.

(45) Първо, що се отнася до правото на достъп, ПЗД предоставя на физическите лица правото да получат от ЕПО потвърждение дали се обработват засягащи ги лични данни или не, и ако това е така, да получат лесен достъп до личните данни ([105]) на разумни интервали от време ([106]). Освен това физическите лица имат право да получат информация, по-специално относно целта на обработването, засегнатите категории данни, получателите, с които се споделят данните, и предвидения срок, за който данните ще се съхраняват ([107]).

(46) Второ, в ПЗД се посочва, че правото на коригиране, предвидено в ПЗД, позволява на физическите лица неточни техни данни да бъдат коригирани или непълни данни — допълнени (например чрез предоставяне на допълнителна декларация) ([108]). След коригирането администраторът е длъжен да съобщи за него на всеки получател, на когото са били разкрити личните данни ([109]). Съгласно ПЗД правото на коригиране се прилага за обективни и фактически данни, а не за субективни твърдения ([110]), въпреки че в този случай физическите лица имат право да допълват съществуващите данни с второ становище или контраекспертиза или да представят коментари ([111]).

(47) Трето, ПЗД също така предоставя на физическите лица право на изтриване ([112]), по-специално ако а) личните данни вече не са необходими за целта, за която се обработват; б) субектът на данните оттегли съгласието си и няма друго правно основание за обработването; в) субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество; г) данните са били обработени незаконосъобразно; или д) данните трябва да бъдат изтрити, за да се спази правно задължение, което важи за администратора ([113]). Администраторът трябва да съобщи за всяко изтриване на всеки получател, с когото данните са били споделени, освен ако това се окаже невъзможно или изисква несъразмерно големи усилия ([114]). По подобен начин, ако администраторът е направил личните данни обществено достояние, той трябва да предприеме разумни стъпки, за да информира другите администратори, които ги обработват, че физическото лице е поискало изтриване на данните ([115]). Правото на изтриване не се прилага за следните сценарии, доколкото обработването на данните е необходимо: а) за упражняване на правото на свобода на изразяване на мнение и свобода на информация; б) за спазване на правно задължение на ЕПО или задължение, произтичащо от задължението на ЕПО да сътрудничи на договарящите държави ([116]), или за упражняване на официални правомощия, предоставени на ЕПО ([117]); в) от съображения за сътрудничество с договарящите държави в областта на общественото здраве ([118]); г) за целите на архивирането, научните или историческите изследвания и статистическите цели (доколкото има вероятност изтриването да направи невъзможно или сериозно да затрудни постигането на целите на обработването); или д) за установяването, упражняването или защитата на правни претенции ([119]).

([105]) По-специално администраторът трябва да предостави копие в разбираема форма на данните, които са в процес на обработване, и на цялата налична информация (от всякакъв вид, независимо от нейното естество (обективно или субективно), съдържание (включително всякакъв вид предприета дейност) или формат (досие на хартиен носител, компютърни записи, електронни писма); вж. член 18, параграф 3 от ПЗД. Същевременно правото на получаване на копие от данните не може да засегне неблагоприятно правата и свободите на други лица (член 18, параграф 5 от ПЗД).

([106]) Член 18, параграф 1 от ПЗД.

([107]) Член 18, параграфи 2 и 3 от ПЗД.

([108]) Член 19, параграф 1 от ПЗД.

([109]) Член 19, параграф 3 от ПЗД. Ако субектът на данни поиска това, администраторът трябва да го информира за тези получатели.

([110]) Това тълкуване бе прието в съответствие с Насоките на ЕНОЗД относно правата на физическите лица при обработването на лични данни. https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf. Вж. по-специално, стр. 18, насоки относно правото на коригиране, във връзка с „обективни и фактически данни“ и „субективни твърдения“.

([111]) Член 19, параграф 2 от ПЗД.

([112]) Изтриването на данни означава „заличаване на съхранявани данни по начин, който не позволява възстановяването им“ (член 3, параграф 1, буква х) от ПЗД). Позоваването на „съхранявани данни“ обхваща всички данни, събрани и съхранявани от администратора (и всички трети страни от името на администратора).

([113]) Член 20, параграф 1 от ПЗД.

([114]) Член 20, параграф 4 от ПЗД.

([115]) Член 20, параграф 2 от ПЗД.

([116]) Съгласно член 20 от Протокола за привилегиите и имунитетите на ЕПО от ЕПО може да се изисква да предостави лични данни на договарящите държави в рамките на административни или съдебни производства, например за изчисляване и прехвърляне на пенсионни права на персонала, за данъчни разследвания или в контекста на граждански дела срещу служители на ЕПО.

([117]) Тук става въпрос за ситуации, при които съгласно ЕПК, ДПК или правни инструменти, приети на тази основа, от ЕПО се изисква да обработва лични данни във връзка с процедурата за издаване на патенти (например поддържане на информация в Европейския патентен регистър и Европейския патентен бюлетин съгласно член 127 и 129 от ЕПК).

([118]) Обработването на здравни данни по причини от обществен интерес в областта на общественото здраве трябва да бъде в съответствие с член 11, параграф 2, буква ж) от ПЗД.

([119]) Член 20, параграф 3 от ПЗД.

(48) Четвърто, член 21 от ПЗД предвижда право на ограничаване на обработването, т.е. маркиране на лични данни с цел ограничаване на обработването им в бъдеще (включително програмни мерки за трайно възпрепятстване на достъпа до такива данни) ([120]). По-конкретно позоваване на това право може да се направи, когато точността на личните данни е оспорена от физическото лице (за срок, изискван от администратора, за да се провери точността) или когато обработването е незаконосъобразно, но физическото лице се противопоставя на изтриването на данните ([121]). Когато обработването е ограничено, личните данни могат, с изключение на съхранението, да се обработват само с изричното съгласие на физическото лице за установяване, упражняване или защита на правни претенции, за защита на правата на други лица или за изпълнение на задача, изпълнявана при осъществяването на официалните дейности на ЕПО (т.е. задача, която е необходима за административната и техническата работа, която ЕПО е длъжна да извършва в съответствие с ЕПК) ([122]).

(49) Пето, правото на възражение е установено в член 1Б, параграф 4 от Служебния правилник и в член 23 от ПЗД. По-специално физическите лица имат право по всяко време да възразят срещу обработването на лични данни, извършвано за изпълнението на задача при упражняването на официалните дейности на ЕПО или при законното упражняване на официалните правомощия, предоставени на администратора ([123]). Физическите лица трябва да бъдат информирани за съществуването на такова право по ясен начин и най-късно в момента на първата комуникация с тях ([124]). В случай че дадено лице възрази срещу обработването на лични данни, в ПЗД се изисква администраторът да прекрати обработването, освен ако е в състояние да докаже наличието на убедителни законни основания за обработването, които имат преимущество пред интересите, правата и свободите на субекта на данните, или за установяването, упражняването или защитата на правни претенции ([125]).

(50) Шесто, с ПЗД се установява право на преносимост на данните, като на физическите лица се предоставя възможност да получават своите лични данни в структуриран, широко използван и машинночетим формат и да предават тези данни на друг администратор ([126]). Това право важи, когато обработването се извършва с автоматизирани средства и въз основа на съгласието на физическото лице или за изпълнението на договор с физическото лице или в негов интерес ([127]).

(51) Накрая, съгласно ПЗД физическите лица имат право да не бъдат обект на автоматизирано вземане на решения, т.е. на решение, основаващо се единствено на автоматизирано обработване, включително профилиране, което поражда правни последици за тях или по подобен начин ги засяга в значителна степен ([128]). В ПЗД се посочва, че автоматизирано вземане на решения може да се извършва, когато се основава на изричното съгласие на субекта на данните или ако е необходимо за сключването или изпълнението на договор с физическото лице, като в този случай администраторът трябва да осигури подходящи гаранции, като например чрез предоставяне на правото на получаване на човешка намеса, изразяване на гледната точка на физическите лица и оспорване на решението ([129]). Автоматизираното вземане на решения може да бъде разрешено и с правен акт, ако в този акт се предвиждат подходящи мерки за защита на правата на физическите лица ([130]). Ако администраторът участва в автоматизирано вземане на решения, включително профилиране, той трябва проактивно да информира лицето за това като част от задълженията си за прозрачност и да предостави съдържателна информация относно използваната логика, както и относно значението и предвидените последици от подобно обработване за субекта на данните ([131]). Същата информация трябва да бъде предоставена при поискване ([132]).

([120]) Член 3, параграф 1, буква в) от ПЗД.

([121]) Член 21, параграф 1 от ПЗД.

([122]) Член 21, параграф 2 от ПЗД.

([123]) Когато в рамките на процедурата за издаване на патент ЕПО трябва по закон, т.е. съгласно ЕПК и ДПК, да обработва лични данни, физическите лица не могат да възразят срещу обработването; вж. точка 28 от приложението към Решение *PGP*. Когато лични данни се обработват за научни или исторически изследвания или за статистически цели, субектите на данни имат право да възразят на основания, свързани с тяхното конкретно положение, срещу обработването на лични данни, освен ако обработването е необходимо за изпълнението на задача, изпълнявана при законното упражняване на официалните правомощия, предоставени на администратора, включително обработването, необходимо за управлението и функционирането на Ведомството (член 23, параграф 4 от ПЗД).

([124]) Член 23, параграф 2 от ПЗД.

([125]) Член 23, параграф 1 от ПЗД.

([126]) Член 22, параграф 1 от ПЗД.

([127]) Тъй като обработването на лични данни в контекста на процедурата за издаване на патент не се базира на нито едно от тези основания, правото на преносимост на данните не се прилага в този контекст; вж. точки 29—30 от приложението към Решение *PGP*.

([128]) Член 24, параграф 1 от ПЗД. Съгласно определението в член 3, параграф 1, буква г) от ПЗД „профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здравословно състояние, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.

([129]) Член 24, параграф 3 от ПЗД.

([130]) Член 24, параграф 2, буква б) от ПЗД.

([131]) Вж, член 16, параграф 2, буква е) и член 17, параграф 2, буква е) от ПЗД.

([132]) Член 18, параграф 1, буква з) от ПЗД.

2.4.6.2. *Ограничения на индивидуалните права*

(52) Подобно на член 23 от Регламент (ЕС) 2016/679 и член 25 от Регламент (ЕС) 2018/1725, в член 25 от ПЗД се предвижда, че със специфични правни разпоредби в правната рамка на ЕПО може да се ограничава прилагането на правата, посочени в съображения 43—51 ([133]) (т.е. временно да се ограничи тяхното прилагане) ([134]), когато подобно ограничение е съобразено със същността на основните права ([135]) и свободи и е необходима и пропорционална мярка в едно демократично общество за гарантиране на конкретни цели ([136]). Освен това ограничението трябва да бъде предвидено в „ясни и точни“ разпоредби, които имат за цел да породят правни последици по отношение на субектите на данни и които трябва да бъдат приети най-малко на равнището на председателя на Ведомството ([137]). Подобни разпоредби трябва по-специално да определят целта на обработването, обхвата на ограничението, предпазните мерки за предотвратяване на злоупотреби, сроковете за съхранение и приложимите гаранции ([138]).

