Насоки

Насоки № 4/2019 относно член 25

Защита на данните на етапа на проектирането и по подразбиране

Версия 2.0

Приети на 20 октомври 2020 г.

История на версиите

Версия 1.0	13 ноември 2019 г.	Приемане на насоките за обществена консултация
Версия 2.0	20 октомври 2020 г.	Приемане на насоките от ЕКЗД след обществена консултация

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 70, параграф 1, буква д) от 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 (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за ЕИП и по-конкретно приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.,

като взе предвид членове 12 и 22 от своя Правилник за дейността,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

Резюме

В съвременния все по-цифровизиран свят спазването на изискванията за защита на данните на етапа на проектирането и по подразбиране има определяща роля за насърчаването на неприкосновеността на личния живот и защитата на данните в обществото. Поради това е от особено важно значение администраторите на лични данни да се отнасят сериозно към тази отговорност и да изпълняват задълженията, предвидени в ОРЗД, когато планират операции по обработване.

Настоящите насоки предоставят общи указания във връзка със задължението за защита на данните на етапа на проектирането и по подразбиране (ЗДЕПП), както е посочено в член 25 от ОРЗД. ЗДЕПП е задължение на всички администратори на данни, независимо от мащаба и степента на сложност на дейността по обработване. За да може администраторът на данни да изпълни изискванията за ЗДЕПП, е особено важно той да разбира принципите на защита на данните, както и правата, и свободите на субектите на данни.

Основното задължение е предприемането на *подходящи* мерки и осигуряването на необходимите гаранции, които обезпечават *ефективното изпълнение* на *принципите на защита на данните* и съответно *правата и свободите на субектите на данни на етапа на проектирането и по подразбиране*. В член 25 са определени изискванията за защита на етапа на проектирането и по подразбиране, които трябва да бъдат взети предвид. Те ще бъдат разгледани по-подробно в настоящите насоки.

В член 25, параграф 1 е предвидено, че администраторите следва да вземат предвид ЗДЕПП в началните етапи или когато планират нова операция по обработване. Администраторите прилагат ЗДЕПП *преди* обработването, а също така *текущо* по време на обработването, като проверяват редовно ефективността на определените мерки и гаранции. ЗДЕПП се прилага и към съществуващи системи, които обработват лични данни.

Насоките съдържат и указания как ефективно да се прилагат принципите на защита на данните, залегнали в член 5 от ОРЗД, където илюстративно са изброени ключовите елементи на етапа на проектирането и по подразбиране, както и примери от практиката. Администраторът следва да отчете дали предложените мерки са подходящи предвид конкретната дейност по обработване.

ЕКЗД е формулирал препоръки за това, как администраторите, обработващите лични данни и производителите могат да си сътрудничат за постигане на ЗДЕПП. Комитетът насърчава администраторите на данни в промишлеността, обработващите лични данни и производителите да използват ЗДЕПП като средство за постигане на конкурентно предимство, когато предлагат на пазара своите продукти на вниманието на администратори и субекти на данни. Освен това той насърчава всички администратори да използват сертификати и кодекси за поведение.

1 ОБХВАТ

1. Фокусът на насоките е върху прилагането от администраторите на защита на данните на етапа на проектирането и по подразбиране (наричана по-нататък „ЗДЕПП“) въз основа на задължението, предвидено в член 25 от ОРЗД.[1] Настоящите насоки могат да бъдат полезни и за други участници, например обработващи лични данни и производители на продукти, услуги и приложения (наричани по-нататък „производители“), които не са посочени пряко в член 25, при създаването на съвместими с ОРЗД продукти и услуги, които дават възможност на администраторите да изпълняват задълженията си за защита на данните.[2] В съображение 78 към ОРЗД е посочено, че принципите на ЗДЕПП следва да се вземат предвид и във връзка с процедурите по възлагане на обществени поръчки. Въпреки че всички администратори имат задължението да интегрират ЗДЕПП в дейностите си по обработване, тази разпоредба насърчава приемането на принципите на защита на данните, съгласно които държавните администрации трябва да дават пример. Администраторът е отговорен за изпълнението на задълженията за ЗДЕПП по отношение на обработването, осъществявано от подчинените му обработващи лични данни и техните подизпълнители, което предполага, че те следва да вземат предвид това задължение, когато сключват договори с тези лица.