(53) Понастоящем единственият правен инструмент, който предвижда ограничения на индивидуалните права, е Циркулярно писмо 420 (правно обвързващ инструмент, приет от председателя). В него се изяснява как и при какви условия администраторът може да прилага ограничения и се определят изчерпателно конкретните сценарии, при които правата могат да бъдат ограничавани, както и за кои цели ([139]). По-специално в него се предвижда, че ЕПО може да ограничава индивидуалните права за определени конкретни цели: а) и б) при провеждане на разследвания или дисциплинарни производства по отношение на своите служители ([140]); в) в контекста на вътрешното уреждане на спорове или установяването, упражняването или защитата на правни претенции, включително при арбитраж, с цел запазване на поверителността на информация и документи, получени от страните, встъпилите страни или други законни източници; г) при обработване на здравни данни в медицински процедури и досиета, но само за да се защитят правата на физическите лица ([141]); д) и е) при провеждане на вътрешни одити и проверки (последните се извършват от ДЛЗД); ж) за целите на управлението на ИТ инциденти и доклади за инциденти, свързани с физическата сигурност; и з) когато предоставя или получава съдействие на или от компетентни публични органи, включително от договарящите държави на ЕПО и международни организации, или когато си сътрудничи с тях по дейности, определени в съответните споразумения за нивото на обслужване, меморандуми за разбирателство и споразумения за сътрудничество, по тяхно искане или по собствена инициатива на Ведомството ([142]).

([133]) С изключение на правото на възражение, за което Циркулярно писмо 420 не предвижда никакви ограничения; вж. член 3, параграф 3. Освен това съгласно член 9 от Циркулярно писмо 420 ЕПО може да ограничи съобщаването на дадено нарушение на сигурността на данните на определено физическо лице.

([134]) Вж. определението за „ограничения“ в член 2 от Циркулярно писмо 420.

([135]) Ограничения, които са толкова широкообхватни и инвазивни, че на практика изпразват основно право от съдържанието му и възпрепятстват физическото лице да го упражнява, не могат да бъдат основателни; вж. член 4, параграф 3 от Циркулярно писмо 420.

([136]) Това означава сигурността на ЕПО, обществената сигурност или отбраната на договарящите държави; предотвратяването, разследването, разкриването и наказателното преследване на престъпления или изпълнението на наказания, включително защитата срещу и предотвратяването на заплахи за обществената сигурност; други съществени интереси на ЕПО, свързани с основната ѝ мисия, или във връзка със задължения, произтичащи от задължението за сътрудничество с договарящите държави, включително парични, бюджетни и данъчни въпроси, обществено здраве и социална сигурност; вътрешната сигурност на Ведомството, включително на неговите електронни съобщителни мрежи; защитата на независимостта на съдебната и квазисъдебната власт и на съдебните и квазисъдебните производства; предотвратяването, разследването, разкриването и наказването на нарушения на етичните кодекси при регламентираните професии; контролна, инспекционна или регулаторна функция, свързана, дори само понякога, с упражняването на официални правомощия; защитата на субекта на данните или правата и свободите на други лица и изпълнението на гражданскоправни искове (член 25, параграф 1 от ПЗД).

([137]) Член 25, параграф 3 от ПЗД.

([138]) Член 25, параграф 2 от ПЗД.

([139]) Член 1 от Циркулярно писмо 420.

([140]) Член 4, параграф 1, букви а) и б) от Циркулярно писмо 420.

([141]) Това се отнася само до обработването на здравни данни на служителите на ЕПО (и не е от пряко значение за целите на установяването на адекватното ниво на защита, което се отнася до обработването на данни, предавани от администратор или обработващ лични данни, за който се прилага ОРЗД). В член 8 от Циркулярно писмо 420 допълнително се пояснява как могат да се прилагат ограничения на правото на достъп до медицински данни/досиета. По-специално се уточнява, че подобно ограничение може да се прилага само по отношение на правото на пряк достъп до техните лични медицински данни и/или досиета от психологическо или психиатрично естество, които се обработват от Ведомството, но само ако има вероятност достъпът до тези данни да засегне неблагоприятно и да представлява непосредствена опасност за живота и здравето на субекта на данните или на други лица.

([142]) Член 4, параграф 1 от Циркулярно писмо 420. Тази разпоредба обикновено се отнася само до личните данни на служителите на ЕПО. Тя се отнася до случаите, в които ЕПО е длъжна да си сътрудничи с националните органи на договарящите държави съгласно член 131 от ЕПК (с който се урежда сътрудничеството между ЕПО и националните съдилища на договарящите държави при разследвания/производства, свързани с издаването на патенти) и съгласно член 20, параграф 1 от Протокола за привилегиите и имунитетите на ЕПО (вж. също точка 95). Такъв може да бъде например случаят, когато от служители на ЕПО се иска да свидетелстват пред национален съд на договаряща държава в контекста на национално наказателно производство, или когато от ЕПО се иска да предостави информация за заплатите на своя персонал в граждански (семейноправни) производства и т.н.

(54) Администраторът определя, с оглед на съответните обстоятелства, дали дадено ограничение може да бъде приложено в конкретен случай или не ([143]). Когато решава дали да приложи ограничение, администраторът, с участието на ДЛЗД, първо трябва да прецени дали то е необходимо и пропорционално в конкретния случай ([144]). Тази оценка включва претегляне на потенциалните рискове за правата и свободите на субекта на данните спрямо рисковете и свободите на други субекти на данни и рисковете от възпрепятстване на целта и резултата от операцията по обработване ([145]). Ограниченията трябва да бъдат документирани, включително чрез записване на оценката на ограничените права и за колко време, по какви причини и на какви основания се ограничават ([146]). Освен това, докато се прилага дадено ограничение, трябва да бъдат въведени подходящи технически и организационни мерки ([147]). Всяко ограничение може да се прилага само докато са налице причините за съществуването му ([148]). Ако дадено право е ограничено, администраторът трябва да информира физическото лице за основните причини за това и за правото му да подаде жалба ([149]).

2.4.6.3. *Специфични правила в контекста на процедурата за издаване на патент*

(55) Разпоредбите на учредителния договор на ЕПО (т.е. ЕПК), на ДПК и приложимите съгласно тях разпоредби (взети заедно — първичното законодателство за ЕПО) съдържат определени специфични изисквания в контекста на процедурата за издаване на патенти, които могат да повлияят на упражняването на определени права съгласно ПЗД ([150]). В Решение *PGP* се прави преглед на тези изисквания на първичното законодателство, обяснява се как могат да се упражняват правата на субектите на данни в този контекст и ясно се посочват възможните изключения ([151]). В Циркулярно писмо 420 се посочва, че разпоредбите, които могат да ограничат прилагането на правата за защита на данните, трябва ясно да определят обхвата на всяко изключение и по този начин да балансират различните засегнати интереси ([152]).

(56) Първо, съгласно член 127 от ЕПК Ведомството е длъжно да поддържа Европейския патентен регистър, в който се публикуват някои законно определени лични данни. Съгласно първичното законодателство заявките за патенти трябва да бъдат публикувани по време на процедурата по издаване на патент, обикновено възможно най-скоро след изтичането на срок от осемнадесет месеца от датата на подаване на заявката. В ЕПК се предвижда, че достъпът до личните данни, включени в такива заявки за патенти, може да бъде осъществен чрез проверка на досиетата или чрез проверка на регистъра ([153]). Преди публикуването заявките за патенти не са на разположение за проверка без изричното съгласие на заявителя. Подобни правила са установени в ДПК ([154]).

([143]) Член 2 от Циркулярно писмо 420.

([144]) Член 25, параграф 3, буква а) от ПЗД. Вж. също член 6 от Циркулярно писмо 420.

([145]) Член 5, параграф 5 от Циркулярно писмо 420.

([146]) Член 4, параграф 4 от Циркулярно писмо 420. Тази документация трябва да бъде предоставена на Комитета по защита на данните при поискване (член 4, параграф 7 от циркулярно писмо 420).

([147]) Мерките трябва да включват например сигурно съхранение, защитена електронна среда, която предотвратява незаконен и случаен достъп или предаване на електронни данни на неоправомощени лица, както и наблюдение на ограниченията и периодичен преглед на тяхното прилагане, вж. член 5, параграф 2 от Циркулярно писмо 420.

([148]) Член 4, параграф 5 и член 5, параграф 3 от Циркулярно писмо 420.

([149]) Член 25, параграф 3, буква б) от ПЗД. Тази информация може да бъде отложена, пропусната или отказана, ако би премахнала ефекта от ограничението, вж. член 25, параграф 4 от ПЗД. Това допълнително ограничение може да се прилага само в надлежно обосновани случаи и докато и доколкото това е необходимо и пропорционално (член 7, параграф 4 от Циркулярно писмо 420). Обосновката на подобно ограничение трябва да се преразглежда редовно. В допълнение към специалното изискване за информиране на физическите лица за евентуално ограничение на техните права, ЕПО трябва да предостави обща информация на своя интранет и/или уебсайт за дейностите, които могат да включват ограничения на правата (член 7, параграф 1 от Циркулярно писмо 420).

([150]) Член 2 от Циркулярно писмо 420 (правни разпоредби на ЕПО).

([151]) Член 1 и приложението към Решението *PGP*.

([152]) Член 2 от Циркулярно писмо 420.

([153]) Точки B.13 и B.14 от приложението към Решението *PGP* и член 128 от ЕПК. Някои части от досиетата са изключени от проверката на досиета съгласно член 128, параграф 4 и правило 144 от Правилника за прилагане на ЕПК и решението на председателя на ЕПО от 12.7.2007 г. относно документи, изключени от проверката на досиета (Специално издание № 3, ОВ Европейско патентно ведомство 2007, J.3). Изключените части са следните: документи, свързани с изключването на членове на апелативните състави или на разширения апелативен състав или с възраженията срещу тях; проекти на решения и известия, както и всички други документи, използвани за изготвянето на решения и известия, които не се съобщават на страните; наименованието на изобретателя, ако той се е отказал от правото си да бъде споменат, както и всеки друг документ, изключен от проверка от страна на председателя на Европейското патентно ведомство на основание, че тази проверка няма да служи за информиране на обществеността относно заявката за европейски патент или европейския патент, като например: медицински свидетелства; искания за изключване от проверка на досиета и свързаната с това кореспонденция; информация, чието публикуване би било във вреда на законните лични или икономически интереси и не би включвало информация от значение за процедурата по заявка или издаване на патент.

([154]) Вж. член 3 от Решението на председателя на Ведомството от 20.2.2019 г. относно онлайн проверката на документи, съдържащи се в съхраняваните от Ведомството документи като получаващо ведомство, международен орган за търсене или орган, определен за допълнително търсене (ОВ Европейско патентно ведомство 2019, A17). Вж. в това отношение член 30 от ДПК по отношение на публичния достъп до досиета, както и правила 94 и 48 от ДПК. Ведомството се позовава на тези разпоредби, когато действа като компетентна служба или орган съгласно ДПК в съответствие с членове 151—153 от ЕПК.

(57) Второ, в ЕПК специално е уредена възможността да се правят промени в информацията, използвана в рамките на процедура за издаване на патент ([155]). По-конкретно в ЕПК се предвижда само възможност за поправяне на грешки в документите, подадени до ЕПО ([156]), коригиране на грешки в решенията ([157]), корекции на преводите ([158]) и поправка на наименованието на изобретателя ([159]). Следователно само в тези случаи може да бъде направена поправка на личните данни, включени в документите, използвани в процедурата по издаване на патент. Същото важи и за възможността за получаване на ограничение на обработването на данни ([160]).

(58) Трето, ЕПК налага специфични изисквания за съхранение и публикуване на някои документи, използвани в процедурата по издаване на патенти, които оказват влияние върху възможността за получаване на заличаване на съдържащата се в тях информация, включително личните данни ([161]). По-специално публикуваните заявки за патенти и информацията за патентите, публикувана в Европейския патентен бюлетин, трябва да бъдат запазени и публично достъпни ([162]). В резултат от това заличаването на съдържащите се в тези документи лични данни би било в противоречие с основните правни задължения на ЕПО (член 129, буква а) от ЕПК) и не може да бъде получено. Други досиета трябва да се съхраняват от ЕПО за срок, посочен в ЕПК, който по принцип е пет години ([163]). Докато този срок е приложим, заличаването на информация, съдържаща се в тези досиета (включително лични данни), не може да бъде получено.

(59) Поради това, като се има предвид по-специално ограниченият им обхват и условията за тяхното прилагане, може да се счита, че ограниченията относно упражняването на правата, произтичащи от разпоредбите, посочени в съображения 55—58, се свеждат до това, което е необходимо и пропорционално, за да се гарантира правилното функциониране на процедурата по издаване на патенти, както се изисква в обществен интерес за изпълнението на официалните задачи на ЕПО. Доколкото упражняването на правата на защита на данните не е конкретно регламентирано в ЕПК и ДПК, т.е. във всички други сценарии, различни от описаните в съображения 55—58, изискванията на ПЗД се прилагат изцяло.

2.4.7. ***Последващо предаване на данни***

(60) Нивото на защита на личните данни, което се осигурява за данните, предавани от Съюза на ЕПО, не трябва да бъде подкопавано от по-нататъшното предаване на тези данни на получатели в трета държава или друга международна организация.

(61) В ПЗД се прави разграничение между „изпращане на лични данни“ (т.е. споделяне на данни от ЕПО с договарящите държави) и „предаване на лични данни“ (споделяне на данни от ЕПО с всяко друго лице или образувание извън ЕПО) ([164]).

2.4.7.1. *Изпращане на данни*

(62) Най-напред в ПЗД се предвижда, че може да се извърши изпращане на данни на национална служба за интелектуална собственост на договаряща държава от ЕПО, ако данните са необходими за а) упражняването на компетенции или официални правомощия на получателя и б) изпращането е необходимо за изпълнението на официалните задачи/правомощия на ЕПО ([165]). Тези изпращания се осъществяват в рамките на процедурата по издаване на патенти, предвидена съгласно ЕПК и ДПК ([166]).

([155]) Корекция или поправка съгласно тези разпоредби може да доведе до актуализиране на вписванията в Европейския патентен регистър и Европейския патентен бюлетин и на публикациите на заявката или патента. Това обаче няма да промени със задна дата съдържанието на досието (което ще продължи да съдържа всички изявления на страните и съобщенията и решенията на ЕПО). Това също така няма да доведе до оттегляне или заличаване на по-ранни публикации (точка B.19 от приложението към Решението *PGP*). Това важи и съгласно членове 19 и 34 от ДПК, когато ЕПО действа като компетентен орган/служба въз основа на членове 151—153 от ЕПК.

([156]) Правило 139 от Правилника за прилагане на ЕПК.

([157]) Правило 140 от Правилника за прилагане на ЕПК. В решенията на ЕПО могат да се поправят само езикови грешки, грешки в транскрипцията и явни грешки.

([158]) Член 14, параграф 2, второ изречение от ЕПК.

([159]) Правило 21 от Правилника за прилагане на ЕПК. Неправилното наименование на изобретател може да бъде поправено при поискване и само със съгласието на погрешно посоченото лице, а когато такова искане е подадено от трето лице — със съгласието на заявителя или притежателя на патента.

([160]) Точка B.25 от приложението към Решение *PGP*.

([161]) Точки B.22—B.23 от приложението към Решение *PGP*.

([162]) Член 129 от ЕПК.

([163]) Правило 147, параграфи 4 и 5 от Правилника за прилагане на ЕПК.

([164]) Член 3, параграф 1, букви т) и у) от ПЗД.

([165]) Член 8, параграф 2 от ПЗД.

([166]) Вж. по-специално членове 130, 131 и 135 от ЕПК, както и съответните правила от Правилника за изпълнение на ЕПК (например правила 148—150). Вж. също членове 12, 18, 20 и 36 от ДПК, както и правила 22, 23, 23a, 44, 47 и 71 от Правилника за прилагане.

(63) Освен това ПЗД позволява изпращането на данни на публичен орган на договаряща държава от ЕПО ([167]), когато данните са необходими за изпълнението на задачите на този публичен орган и изпращането е съвместимо със задачите и функционирането на ЕПО ([168]). Подобно изпращане не се изисква изрично съгласно ЕПК или други правни инструменти, уреждащи процедурата по издаване на патенти, но все пак може да е необходимо за изпълнението на задачите на ЕПО, като например сътрудничеството на ЕПО с договарящите държави чрез процеси на консултации; командироването и разполагането на експерти; или предоставянето на информация за служителите на ЕПО с цел определяне на социални обезщетения, данъчни изисквания и др.

(64) ДЛЗД е подготвило образци за клаузи, които да бъдат включени в меморандуми за разбирателство, уреждащи подобно изпращане на данни, описано в съображения 62 и 63, в които между другото се предвиждат принципи за защита на данните, по-нататъшно обработване само за съвместими цели, права за субектите на данни, както и задължения по отношение на сигурността на данните, нарушенията на тази сигурност и независимия надзор ([169]).

(65) И в двата сценария, описани в съображение 62 и 63, получателят съгласно ПЗД трябва да представи доказателства, че е необходимо данните да бъдат изпратени за конкретна цел, произтичаща от задълженията на ЕПО за сътрудничество с договарящата държава или държави ([170]). За всяко изпращане администраторът трябва да е в състояние да демонстрира, че то е необходимо и пропорционално по отношение на конкретната цел, за която се споделят данните ([171]). Всяко предаване на данни трябва да се извършва по начин, който гарантира, че нивото на защита, осигурявано от ПЗД, остава непроменено ([172]). Съгласно насоките, издадени от ДЛЗД, това означава, че са налице подходящи гаранции, включително гаранция, че споделяните данни трябва да бъдат сведени до минимум и ограничени до това, което е адекватно, от значение и строго необходимо за постигането на тази цел ([173]). Ако има причина да се предполага, че законните интереси на съответното лице може да бъдат засегнати, администраторът трябва да установи, че изпращането на личните данни за тази конкретна цел е пропорционално, след като претегли различните интереси в случая ([174]).

(66) По отношение на тези два сценария е важно също така да се отбележи, че всички договарящи държави от ЕПО са страни по Европейската конвенция за защита на правата на човека и основните свободи, се намират под юрисдикцията на Европейския съд по правата на човека и са страни по Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108).

(67) Не на последно място ПЗД позволява изпращането на данни на обработващ лични данни, намиращ се в Европейското икономическо пространство (ЕИП), при условие че се гарантира спазването на изискванията, определени в ПЗД за ангажирането на обработващи лични данни ([175]).

2.4.7.2. *Предаване на данни*

(68) Споделянето на лични данни с всеки субект извън ЕПО, различен от публичен орган или национална служба за интелектуална собственост на договарящите държави от ЕПО, или обработващ лични данни в ЕИП, се счита за „предаване“ на лични данни, подлежащо на специфични изисквания съгласно ПЗД ([176]). Тези изисквания се прилагат например за споделянето на данни с обработващи лични данни извън ЕИП, с администратори, намиращи се в договарящите държави или извън тях, публични органи в държави, различни от договарящите държави, и други международни организации. По принцип в ПЗД се изисква нивото на защита, гарантирано на физическите лица от

([167]) Например национален или местен орган, както и друг публичноправен орган, като например болница или университет.
([168]) Член 8, параграф 1 от ПЗД.
([169]) Преглед на изискването на образеца на клауза за защита на данните на ЕПО за меморандуми за разбирателство, достъпен на адрес https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-template-data-protection-clause-for-mous.pdf.
([170]) Член 8, параграф 3 от ПЗД.
([171]) Член 8, параграф 4 от ПЗД.
([172]) Обяснителна бележка „Изпращане и предаване на лични данни от ЕПО“ (Бележка за изпращането и предаването), на разположение на адрес https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, стр. 4. Вж. по-специално „В ПЗД на Европейското патентно ведомство [...] се определя общият принцип на адекватна защита, особено приложим към международния поток от данни“.
([173]) Бележка за изпращането и предаването, налична в бележка под линия 12.
([174]) Член 8, параграф 3 от ПЗД.
([175]) Член 8, параграфи 1, 2 и 5 от ПЗД.
([176]) Член 9, параграф 1 от ПЗД.

ЕПО, да не се подкопава при предаването на данни на трети страни ([177]). Съгласно насоките на ДЛЗД защитата, предоставена на предадените лични данни в третата държава или международната организация, трябва да бъде „по същество равностойна на защитата, гарантирана в ПЗД“ ([178]).