2. Залегналото в член 25 изискване предполага, че администраторите трябва да гарантират, че принципите на защита на данните са отразени в проектирането на обработването на лични данни и като вариант на действие по подразбиране, като това е валидно за всички етапи от цикъла на обработване. Прилагане на ЗДЕПП се изисква и по отношение на системите за обработване, които са съществували преди влизането в сила на ОРЗД. Администраторите трябва да осигурят възможност за постоянно осъвременяване на дейностите по обработване в съответствие с ОРЗД. Повече информация относно това, как следва да се поддържа съответствието на съществуващи системи с изискванията за ЗДЕПП може да се намери в точка 2.1.4 от настоящите насоки. Основният смисъл на разпоредбата е да се осигури *подходяща* и *ефективна* защита на данните както на етапа на *проектирането*, така и по *подразбиране*, което означава, че администраторите трябва да са в състояние да докажат, че обработването включва подходящи предпазни мерки и гаранции, че принципите на защита на данните и правата и свободите на субектите на данни са ефективни.

[1] Предоставените тук тълкувания важат в еднаква степен за член 20 от Директива (ЕС) 2016/680 и член 27 от Регламент (ЕС) 2018/1725.

[2] В съображение 78 към ОРЗД тази необходимост е ясно посочена: „*При разработването, проектирането, подбора и използването на приложения, услуги и продукти, които се основават на обработване на лични данни или обработват лични данни, за да изпълнят функцията си, производителите на продукти, услуги и приложения следва да бъдат насърчавани да вземат предвид правото на защита на лични данни при разработването и проектирането на такива продукти, услуги и приложения и като отчитат надлежно достиженията на техническия прогрес, да се уверят, че администраторите и обработващите лични данни са в състояние да изпълняват своите задължения за защита на данните*“.

3. В Глава 2 от Насоките е поставен акцент върху тълкуването на изискванията по член 25 и са разгледани правните задължения, въведени с тази разпоредба. Примери за прилагане на ЗДЕПП по отношение на отделните принципи на защита на данните са представени в Глава 3.

4. В Глава 4 от Насоките е разгледана възможността за създаване на механизъм за сертифициране, с който да се доказва съответствие с изискванията на член 25, а в Глава 5 са представени начините, по които надзорните органи могат да осигуряват прилагането на член 25. На последно място, в Насоките са поместени допълнителни препоръки за заинтересованите страни за успешно прилагане на ЗДЕПП. ЕКЗД отчита предизвикателствата, с които се сблъскват малките и средните предприятия (наричани по-нататък „МСП“) в усилията си за постигане на пълно изпълнение на задълженията за ЗДЕПП и в Глава 6 е поместил допълнителни препоръки, адресирани конкретно към МСП.

2 АНАЛИЗ НА ЧЛЕН 25, ПАРАГРАФИ 1 И 2 ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ НА ЕТАПА НА ПРОЕКТИРАНЕТО И ПО ПОДРАЗБИРАНЕ

5. Целта на настоящата глава е да разгледа изискванията и да формулира насоки, свързани съответно със защитата на данните на етапа на проектирането съгласно член 25, параграф 1 от ОРЗД и със защитата на данните по подразбиране съгласно член 25, параграф 2 от ОРЗД. Защитата на данните на етапа на проектирането и защитата на данните по подразбиране са понятия, които се допълват и укрепват взаимно. Интересите на субектите на данни ще бъдат по-добре защитени от мерките за защита на данните по подразбиране, ако успоредно с това е осигурена и защита на данните на етапа на проектирането, и обратно.

6. ЗДЕПП е изискване към всички администратори на лични данни, включително малките предприятия и многонационалните компании. С оглед на това сложността при прилагането на ЗДЕПП варира в зависимост от конкретната операция по обработване. Администраторът и субектът на данните могат да извлекат ползи от прилагането на ЗДЕПП във всички случаи, независимо от мащаба.

2.1 Член 25, параграф 1: Защита на данните на етапа на проектирането

2.1.1 Задължение на администратора е да прилага подходящи технически и организационни мерки и необходимите гаранции в процеса на обработване

7. В съответствие с член 25, параграф 1 администраторът прилага *подходящи* технически и организационни *мерки*, разработени с цел прилагане на принципите на защита на данните, и въвежда *необходимите гаранции* в процеса на обработване, за да се спазят нормативните изисквания и да се защитят правата, и свободите на субектите на данни. Подходящите мерки и необходимите гаранции служат на една и съща цел — защита на правата на субектите на данни и гарантиране, че защитата на техните лични данни е част от процеса на обработване.