(69) Съгласно ПЗД предаването на лични данни извън ЕПО може преди всичко да се извърши, ако държавата, в която се намира получателят, или международната организация гарантират адекватно ниво на защита и ако предаването се извършва единствено с цел да се даде възможност на ЕПО да изпълнява задачи в рамките на своята компетентност ([179]). Решение относно адекватното ниво на защита се приема от председателя на Ведомството ([180]), който в случай на съмнение решава след консултация с ДЛЗД и Комитета по защита на данните ([181]). ДЛЗД е разработило „референтен документ относно адекватното ниво на защита“, в който се определят критериите за решенията относно адекватното ниво на защита ([182]). По-специално в правната рамка на третата държава или международната организация трябва да се предвиждат ключови принципи за защита на данните, права на субектите на данни, правила за последващо предаване на данни, процедурни механизми и механизми за правоприлагане и правна защита за физическите лица. Ако председателят приеме решение относно адекватното ниво на защита, предаването може да се извърши без осигуряване на допълнителни гаранции ([183]). Понастоящем ЕПО счита, че държавите членки, както и Норвегия, Исландия и Лихтенщайн, всички държави, които се ползват от решение на Комисията относно адекватното ниво на защита ([184]), и институциите и органите на Съюза осигуряват адекватно ниво на защита ([185]).

(70) Съгласно ПЗД при липса на решение относно адекватното ниво на защита администраторът или обработващият лични данни може да предават лични данни на получатели извън ЕПО само ако администраторът или обработващият лични данни са предоставили подходящи гаранции и при условие че са налице упражняеми права на субектите на данни и ефективни средства за правна защита за субектите на данни ([186]). Подобни подходящи гаранции могат да бъдат включени в административни договорености с публични органи или международни организации, в договорни клаузи (след консултация със Комитета по защита на данните) ([187]) или в механизми за сертифициране ([188]). ДЛЗД е разработило обобщено описание на разпоредбите, които да бъдат включени в административните договорености ([189]). На разположение е и образец на споразумение за защита на данните при предаване на обработващи лични данни ([190]). Съгласно насоките на ДЛЗД ЕПО трябва да прецени дали вносителят на данни би бил възпрепятстван да изпълни задълженията си по инструмент за предаване на данни поради правната рамка, на която е подчинен, и ако е необходимо — да въведе допълнителни мерки ([191]). За да се извърши тази оценка, в обяснителните бележки на ЕПО относно изпращането и предаването на лични данни ДЛЗД препоръчва да се вземат предвид съответните насоки на ЕКЗД и на Европейския надзорен орган по защита на данните ([192]).

(71) Съгласно ПЗД за предаването на данни на държави или организации, които се ползват от решение относно адекватното ниво на защита, както и за предаването на данни въз основа на подходящи гаранции, ЕПО трябва да докаже необходимостта и пропорционалността на всяко предаване за целите на обработването ([193]). Освен това, след като претегли различните засегнати интереси, ЕПО трябва да установи, че предаването е пропорционално, ако има основание да се смята, че законните интереси на субектите на данни могат да бъдат накърнени ([194]). Освен това трябва

([177]) Член 9, параграф 1 от ПЗД.

([178]) Бележка за изпращането и предаването, стр. 11 и бележка под линия 8. „Трета държава“ се определя в ПЗД като държава, която не е договаряща държава по ЕПК; вж. член 3, параграф 1, буква ф) от ПЗД.

([179]) Член 9, параграф 2 от ПЗД.

([180]) Вж. член 1, параграф 2, буква а) от ПЗД във връзка с член 10, параграф 2, буква а) от ЕПК и член 9, параграф 2 от ПЗД.

([181]) Член 9, параграф 3 от ПЗД.

([182]) Кратко описание на референтния справочник на ЕПО, достъпен на адрес https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-adequacy-referential-methodology.pdf.

([183]) Бележка под линия 49 от Бележката за изпращането и предаването.

([184]) С изключение на Рамката за защита на личните данни между ЕС и САЩ.

([185]) Вж. Решение на председателя на Европейското патентно ведомство от 17 ноември 2022 г. относно държави и образувания, за които се счита, че осигуряват адекватна защита на личните данни, достъпно на адрес https://www.epo.org/en/legal/official-journal/2022/12/a111.html.

([186]) Член 9, параграфи 4 и 5 от ПЗД.

([187]) В това отношение насоките на ДЛЗД се позовават на стандартните договорни клаузи, приети от Европейската комисия, като предоставящи добър обзор на гаранциите, които трябва да бъдат включени. Вж. Бележката за изпращането и предаването, стр. 8.

([188]) Член 9, параграф 5 от ПЗД. Вж. също Бележката за изпращането и предаването, стр. 8.

([189]) Общ преглед на изискването на образците на ЕПО за административни договорености, достъпен на адрес https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-epo's-administrative-arrangements-modules.pdf.

([190]) Вж. приложение Д към общите условия на договора за ЕПО, достъпно на адрес https://link.epo.org/web/general_conditions_of_contract_en.pdf.

([191]) Бележка за изпращането и предаването, стр. 9.

([192]) Бележка за изпращането и предаването, стр. 9.

([193]) Член 9, параграф 6 от ПЗД. В случай че има причина да се предположи, че законният интерес на субекта на данните може да бъде накърнен, администраторът трябва да докаже, че предаването е пропорционално за тази конкретна цел, след като е претеглил различните конкуриращи се интереси.

([194]) Член 9, параграф 6 от ПЗД.

да се гарантира (чрез договорни гаранции), че получателят може да обработва или използва данните само за целите, за които те са били предадени, и трябва да ги изтрие веднага след като целта бъде постигната ([195]).

(72) Съгласно ПЗД при липса на решение относно адекватното ниво на защита или на подходящи гаранции предаването на лични данни извън ЕПО е допустимо „само по изключение“, ако се прилага т.нар. „дерогация“ при условия, сходни с тези в съответните разпоредби на правото на Съюза в областта на защитата на данните ([196]). Случаят е такъв, когато а) субектът на данните изрично е дал съгласието си за предаването ([197]); б) и в) предаването е спорадично и е необходимо за изпълнението на договор със субекта на данните или в негов интерес (или за изпълнението на преддоговорни мерки по искане на субекта на данните) ([198]); г) предаването е необходимо за изпълнението на задача при упражняването на официалните дейности на ЕПО или при легитимното упражняване на официални правомощия, предоставено на администратора ([199]); д) предаването е спорадично и необходимо за установяването, упражняването или защитата на правни претенции ([200]); е) предаването е необходимо, за да бъдат защитени жизненоважните интереси на физическо лице, когато субектът на данните е физически или юридически неспособен да даде своето изрично съгласие ([201]); или ж) предаването се извършва от регистър, предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, доколкото условията за подобна справка са изпълнени в конкретния случай ([202]). По своята същност и съгласно насоките на ДЛЗД тези дерогации не могат да се използват за систематично и редовно предаване на данни ([203]).

(73) Не на последно място, що се отнася до предаването на специфични категории данни на държави или организации, които не се ползват от решение относно адекватното ниво на защита, председателят може допълнително да ограничи такова предаване по важни причини, свързани със легитимното упражняване на официалните правомощия, предоставени на Ведомството ([204]). Досега председателят не се е възползвал от тези правомощия.

2.4.8. ***Отчетност***

(74) Съгласно принципа на отчетност образуванията, които обработват данни, са длъжни да въведат подходящи технически и организационни мерки за ефективно спазване на своите задължения за защита на данните, както и да могат да докажат това спазване, по-специално пред компетентния надзорен орган.

(75) В член 4, параграф 1 от ПЗД се установява общ принцип на отчетност, като се пояснява, че администраторът носи отговорност и трябва да може да докаже спазването на ПЗД. По-специално администраторът трябва да прилага подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже съответствие, като взема предвид естеството, обхвата, контекста и целите на обработването, както и различната вероятност и тежест на всички рискове за правата на физическите лица ([205]). В това отношение с ПЗД също така се прилагат принципите на

([195]) Член 9, параграф 6 от ПЗД.

([196]) Вж. член 10 от ПЗД, както и Бележката за изпращането и предаването, стр. 9—11.

([197]) Член 10, параграф 1, буква а) от ПЗД. В този случай лицето трябва да бъде информирано за възможните рискове поради липсата на адекватно ниво на защита и подходящи гаранции. ЕПО не може да използва тази дерогация при упражняването на официалните си дейности (член 10, параграф 2 от ПЗД).

([198]) Член 10, параграф 1, букви б) и в) и член 10, параграф 2 от ПЗД. ЕПО не може да използва тези дерогации при упражняването на официалните си дейности (член 10, параграф 2 от ПЗД).

([199]) Член 10, параграф 1, буква г) от ПЗД. Тези официални дейности или правомощия трябва да бъдат установени въз основа на ЕПК или други приложими правни разпоредби на Европейската патентна организация (член 10, параграф 4 от ПЗД). Това включва обработването, необходимо за управлението и функционирането на Ведомството или за изпълнението на задълженията, произтичащи от задължението на ЕПО за сътрудничество с договарящите държави. Предаване на данни може да се извършва например за изпълнение на задължения между Ведомството и национални органи, данъчни или митнически администрации, органи за финансов надзор и служби, компетентни по въпросите на социалната сигурност или общественото здраве, например в случай на проследяване на контакти при заразни болести (член 10, параграф 6 от ПЗД).

([200]) Член 10, параграф 1, буква д) и член 10, параграф 2 от ПЗД.

([201]) Член 10, параграф 1, буква е) от ПЗД.

([202]) Член 10, параграф 1, буква ж) от ПЗД. Освен ако това е разрешено от правните разпоредби на Европейската патентна организация, подобно предаване не може да включва всички лични данни или цели категории данни, съдържащи се в регистъра, а когато регистърът е предназначен за справка от лица, които имат законен интерес, предаването следва да се извършва единствено по искане на тези лица или ако те са получателите, като се вземат изцяло под внимание интересите и основните права на субекта на данните (член 10, параграфи 2 и 5 от ПЗД).

([203]) Бележка за изпращането и предаването, стр. 10.

([204]) Което, както бе споменато по-горе, включва обработването, необходимо за неговото управление и функциониране или за изпълнението на задължения в рамките на сътрудничеството му с договарящите държави. Вж. член 10, параграф 6 от ПЗД.

([205]) Член 26, параграф 1 от ПЗД.

защита личния живот още при проектирането и по подразбиране, като от администратора се изисква да прилага мерки за прилагане на принципите за защита на данните и да гарантира спазването на ПЗД, както и че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването ([206]).

(76) Администраторът и обработващите лични данни трябва да поддържат регистър на дейностите по обработване, който съдържа, наред с другото, информация относно целта на обработването, категориите обработвани данни, категориите получатели, на които се разкриват данните, и всяко предаване на лични данни ([207]). Тези записи по принцип са публично достъпни (освен ако не съдържат поверителна информация) и са включени в публично достъпен регистър за защита на данните и трябва да бъдат предоставени на разположение на Комитета по защита на данните при поискване ([208]). Всяко оперативно звено трябва също така да назначи поне едно лице за връзка по защитата на данните (за срок от една до три години с възможност за подновяване на мандата), което трябва да премине задължително обучение по защита на данните и да подпомага администратора при изпълнението на неговите задължения ([209]).

(77) Не на последно място ПЗД предоставя различни инструменти, които могат да подпомогнат администратора и обработващите лични данни в усилията им за осигуряване на спазване на изискванията. Например съгласно ПЗД придържането към одобрени механизми за сертифициране може да послужи като доказателство за спазване на задълженията по ПЗД ([210]). Освен това при определени условия ПЗД изисква извършването на оценка на въздействието върху защитата на данните или предварителна консултация с ДЛЗД и Комитета по защита на данните. Оценка на въздействието върху защитата на данните се изисква, когато има вероятност даден вид обработване да доведе до висок риск за правата и свободите на дадено лице ([211]). Това се изисква например, когато е налице систематична и подробна оценка на личните аспекти, на които се основават автоматизираните решения, или когато е налице широкомащабно обработване на специални категории данни ([212]). Ако оценката на въздействието покаже, че обработването би довело до висок риск за правата и свободите на физическите лица и рискът не може да бъде ограничен чрез разумни мерки за сигурност, администраторът трябва да се консултира с Комитета по защита на данните ([213]). Комитетът по защита на данните трябва да предостави писмено становище, ако е на мнение, че планираното обработване би било в нарушение на ПЗД ([214]). В по-общ план от администратора се изисква да се консултира с ДЛЗД при изготвянето на правила или оперативни документи относно прилагането на ограничения на индивидуални права ([215]).

2.5. **Надзор и привеждане в изпълнение**

(78) С цел да се гарантира, че адекватното ниво на защита на данните се осигурява и на практика, следва да има независим надзорен орган с правомощия за наблюдение и осигуряване на спазването на правилата за защита на данните. Този орган следва да действа с пълна независимост и безпристрастност при изпълнението на своите задължения и при упражняването на правомощията си.

(79) Съгласно правната рамка на ЕПО два органа упражняват надзор върху спазването на правилата за защита на данните от страна на ЕПО: ДЛЗД и Комитетът по защита на данните. Двата органа са създадени по силата на член 32А от Служебния правилник, а техният статут и правомощия са допълнително уточнени в ПЗД ([216]). Техните роли се допълват взаимно и включват сътрудничество, като същевременно всеки орган остава независим при изпълнението на съответните си функции.

([206]) Член 27, параграфи 1 и 2 от ПЗД.

([207]) Член 32, параграфи 1 и 2 от ПЗД. Съгласно член 4, параграф 1 от ПЗД администраторът трябва да следва „структуриран и основан на риска подход към разработването и документирането на операциите по обработване“. Администраторът трябва също така да е в състояние да докаже на субектите на данни по всяко време, че при извършването на операциите по обработване се спазват документираните ангажименти и условия.

([208]) Член 32, параграфи 4, 5 и 6 от ПЗД.

([209]) Член 45 от ПЗД.

([210]) Член 26, параграф 3 от ПЗД.

([211]) Администраторът трябва да се консултира с ДЛЗД относно необходимостта от извършване на оценка на въздействието, което на свой ред може да се консултира с Комитета по защита на данните в случай на съмнение. Вж. член 38, параграфи 1 и 2 от ПЗД.

([212]) Член 38, параграф 4 от ПЗД.

([213]) Член 38, параграф 6 от ПЗД.

([214]) Член 38, параграфи 7 и 8 и член 39 от ПЗД.

([215]) Член 40, параграф 2 от ПЗД.

([216]) Член 32А, параграфи 1 и 2 от Служебния правилник, в които се предвижда, че ролята на ДЛЗД е да наблюдава прилагането на разпоредбите относно защитата на личните данни, да съветва различните оперативни звена на ЕПО относно изпълнението на техните задължения и да им предоставя оперативна документация, необходима за практическото изпълнение на изискванията за защита на данните. От Комитета по защита на данните се изисква да гарантира „независим, ефективен и безпристрастен надзор на разпоредбите, приложими за защитата на личните данни“. Може да съществува различен независим надзорен механизъм за надзор на спазването на изискванията от страна на апелативните състави при обработването на лични данни в качеството им на съдебни органи (вж. също член 2, параграф 6 от ПЗД).

2.5.1. ***Независимост***

(80) Съгласно Служебния правилник ДЛЗД и Комитетът по защита на данните действат напълно независимо от всякаква вътрешна или външна намеса при изпълнението на своите задачи и упражняването на правомощията си ([217]). Този принцип се допълва от различни допълнителни гаранции, които осигуряват тяхната независимост.

(81) ДЛЗД (и неговите заместници) се назначават от председателя на Ведомството въз основа на професионалните им квалификации, и по-специално на експертните им познания в областта на правото и практиките за защита на данните ([218]). ДЛЗД се назначава за срок от три до пет години, който може да бъде подновен. Комитетът по защита на данните бива консултиран преди всяко предложение за отстраняване или освобождаване от длъжност на ДЛЗД ([219]). Целта на тази предварителна консултация преди отстраняване или освобождаване от длъжност на ДЛЗД е да се осигури допълнителен контрол и преразглеждане в случай на предложение за отстраняване или освобождаване от длъжност. Подобно отстраняване или освобождаване от длъжност може да бъде предложено по една от следните причини ([220]): когато ДЛЗД вече не отговаря на условията, необходими за изпълнението на задълженията ([221]); при професионална некомпетентност ([222]); или в резултат на дисциплинарни мерки ([223]). В ПЗД също така се установява, че ДЛЗД не може да бъде освободено от длъжност или санкционирано за изпълнението на своите задачи и не може да получава никакви инструкции ([224]). ДЛЗД трябва да участва във всички въпроси, свързани със защитата на личните данни, и изготвя годишни отчети за дейността на вниманието на председателя на Ведомството и Административния съвет ([225]). Ведомството трябва да осигурява на ДЛЗД необходимите ресурси за изпълнение на неговите задачи ([226]).

(82) Комитетът по защита на данните се състои от трима външни експерти в областта на защитата на данните, а именно председател и двама други членове ([227]), както и един заместник-член, назначени от председателя на ЕПО за срок от три години, който може да бъде подновяван ([228]). Членовете на Комитета по защита на данните трябва да притежават квалификациите, необходими за заемане на съдебна длъжност, или да бъдат специалисти по защита на данните с доказани експертни познания и опит в областта на правото за защита на данните, придобити на национално или международно равнище. Те не могат да бъдат служители на ЕПО или да са били наети от нея през последните десет години ([229]). Съгласно член 48, параграф 6 от ПЗД членовете на Комитета по защита на данните са напълно независими при изпълнението на своите функции. По-конкретно членовете на Комитета не могат да търсят инструкции от Ведомството или от Административния съвет и не могат да бъдат обвързани от подобни инструкции. В Процедурния правилник на Комитета се предвижда също, че той трябва да действа безпристрастно и напълно независимо при изпълнението на своите задачи ([230]). Освен това членовете на Комитета могат да бъдат освобождавани

([217]) Член 32A, параграфи 4 и 5 от Служебния правилник.

([218]) Член 41 от ПЗД.

([219]) Член 42, параграф 8 от ПЗД. Тази консултация се провежда независимо от основанието или причината за дадено предложение за отстраняване или освобождаване от длъжност.

([220]) Член 50 от Служебния правилник.

([221]) Вж. член 53, параграф 1 от Служебния правилник, който гласи, че „органът по назначаването може да реши да прекрати служебното правоотношение на служител: а) ако договарящата държава, чийто гражданин е служителят, престане да бъде страна по конвенцията; б) ако служителят откаже да бъде прехвърлен в държава, различна от тази, в която работи; в) ако в случай на служител, назначен от Административния съвет в съответствие с член 11, параграфи 1 и 2 от Конвенцията, Административният съвет вземе такова решение в интерес на Организацията; г) който е работил непрекъснато в продължение на една година или по-малко на срочен трудов договор; д) ако в резултат на своите действия, той престане да отговаря на условията, предвидени в член 8, буква а) или б) [т.е. да е гражданин на една от договарящите държави от ЕПО, освен ако е разрешено изключение от органа по назначаването, и да се ползва с пълни граждански права]; или е) в другите случаи, изрично предвидени в настоящия Служебен правилник“.
Вж. също член 13, параграф 4, буква б) от Служебния правилник, където се посочва, че „Докладът за длъжностното лице в изпитателен срок може да бъде изготвен по всяко време в рамките на този срок, ако изпълнението на неговите задължения, ефикасността и поведението му се окажат незадоволителни. Въз основа на доклада или докладите за изпитателния срок органът по назначаването може да:
— уволни новоназначено лице в изпитателен срок,
— реши да върне преместеното, повишено или преназначено длъжностно лице в изпитателен срок на предишната му длъжност, или, ако тя е вече заета, на длъжност, съответстваща на степента на предишната му длъжност, за която то отговаря на изискванията“.

([222]) В член 52 от Служебния правилник се предвиждат критериите и процедурите, които трябва да се следват в случай на установена „професионална некомпетентност“.

([223]) Член 94 от Служебния правилник.

([224]) Член 42, параграф 3 от ПЗД. Въпреки че ДЛЗД може да изпълнява и други задачи, тези задачи не може да водят до конфликт на интереси (член 42, параграф 6 от ПЗД).

([225]) Член 42, параграфи 1 и 3 от ПЗД.

([226]) Член 42, параграф 2 от ПЗД.

([227]) Член 48, параграф 1 от ПЗД.

([228]) Член 48, параграфи 1 и 3 от ПЗД.

([229]) Член 48, параграф 2 от ПЗД.

([230]) Член 1, параграф 1 от Процедурния правилник на Комитета по защита на данните, CA/26/21 Add. 1, приет на 11 юни 2021 г. На разположение на адрес: https://link.epo.org/web/data_protection_board-rules_of_procedure_en.pdf.

от длъжност от ЕПО само по сериозна причина ([231]). Членовете на Комитета по защита на данните са обвързани със задължение за поверителност ([232]) и трябва да се въздържат от действия в случаи, в които е налице конфликт на интереси и по-специално на техен личен интерес ([233]). От ЕПО се изисква да подпомага Комитета за защита на данните при изпълнението на неговите задачи, като му осигурява необходимите ресурси, както и правна и административна подкрепа (чрез секретариат и като му предоставя достъп до лични данни и операции по обработване) ([234]).

2.5.2. ***Задачи и правомощия***

(83) Задачите на ДЛЗД включват следното: информиране и съответно съветване на администратора или обработващите лични данни за техните задължения; повишаване на осведомеността и предоставяне на обучение на персонала, участващ в операциите по обработване; гарантиране, че субектите на данните са информирани за техните права съгласно ПЗД; и независимо наблюдение на вътрешното прилагане и спазването на ПЗД, както и на други правни разпоредби на ЕПО, които имат последици за защитата на данните ([235]). Субектите на данни могат да се свързват с ДЛЗД по всеки въпрос, свързан с обработването на техните данни или упражняването на техните права ([236]), а администраторът и обработващите лични данни могат да се консултират с ДЛЗД по всеки въпрос, свързан с тълкуването и прилагането на ПЗД ([237]).