8. Понятията *технически и организационни мерки* и необходими *гаранции* може да се разбират в широк смисъл като всеки метод или средство, които администраторът може да използва в процеса на обработване. *Подходящи* означава, че мерките и необходимите гаранции следва да са годни да осигурят постигането на определената цел, т.е. те трябва да осигуряват

ефективното прилагане на принципите на защита на данните[3]. Следователно, изискването за подходящ характер е тясно свързано с изискването за ефективност.

9. Дадена техническа или организационна мярка и гаранция може да включва всичко — от използване на усъвършенствани технически решения до основно обучение на персонала. Примерите, които могат да са подходящи, в зависимост от характера и рисковете, свързани със съответната операция по обработване, включват псевдонимизиране на лични данни[4], съхранение на наличните лични данни в структуриран, широко използван и пригоден за машинно четене формат, предоставяне на възможност на субектите на данни да се намесват в дейността по обработване, предоставяне на информация за съхранението на лични данни, експлоатация на системи за откриване на зловреден софтуер, организиране на обучение на служителите по базова „киберхигиена“, въвеждане на системи за управление на неприкосновеността на личния живот и сигурността на информацията, въвеждане на договорни задължения за обработващите лични данни да прилагат определени практики за свеждане на данните до минимум и т.н.

10. Определянето на подходящите мерки може да бъде подпомогнато чрез използване на стандарти, най-добри практики и кодекси за поведение, утвърдени от сдружения и други органи, представляващи групи администратори на данни. Администраторът трябва обаче да се увери в подходящия характер на мерките по отношение на конкретната операция по обработване.

2.1.2 Разработени с цел ефективно прилагане на принципите на защита на данните и защита на правата и свободите на субектите на данни

11. *Принципите на защита на данните* са определени в член 5 (наричани по-нататък „принципите“), а *правата и свободите на субектите на данни* са основните права и свободи на физическите лица, и по-конкретно тяхното право на защита на данните, чиято защита е определена в член 1, параграф 2 като цел на ОРЗД (наричани по-нататък „правата“)[5]. Точната формулировка може да се намери в текста на Хартата на основните права на Европейския съюз. За администратора е особено важно да разбира съдържанието на *принципите* и *правата* като основание за защитата, гарантирана от ОРЗД, и по-конкретно задължението за ЗДЕПП.

12. Когато се планира въвеждането на подходящите технически и организационни мерки, и гаранции, те трябва да бъдат *разработени* с оглед на ефективното прилагане на всеки от посочените по-горе принципи и произтичащата от тях защита на права.

Постигане на ефективност

13. Ефективността стои в основата на понятието за защита на данните на етапа на проектирането. Изискването за ефективно прилагане на принципите означава, че администраторите трябва да осигуряват необходимите мерки и гаранции за защита на тези принципи, за да бъдат обезпечени правата и свободите на субектите на данни. Всяка реализирана мярка трябва да доведе до желаните резултати по отношение на предвиденото от администратора обработване. От тази констатация произтичат две последици.

14. Първо, тя означава, че член 25 не изисква осъществяването на специфични технически или организационни мерки, а само това, че избраните мерки и гаранции следва да бъдат подходящи

[3] „Ефективността“ е разгледана по-долу в точка 2.1.2
[4] Определение на това понятие се съдържа в член 4, параграф 5 от ОРЗД.
[5] Вж. съображение 4 към ОРЗД.

с оглед на прилагането на принципите на защита на данните в рамките на разглежданата дейност по обработване. Във връзка с това мерките и гаранциите следва да бъдат разработени така, че да са надеждни, а администраторът трябва да има капацитет да реализира допълнителни мерки, за да противодейства на възможно нарастване на нивото на риска[6]. Следователно ефективността на мерките зависи от характера на конкретната дейност по обработване и от оценката на определени елементи, които трябва да се вземат предвид, когато се определят средствата за обработване. Посочените елементи са разгледани по-долу в точка 2.1.3.

15. Второ, администраторите трябва да могат да докажат, че принципите се прилагат.