(84) Като част от надзорната си роля ДЛЗД има правомощието да извършва одити и разследвания във връзка със защитата на данните ([238]). Одитите са по инициатива на ДЛЗД съгласно годишен одитен план, който се изготвя след консултация с Комитета по защита на данните ([239]). Одитът е съсредоточен върху оценката на записите, декларациите и съответната документация за защита на данните, например за да се провери точността и пълнотата на съответната документация за защита на данните, правилното прилагане на методиките за управление на риска, точността и навременността на отговорите до субектите на данни или правилното провеждане и броя на оценките на въздействието върху защитата на данните ([240]). Според информацията, получена от Комисията от ДЛЗД, през 2023 г. са проведени три одита, а през 2024 г. — четири. ДЛЗД може да започне разследване по собствена инициатива, въз основа на искане, получено от Комитета по защита на данните или от орган в рамките на ЕПО (например председателя на Ведомството или администратор с делегирани правомощия), или въз основа на информация, получена по друг начин (включително например от трети страни и физически лица) ([241]). Разследванията, поискани от Комитета по защитата на данните, се провеждат от ДЛЗД по независим начин. Комитетът по защита на данните може да коментира и/или да поиска допълнително разследване по всеки потенциално възникнал въпрос ([242]). Проверките са съсредоточени върху операциите по обработване или конкретни аспекти от тях, или събития, свързани с тях, с цел да се гарантира, че въпросното обработване отговаря на изискванията на ПЗД и да се гарантира защитата на правата и свободите на субектите на данни ([243]).

(85) ДЛЗД има достъп до цялата съответна информация, включително обработваните лични данни, както и до всички офиси, инсталации за обработка на данни и носители на данни ([244]). От всички служители и оперативни звена на ЕПО се изисква да подпомагат ДЛЗД при изпълнението на неговите задължения, включително чрез предоставяне на достъп до помещения и съответната информация ([245]).

([231]) По-специално в споразумението за предоставяне на услуги между ЕПО и Комитета се предвижда, че то „може да бъде прекратено, без да се засяга правото на прекратяване по сериозна причина, [само] от [члена на Комитета по защита на данните] с писмено предизвестие от шест (6) месеца“. Тъй като споразумението за услуги се урежда от германското право, понятието за сериозна причина трябва да се тълкува в съответствие с член 626 от германския Граждански кодекс. Съгласно съдебната практика това условие може да бъде изпълнено например в случай на повтарящо се и продължаващо нарушение на приложимите задължения (например по отношение на конфликтите на интереси) или при лишаване от свобода.

([232]) Член 48, параграф 5 от ПЗД.

([233]) Член 48, параграф 7 от ПЗД.

([234]) Член 48, параграф 10 от ПЗД. Секретариатът изпълнява задачите си независимо от всякаква неправомерна намеса и изключително под инструкциите на председателя на Комитета по защита на данните. Той предоставя правна, административна и логистична подкрепа на Комитета. Вж. член 2 от Процедурния правилник на Комитета по защита на данните.

([235]) Член 43, параграф 1 от ПЗД.

([236]) Член 43, параграф 1, буква к) от ПЗД.

([237]) Член 42, параграфи 4 и 7 от ПЗД.

([238]) Член 43, параграф 1, буква г) от ПЗД. Вж. също Бележката относно надзора над защитата на данните „How the Data Protection Office Conducts DP Audits and DP Inspections“ („Как Службата за защита на данните извършва одити и проверки в областта на защитата на данните“), достъпна на адрес https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

([239]) Комитетът по защита на данните може да формулира предложения относно областите, в които следва да се извършват одити, вж. Бележката относно надзора над защитата на данните, стр. 4.

([240]) Бележка относно надзора над защитата на данните, стр. 4.

([241]) Бележка относно надзора над защитата на данните, стр. 7.

([242]) Бележка относно надзора над защитата на данните, стр. 6.

([243]) Бележка относно надзора над защитата на данните, стр. 6.

([244]) Член 43, параграф 5 от ПЗД.

([245]) Член 46 от ПЗД.

(86) След като приключи одит или разследване, ДЛЗД приема доклад, в който излага своите констатации, заключения и препоръчителни корективни мерки ([246]). Подобни мерки могат например да включват превантивни или смекчаващи мерки за подобряване на спазването, както и мерки за отстраняване на неспазването (например за привеждане на обработването в съответствие с ПЗД, за обработване на искания от субекти на данни за упражняване на техните права, за спиране или прекратяване на обработване и др.) ([247]). ДЛЗД може също така да насочи вниманието на компетентния орган по назначаването към неспазването на ПЗД от страна на служители и да препоръча започване на административно разследване, за да се определи дали са необходими дисциплинарни или други действия ([248]). Всеки служител, който не спазва ПЗД, независимо дали умишлено или поради небрежност, може да подлежи на дисциплинарни санкции или други действия съгласно Служебния правилник ([249]).

(87) Резултатите от одитите и разследванията трябва да бъдат съобщени на Комитета по защита на данните ([250]). Докладът от даден одит или разследване трябва да бъде споделен с Комитета по защита на данните при поискване. Комитетът има право да коментира доклада на ДЛЗД, включително констатациите на ДЛЗД относно това дали е извършено нарушение на ПЗД и относно предложените корективни мерки, и може да иска допълнителни мерки за разследване ([251]). Ако при одит или проверка от ДЛЗД се стигне до заключението, че е налице неспазване (т.е. нарушение на ПЗД), докладът на ДЛЗД трябва да бъде представен на Комитета по защита на данните за валидиране на заключенията и препоръчаните корективни мерки. В случай че Комитетът по защита на данните не е съгласен със заключенията или препоръчаните от ДЛЗД корективни мерки, Комитетът споделя своите коментари с ДЛЗД, включително с цел изменение на предложените заключения и препоръчаните корективни мерки, като ДЛЗД следва да ги приложи по съответния начин. Корективните мерки, валидирани от Комитета по защита на данните, са обвързващи за администратора и администраторите с делегирани правомощия и физическите лица могат да се позовават на тях пред механизмите за правна защита, описани в съображение 95 ([252]). ДЛЗД трябва да провери дали корективните мерки са били изпълнени (по принцип шест месеца след съобщаването им) и да докладва ежегодно на председателя на Ведомството за степента им на изпълнение ([253]).

(88) Освен осигуряването на спазване на ПЗД, задачите на Комитета по защита на данните включват съветване на председателя на Ведомството във връзка с приемането на решения относно адекватното ниво на защита, съветване на администратора относно необходимостта от извършване на оценка на въздействието върху защитата на данните и разглеждане на жалби от физически лица (вж. съображения 92—96) ([254]).

2.6. **Правна защита**

(89) С цел да се осигури адекватна защита, и по-специално упражняване на индивидуалните права, на субекта на данни следва да се предоставят ефективни средства за правна защита, включително обезщетение за вреди.

(90) Правната рамка на ЕПО предлага правна защита на физическите лица чрез комбинация от възможни действия.

(91) Първо, субектите на данни, които считат, че обработването на личните им данни от ЕПО нарушава техните права (т.е. нарушава ПЗД), могат да подадат искане за преразглеждане от администратора с делегирани правомощия в съответствие с член 49 от ПЗД. Администраторът с делегирани правомощия ще разгледа жалбата и ще вземе решение ([255]). Преди да вземе решение, администраторът с делегирани правомощия трябва да се консултира с ДЛЗД, което предоставя писмено становище не по-късно от петнадесет календарни дни след получаване на искането за преразглеждане ([256]). Администраторът с делегирани правомощия трябва да отговори на лицето в срок от един месец

([246]) Бележка относно надзора над защитата на данните.
([247]) Бележка относно надзора над защитата на данните, стр. 2 (определение за „препоръки“).
([248]) Член 43, параграф 6 от ПЗД.
([249]) Член 54 от ПЗД. Дисциплинарните санкции се налагат от председателя на Ведомството, който разполага с дисциплинарни правомощия по отношение на персонала на ЕПО, вж. член 10 от ЕПК и член 93 и сл. от Служебния правилник.
([250]) Бележка относно надзора над защитата на данните, стр.7.
([251]) Бележка относно надзора над защитата на данните, стр. 3—4 и стр. 8.
([252]) Решение на председателя на Европейското патентно ведомство от 12.7.2024 г. относно приложимостта на препоръките на ДЛЗД, одобрени от Комитета по защита на данните, в рамките на одити и проверки за защита на данните, https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf.
([253]) Бележка относно надзора над защитата на данните, стр. 5 и стр. 9.
([254]) Член 47 от ПЗД.
([255]) Член 49, параграф 1 от ПЗД. Искането трябва да бъде подадено не по-късно от три месеца от деня, в който субектът на данните е бил уведомен или по друг начин е узнал за обработването на лични данни, за което се твърди, че нарушава неговите права.
([256]) Член 49, параграф 2 от ПЗД. Ако ДЛЗД не представи становище до края на този срок, становището вече не е необходимо.

от датата на получаване на искането ([257]). Решението трябва да бъде съобщено на физическото лице заедно с информация относно възможността за получаване на по-нататъшна правна защита ([258]). Ако администраторът с делегирани правомощия не предприеме никакви действия в срок от три месеца, това се счита за мълчаливо отхвърляне на искането.

(92) Второ, физическите лица могат да обжалват решение или мълчаливо отхвърляне на искане за преразглеждане от администратор с делегирани правомощия, като подадат жалба до Комитета по защита на данните ([259]).

(93) При разглеждането на жалба Комитетът по защита на данните трябва да прикани субекта на данните, администратора и, когато е приложимо, обработващия лични данни, да изложат писмено позицията си по съответните твърдения и факти и да представят доказателства или коментари и аргументи относно наличните доказателства ([260]). В този контекст Комитетът по защита на данните може да поиска от страните всякаква информация, от която се нуждае, за да разгледа жалбата, и освен това може да получи допълнителна информация чрез ДЛЗД ([261]). Когато взема решение относно необходимите последващи действия във връзка с дадена жалба, Комитетът по защита на данните трябва да вземе предвид, наред с другото, естеството и тежестта на предполагаемото нарушение, броя на засегнатите субекти на данни, категориите засегнати данни и продължителността на нарушението ([262]). Комитетът по защита на данните може да прикани страните да потърсят уреждане на спора по взаимно съгласие и насърчава и активно улеснява този вид уреждане на спора ([263]). Жалбоподателят може също така да поиска от Комитета по защита на данните да приложи процедура по спешност поради тежестта на предполагаемото нарушение или поради тежестта на риска, на който са изложени правата на физическите лица ([264]).