16. Предприетите мерки и гаранции следва да постигнат желания ефект по отношение на защитата на данните, а администраторът трябва да разполага с документация за реализираните технически и организационни мерки.[7] За целта администраторът може да определи подходящи ключови показатели за ефективност (КПЕ), за да докаже съответствие. КПЕ са определени от администратора измерими стойности, които отразяват с каква степен на ефективност администраторът постига своите цели по отношение на защитата на данните. КПЕ могат да бъдат *количествени*, например процентен дял на фалшивите положителни или фалшивите отрицателни резултати, намаляване на броя на жалбите, намаляване на времето за реакция, когато субектите на данни упражняват правата си, или *качествени*, например оценки на ефективността, използване на скали за оценяване или експертни оценки. Освен с помощта на КПЕ администраторите могат да докажат ефективното прилагане на принципите, като предоставят обосновката за своята оценка на ефективността на предприетите мерки и гаранции.

2.1.3 Елементи, които трябва да бъдат взети предвид

17. В член 25, параграф 1 са изброени елементи, които администраторът трябва да вземе предвид при определяне на мерките във връзка с конкретна операция по обработване. По-долу са дадени насоки за прилагането на тези елементи в процеса на проектиране, който включва проектиране на настройки по подразбиране. Всички тези елементи допринасят за преценката дали дадена мярка е подходяща за ефективното прилагане на принципите. Това означава, че всички тези елементи не са цели сами по себе си, а фактори, които трябва да бъдат отчетени в тяхната съвкупност, за да бъде постигната поставената цел.

2.1.3.1 „Достижения на техническия прогрес“

18. Критерият „достижения на техническия прогрес“ присъства в различни достижения на правото на ЕС, например в законодателството за опазване на околната среда и за безопасността на продуктите. В текста на ОРЗД препратка към „достиженията на техническия прогрес“[8] се прави

[6] „Основните принципи, приложими към администраторите (т.е. легитимност, свеждане на данните до минимум, ограничение на целите, прозрачност, цялостност на данните, точност на данните) трябва да останат непроменени, независимо от характера на обработването и рисковете за субектите на данни. Въпреки това надлежното отчитане на естеството и обхвата на обработването винаги е било неразделна част от прилагането на тези принципи, за да могат те по своята същност да подлежат на мащабиране“. Работна група по член 29, „Изявление за ролята на основания на риска подход в правната рамка за защита на данните“. РД 218, 30 май 2014 г., стр. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Вж. съображения 74 и 78.

[8] Вж. решението по дело „Kalkar“ на Федералния конституционен съд на Германия от 1978 г.: https://germanlawarchive.iuscomp.org/?p=67, което може да даде основа за методология за обективно

не само в член 32 относно мерките за сигурност,[910] но също и в член 25, с което този показател обхваща всички технически и организационни мерки, които са част от обработването.

19. В член 25 с препратката към „достижения на техническия прогрес“ се вменява задължение на администраторите **да отчитат текущия напредък на технологиите**, които се предлагат на пазара при определяне на подходящите технически и организационни мерки. Изискването към администраторите е да познават и следят технологичния прогрес, как технологиите могат да породят рискове и възможности във връзка със защитата на данните и как да се прилагат и актуализират мерките и гаранциите, които *осигуряват ефективното прилагане* на принципите и правата на субектите на данни при отчитане на развиващата се технологична среда.

20. „Достижения на техническия прогрес“ е динамичен критерий, който не може да бъде статично дефиниран в конкретен момент, а трябва да се оценява *непрекъснато* като се вземе предвид технологичния прогрес. Предвид това, администраторът може да установи, че мярка, която преди е осигурявала достатъчно ниво на защита, вече не е подходяща. Следователно пренебрегването на необходимостта от адаптиране към технологичните промени може да доведе до липса на съответствие с член 25.

21. Критерият „достижения на техническия прогрес“ се отнася не само до технологичните, но и до организационните мерки. Липсата на подходящи организационни мерки може да намали или дори изцяло да подкопае ефективността на избраната технология. Примерите за организационни мерки включват приемане на вътрешни политики, обучение, насочено към придобиване на актуални знания за дадена технология, сигурност и защита на данните, и политики за управление на сигурността, и административно управление на информационните технологии.