(94) След като разгледа жалбата, Комитетът по защита на данните издава мотивирано становище до администратора, което включва изложение на фактите, основните аргументи на страните, съображенията на Комитета и неговите препоръки ([265]). В случай на процедура по спешност Комитетът по защита на данните трябва да издаде официално мотивирано становище в срок от два месеца от подаването на жалбата ([266]). В мотивираното си становище Комитетът може да отправи всички препоръки, които счита за необходими, включително съдебно предписание (например прекратяване на незаконосъобразно обработване на данни, заличаване на незаконно обработени данни), обезщетение за материални или нематериални вреди ([267]). Мотивираното становище трябва да бъде съобщено на субекта на данните и на администратора (т.е. председателя на Службата, председателя на апелативните състави, председателя на Административния съвет или председателя на специалния комитет в зависимост от това дали жалбата се отнася до Службата, апелативните състави, Административния съвет или специалния комитет). Администраторът ще вземе окончателно решение със задължителен характер след мотивираното становище на Комитета за защита на данните ([268]). Окончателното решение се съобщава на субекта на данните, на Комитета за защита на данните и на ДЛЗД ([269]). Ако администраторът реши да не се съобрази с един или повече аспекти на мотивираното становище, той обяснява това писмено в решението ([270]).

(95) Субект на данни, който не е удовлетворен от решението на администратора, може да го обжалва на по-горна инстанция и да се позове на мотивираното становище на Комитета по защита на данните в жалбата си. Служителите на ЕПО могат да обжалват решението пред Административния съд на Международната организация на труда ([271]). Всеки друг субект на данни, който не е съгласен с решението на администратора, може в срок от три месеца от получаването на решението да подаде искане до председателя на Ведомството за *ad hoc* арбитраж ([272]). В ПЗД се

([257]) Член 49, параграф 3 от ПЗД. При необходимост този срок може да бъде удължен с още два месеца, като се вземат предвид сложността и броят на исканията. В случай на удължаване администраторът с делегирани правомощия трябва да уведоми субекта на данните за това и за причините за забавянето в срок от един месец от получаването на искането за преразглеждане.

([258]) Член 49, параграф 3 от ПЗД.

([259]) Член 50, параграф 1 от ПЗД. Жалбата до Комитета по защита на данните трябва да бъде подадена в срок от три месеца от получаването на решението или, в случай на мълчаливо отхвърляне, от датата на изтичане на срока за отговор на искането.

([260]) Член 50, параграф 2 от ПЗД.

([261]) По-специално ДЛЗД е длъжно да отговаря на исканията от Комитета по защита на данните и да си сътрудничи с него (член 43, буква и) от ПЗД). От ДЛЗД се изисква също така да улеснява сътрудничеството между Комитета по защита на данните и Ведомството и в този контекст има достъп до всяка имаща отношение информация (член 43, буква й), член 46, букви а) и б) от ПЗД).

([262]) Член 4, параграф 5 от Процедурния правилник на Комитета по защита на данните.

([263]) Член 8 от Процедурния правилник на Комитета по защита на данните.

([264]) Член 11, параграф 1 от Процедурния правилник на Комитета по защита на данните.

([265]) Член 10, параграф 2 от Процедурния правилник на Комитета по защита на данните.

([266]) Член 11, параграф 2 от Процедурния правилник на Комитета по защита на данните.

([267]) Член 50, параграф 3 от ПЗД.

([268]) Член 50, параграф 4 от ПЗД и член 10, параграф 6 от Процедурния правилник на Комитета по защита на данните.

([269]) Член 50, параграф 6 от ПЗД.

([270]) Член 50, параграф 4 от ПЗД. Ако препоръките на Комитета по защита на данните не са пряко относими към субектите на данни, администраторът излага писмено всички евентуални отклонения в документ, който се представя на посочения комитет.

([271]) Член 50, параграф 7 от ПЗД. Вж. член 13 от ЕПК и член 113 от Служебния правилник.

([272]) Член 50, параграф 8 и член 52, параграф 2 от ПЗД. Съгласно ПЗД на Административния съвет и ПЗД на специалния комитет арбитраж може да бъде поискан от председателя на Административния съвет.

предвижда специална процедура, която да се следва в случай на *ad hoc* арбитраж ([273]). По-конкретно, в срок от три месеца от получаването на искането от субекта на данните генералният секретар на Постоянния арбитражен съд трябва да назначи един арбитър въз основа на критериите, определени в ПЗД ([274]). Арбитърът трябва да има юридическа квалификация, да бъде допуснат да практикува право в една от договарящите държави от ЕПО, да е в състояние да демонстрира съответен експертен опит по въпросите на защитата на данните и да е запознат с правото, уреждащо международните организации ([275]). Могат да бъдат назначавани само физически лица, които, освен че отговарят на тези критерии, не са работили нито за ЕПО, нито за субекта на данните. В ПЗД се предвижда, че арбитърът трябва да действа независимо и безпристрастно ([276]), да третира всяка от страните еднакво и да им дава възможност да представят своята позиция на всеки етап от производството ([277]). Арбитражните производства не са публични ([278]) и се уреждат от ЕПК, ПЗД, включително законодателството за прилагането им, правото на международните организации и принципите на международното публично право ([279]). Въпреки че всяка страна трябва да поеме собствените си разходи и разноски за процесуално представителство (освен ако арбитърът не реши друго), хонорарите и разноските на арбитъра, разходите за евентуални експертни съвети и свидетели се заплащат от ЕПО ([280]). Споразумението трябва да бъде сключено под формата на писмено арбитражно решение с договорена формулировка, която е окончателна и обвързваща ([281]).

(96) Всяко физическо лице, което е претърпяло вреди в резултат на нарушение на ПЗД, може да поиска обезщетение от ЕПО, като използва процедурите, описани в съображения 91—95 ([282]). ЕПО не носи отговорност, ако докаже, че не е отговорна за събитието, причинило вредата.

3. ДОСТЪП И ИЗПОЛЗВАНЕ НА ЛИЧНИ ДАННИ, ПРЕДАДЕНИ ОТ СЪЮЗА НА ЕВРОПЕЙСКОТО ПАТЕНТНО ВЕДОМСТВО, ОТ ПУБЛИЧНИ ОРГАНИ

(97) Правната рамка, съгласно която ЕПО оценява и отговаря на искания от публични органи — в своите договарящи държави и в трети държави — относно личните данни, обработвани от ЕПО, произтича от Протокола на ЕПО за привилегиите и имунитетите ([283]), изискванията на ПЗД относно изпращането и предаването на лични данни и международното публично право.

(98) Първо, обработването на лични данни от ЕПО за целите на официалните ѝ дейности е обхванато от имунитетите на Организацията. Имунитетите на ЕПО се допълват от задължение за сътрудничество, посочено в член 20 от Протокола за привилегиите и имунитетите. Като резултат от това, всяко искане от публичен орган от договаряща държава за получаване на данни, обработвани от ЕПО, се оценява от председателя на Ведомството съгласно член 20, параграф 1 от Протокола за привилегиите и имунитетите, в който се предвижда, че Организацията си сътрудничи по всяко време с компетентните органи от договарящите държави, за да улесни доброто правораздаване, да гарантира съблюдаването на полицейските разпоредби и разпоредбите за общественото здраве, трудовите инспекции или друго подобно национално законодателство и за да предотврати злоупотреби с привилегиите, имунитетите и улесненията, предвидени в Протокола. По изключение Организацията може да се откаже от съдебния си имунитет и имунитета си срещу принудително изпълнение ([284]) Когато взема решение по искане за сътрудничество, председателят упражнява право на преценка, като взема предвид съответствието на искането с правната рамка на Организацията ([285]). Заключението може да бъде, че Ведомството може да отговори на искане по Протокола за привилегиите и имунитетите и може да разкрива лични данни само в съответствие с изискванията за изпращане на данни, предвидени в ПЗД (вж. съображения 62—67). Съгласно ПЗД получателят трябва да представи доказателства, че е необходимо данните да бъдат изпратени за конкретна цел, произтичаща от задълженията на ЕПО за сътрудничество с

([273]) Член 52, параграф 1 от ПЗД.
([274]) Член 52, параграф 4 от ПЗД.
([275]) Член 52, параграф 4 от ПЗД.
([276]) Член 52, параграф 4 от ПЗД.
([277]) Член 52, параграф 8 от ПЗД.
([278]) Член 52, параграф 9 от ПЗД.
([279]) Член 52, параграф 6 от ПЗД. Мястото на арбитраж е Хага (член 52, параграф 5 от ПЗД), а езикът, използван по време на производството, трябва да бъде избран от арбитъра, който обаче трябва да бъде един от официалните езици на ЕПО (английски, френски или немски) (член 52, параграф 7 от ПЗД).
([280]) Член 52, параграф 13 от ПЗД.
([281]) Член 52, параграф 10 от ПЗД. Вж. също член 3 и член 34, параграф 2 от Правилника на Постоянния арбитражен съд.
([282]) Член 53 от ПЗД. При определени условия (по-специално приложимите изисквания съгласно германското право) физическите лица могат също така да получат обезщетение за вреди, причинени от служители на ЕПО при изпълнението на техните задължения, съгласно член 9, параграф 2 от ЕПК.
([283]) Протокол за привилегиите и имунитетите на ЕПО. Достъпен на адрес: https://www.epo.org/en/legal/epc/2020/proprim.html.
([284]) Член 3, параграф 1, буква а) от Протокола за привилегиите и имунитетите.
([285]) Това включва възможността за отхвърляне на искане.

договарящата държава или държави ([286]). За всяко изпращане администраторът трябва да е в състояние да демонстрира, че то е необходимо и пропорционално по отношение на конкретната цел, за която се извършва ([287]). Всяко предаване на данни трябва да се извършва по начин, който гарантира, че нивото на защита, осигурявано от ПЗД, остава непроменено ([288]). Съгласно насоките, издадени от ДЛЗД, това означава, че са налице подходящи гаранции, включително гаранция, че споделяните данни трябва да бъдат сведени до минимум и ограничени до това, което е адекватно, от значение и строго необходимо за постигането на тази цел ([289]). Ако има причина да се предполага, че правата и свободите на съответното лице може да бъдат засегнати, администраторът трябва да установи, че изпращането на личните данни за тази конкретна цел е пропорционално, след като претегли различните интереси в случая ([290]).

(99) Второ, не съществува правен инструмент, приложим към ЕПО, който да урежда конкретно обработването на искания от публични органи на трети държави (т.е. които не са договарящи държави от ЕПО) за получаване на данни, обработвани от ЕПО. В резултат от това всяко оповестяване в отговор на такова искане може да се извърши само ако са изпълнени изискванията за международно предаване на данни съгласно ПЗД (както е описано в съображения 68—73). Случаят е такъв само ако за съответната държава е прието решение относно адекватното ниво на защита, което обхваща предаването, ако са налице подходящи гаранции или ако се прилага дерогация.

(100) Спазването на Протокола за привилегиите и имунитетите от страна на председателя на Ведомството, включително начинът, по който се обработват исканията за сътрудничество от страна на публични органи, подлежи на надзор от страна на Административния съвет, докато спазването на изискванията за изпращане и предаване на лични данни в ПЗД подлежи на надзор от страна на ДЛЗД и Комитета за защита на данните, както е описано в съображения 84—88. Физическите лица могат да използват средствата за правна защита, описани в съображения 90—96, по отношение на изпращането или предаването на техни лични данни в нарушение на ПЗД.

4. ЗАКЛЮЧЕНИЯ

(101) Комисията счита, че ЕПО осигурява ниво на защита на личните данни, предавани от Съюза, което по същество е равностойно на гарантираното от Регламент (ЕС) 2016/679.

(102) Въз основа на констатациите в настоящото решение следва да се вземе решение, че ЕПО осигурява адекватно ниво на защита по смисъла на член 45 от Регламент (ЕС) 2016/679, тълкуван в светлината на Хартата на основните права на Европейския съюз, за личните данни, предавани от Съюза на ЕПО.

5. ПОСЛЕДИЦИ ОТ НАСТОЯЩОТО РЕШЕНИЕ И ДЕЙСТВИЯ НА ОРГАНИТЕ ЗА ЗАЩИТА НА ДАННИТЕ

(103) Държавите членки и техните органи са задължени да предприемат необходимите мерки за спазване на актовете на институциите на Съюза, тъй като тези актове по презумпция са законосъобразни и съответно произвеждат правно действие, докато не бъдат оттеглени, отменени вследствие на жалба за отмяна или обявени за невалидни вследствие на производство по постановяване на преюдициално запитване или възражение за незаконосъобразност.

(104) Следователно решение на Комисията относно адекватното ниво на защита, прието съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679, е обвързващо за всички органи на държавите членки, адресати на решението, включително за независимите им надзорни органи. По-специално предаването на данни от администратор или обработващ лични данни в Съюза на ЕПО може да се извършва, без да е необходимо да се получава допълнително разрешение.

([286]) Член 8, параграф 3 от ПЗД.

([287]) Член 8, параграф 4 от ПЗД.

([288]) Обяснителна бележка „Изпращане и предаване на лични данни от ЕПО“ (Бележка за изпращането и предаването), на разположение на адрес https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, стр. 4. Вж. по-специално „В ПЗД на Европейското патентно ведомство [...] се определя общият принцип на адекватна защита, особено приложим към международния поток от данни“.

([289]) Бележка за изпращането и предаването, бележка под линия 12.

([290]) Член 8, параграф 3 от ПЗД.

(105) Следва да се припомни, че съгласно член 58, параграф 5 от Регламент (ЕС) 2016/679 и както е обяснено от Съда на ЕС в решението по дело C-362/14 ([291]), когато национален орган за защита на данните поставя под въпрос, включително въз основа на получена жалба, съгласуваността на дадено решение на Комисията относно адекватното ниво на защита с основните права на неприкосновеност на личния живот и на защита на данните на физическото лице, националното законодателство трябва да предвижда правни способи, позволяващи на съответния орган да представи възраженията си пред национална юрисдикция, която може да бъде длъжна да отправи преюдициално запитване до Съда на ЕС.

6. НАБЛЮДЕНИЕ, СПИРАНЕ НА ДЕЙСТВИЕТО, ОТМЯНА ИЛИ ИЗМЕНЕНИЕ НА НАСТОЯЩОТО РЕШЕНИЕ

(106) Съгласно практиката на Съда на ЕС и член 45, параграф 4 от Регламент (ЕС) 2016/679, след като приеме решение относно адекватното ниво на защита Комисията следва непрекъснато да наблюдава релевантните промени в третата държава или международната организация, за да прецени дали те продължават да гарантират ниво на защита, което по същество е равностойно на нивото в Европейския съюз. Такава проверка е наложителна във всички случаи, когато Комисията получи информация, която поражда основателни съмнения в това отношение.

(107) Поради това Комисията следва непрекъснато да наблюдава положението по отношение на правната уредба на ЕПО и действителните практики за обработване на лични данни, както са оценени в настоящото решение. За да се улесни този процес, ЕПО се приканва да информира Комисията своевременно за съществени промени, имащи отношение към настоящото решение и свързани с обработването на лични данни и ограниченията и гаранциите, приложими към достъпа до лични данни от страна на публичните органи.

(108) На следващо място, за да се даде възможност на Комисията да изпълнява ефективно функцията си по извършване на наблюдение, държавите членки следва да я информират за всички релевантни действия, предприети от националните органи по защита на данните, по-специално във връзка със запитвания или жалби на субекти на данни от Съюза във връзка с предаване на лични данни от Съюза на ЕПО.

(109) В приложение на член 45, параграф 3 от Регламент (ЕС) 2016/679 и с оглед на факта, че нивото на защита, осигурявано от правната рамка на ЕПО, може да се промени, след приемането на настоящото решение Комисията следва периодично да проверява дали констатациите във връзка с адекватното ниво на защита, гарантирано от ЕПО, са все още фактически и правно обосновани. Подобни оценки следва да се извършват най-малко на всеки четири години и следва да обхващат всички аспекти на функционирането на настоящото решение, включително функционирането на съответните механизми за надзор и правоприлагане.

(110) За да извърши прегледа, Комисията следва да се срещне с ЕПО, включително с нейното ДЛЗД и нейния Комитет по защита на данните. В тази среща следва да могат да участват представители на членовете на Европейския комитет по защита на данните. В рамките на прегледа Комисията следва да поиска от ЕПО да предостави изчерпателна информация по всички аспекти, които са от значение за установяването на адекватно ниво на защита. Комисията следва също така да потърси обяснения във връзка с всяка получена от нея информация, която е от значение за настоящото решение, включително от Европейския комитет по защита на данните, отделни органи за защита на данните, групи на гражданското общество, публични или медийни доклади или всякакви други налични източници на информация.

(111) Въз основа на съвместния преглед Комисията следва да изготви публичен доклад, който се представя на Европейския парламент и на Съвета.

(112) Когато наличната информация, по-специално информацията, получена в резултат от наблюдението от страна на Комисията на промените, които биха могли да засегнат функционирането на настоящото решение съгласно член 45, параграф 4 от Регламент (ЕС) 2016/679, или предоставена от ЕПО или органите на държавите членки, показва, че нивото на защита, осигурявано от ЕПО, може вече да не е адекватно, Комисията следва да информира ЕПО за това и да поиска предприемането на подходящи мерки в рамките на определен разумен срок.

(113) Ако при изтичането на посочения срок ЕПО не предприеме тези мерки или не докаже по друг задоволителен начин, че настоящото решение продължава да се основава на адекватно ниво на защита, Комисията ще започне процедурата, посочена в член 93, параграф 2 от Регламент (ЕС) 2016/679, с оглед частично или пълно спиране или отмяна на настоящото решение.

([291]) Решение по дело C-362/14, *Schrems* (*Schrems I*), ECLI:EU:C:2015:650, т. 65.

(114) Като алтернативна възможност Комисията ще започне тази процедура с оглед изменение на решението, по-специално като обвърже предаването на данни с допълнителни условия или като ограничи обхвата на констатацията за адекватност само до предаването на данни, за което продължава да се осигурява адекватно ниво на защита.

(115) Комисията следва също така да разгледа необходимостта от започване на процедурата, водеща до изменение, спиране на прилагането или отмяна на настоящото решение, ако при прегледа или по друг повод ЕПО не предостави информацията или поясненията, необходими за оценката на нивото на защита на личните данни, предавани от Съюза, или за спазването на настоящото решение. Във връзка с това Комисията следва да взема предвид степента, в която съответната информация може да бъде набавена от други източници.

(116) При надлежно обосновани наложителни причини за спешност Комисията ще използва възможността да приеме, в съответствие с процедурата, посочена в член 93, параграф 3 от Регламент (ЕС) 2016/679, актове за изпълнение с незабавно приложение за спиране на прилагането, отмяна или изменение на решението.

7. ЗАКЛЮЧИТЕЛНИ СЪОБРАЖЕНИЯ

(117) Европейският комитет по защита на данните публикува становището си ([292]), като то бе взето предвид при изготвянето на настоящото решение.

(118) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден по силата на член 93, параграф 1 от Регламент (ЕС) 2016/679,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

За целите на член 45 от Регламент (ЕС) 2016/679 Европейската патентна организация осигурява адекватно ниво на защита на личните данни, предавани от Съюза на Европейската патентна организация.

Член 2

Когато компетентните органи в държавите членки упражнят, с цел защита на физическите лица във връзка с обработване на техни лични данни, правомощията си по член 58 от Регламент (ЕС) 2016/679 по отношение на предаване на данни, попадащо в приложното поле, посочено в член 1, съответната държава членка уведомява Комисията за това незабавно.

Член 3

1. Комисията непрекъснато наблюдава прилагането на правната рамка на Европейската патентна организация, на която се основава настоящото решение, за да прецени дали Европейската патентна организация продължава да осигурява адекватно равнище на защита по смисъла на член 1.

2. Държавите членки и Комисията се информират взаимно за случаите, в които Европейската патентна организация не е гарантирала спазването на правната рамка, на която се основава настоящото решение.

3. Най-малко на всеки четири години Комисията оценява констатацията, посочена в член 1, въз основа на цялата налична информация, включително информацията, получена като част от преглед, извършен съвместно с Европейската патентна организация.

([292]) Европейски комитет по защита на данните, Становище 07/2025 относно проекта на решение за изпълнение на Европейската комисия съгласно Регламент (ЕС) 2016/679 относно адекватната защита на личните данни от страна на Европейската патентна организация. На разположение на адрес: https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202507-epo-adequacydecision_en.pdf.

4. Ако Комисията открие признаци, че вече не се осигурява адекватно ниво на защита, тя информира Европейската патентна организация за това. Ако е необходимо, Комисията може да реши да спре прилагането на настоящото решение, да го измени или да го отмени, или да ограничи приложното му поле в съответствие с член 45, параграф 5 от Регламент (ЕС) 2016/679.

Комисията може също така да спре прилагането на настоящото решение, да го измени или да го отмени, ако липсата на сътрудничество от страна на Европейската патентна организация възпрепятства Комисията да определи дали е засегната оценката, посочена в член 1 от настоящото решение.

Член 4

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 15 юли 2025 година.

За Комисията
Michael MCGRATH
Член на Комисията