22. Действащи и утвърдени рамки, стандарти, сертификати, кодекси за поведение и др. в различни области могат да способстват за определяне на текущите „достижения на техническия прогрес“ в дадена практическа област. В областите, където такива стандарти са налице и осигуряват високо ниво на защита на субектите на данни, отговарящо или надхвърлящо предвиденото в законодателството, администраторите следва да ги вземат предвид при проектирането и прилагането на мерките за защита на данните.

2.1.3.2 „Разходи за прилагане“

23. Администраторът може да вземе предвид разходите за прилагане, когато определя и прилага подходящи технически и организационни мерки и необходими гаранции, които осигуряват ефективността на принципите, за да гарантира защитата на правата на субектите на данни. Разходите се отнасят до ресурсите като цяло, включително времето и човешките ресурси.

24. Критерият за оценка на разходите не задължава администратора да изразходва непропорционален обем ресурси, когато са достъпни алтернативни, изискващи по-малко

определение на понятието. На тази основа технологичното ниво на „достиженията на техническия прогрес“ ще бъде определено между технологичното ниво на „съществуващите научни познания и изследвания“ и по-утвърдените „общоприети технологични правила“. Следователно „достиженията на техническия прогрес“ могат да бъдат определени като технологичното ниво на дадена услуга, технология или продукт, които се предлагат на пазара и са най-ефективни за постигане на заложените цели.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

ресурси, но все пак ефективни мерки. Разходите във връзка с прилагането обаче са фактор, който следва да бъде взет предвид във връзка с осъществяването на защитата на данните на етапа на проектирането, а не основание да не се осъществява такава защита.

25. Следователно, всяка предприета мярка трябва да гарантира, че дейността по обработване, предвидена от администратора, не включва обработване на лични данни в нарушение на принципите, независимо от разходите. Администраторите следва да са в състояние да управляват общите разходи, за да могат да прилагат ефективно всички принципи и по този начин да осигурят защитата на правата.

2.1.3.3 „Естество, обхват, контекст и цел на обработването“

26. Администраторите трябва да вземат предвид естеството, обхвата, контекста и целта на обработването, когато определят необходимите мерки.

27. Тези фактори следва да се тълкуват при отчитане на тяхната роля съгласно други разпоредби на ОРЗД, като например членове 24, 32 и 35, с цел включване на принципите на защита на данните в дейностите по обработване.

28. Накратко, понятието за **естество** може да се разбира като присъщите[11] характеристики на обработването. **Обхватът** се отнася до мащаба и диапазона на обработването. **Контекстът** е свързан с обстоятелствата на обработването, които могат да окажат влияние върху очакванията на субекта на данни, а **целта** се отнася до целите на обработването.

2.1.3.4 „Породени от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица“

29. ОРЗД възприема последователен подход, основан на риска, в много от своите разпоредби, като например в членове 24, 25, 32 и 35, с оглед идентифициране на подходящи технически и организационни мерки за защита на физическите лица, техните лични данни и за спазване на изискванията на ОРЗД. Субектите на защита са винаги едни и същи (физическите лица чрез защита на личните им данни) и рисковете са едни и същи (за правата на лицата), като се вземат предвид едни и същи условия (естество, обхват, контекст и цели на обработването).

30. Когато администраторът извършва анализ на риска с цел осигуряване на съответствие с член 25, той трябва да идентифицира рисковете за правата на субектите на данни, произтичащи от потенциално нарушение на принципите и да определи вероятността те да се реализират, и тежестта им, с оглед да предприеме подходящи мерки за ефективно смекчаване на установените рискове. Извършването на систематична и обстойна оценка на дейността по обработване има определящо значение за осъществяването на оценката на риска. Например, администратор оценява конкретните рискове, свързани с липсата на свободно дадено съгласие, което е нарушение на принципа на законосъобразност, в хода на обработване на лични данни на деца и млади хора на възраст до 18 години, които съставляват уязвима група, като в конкретния случай липсва друго правно основание, и предприема подходящи мерки за ефективно смекчаване на установените рискове, свързани с тази група субекти на данни.

[11] Примерите включват специални категории лични данни, автоматизирано вземане на решения, неравноправност във взаимоотношенията, непредвидимо обработване, затруднения, с които се сблъсква субектът на данни във връзка с упражняването на правата си, и др.

31. „Насоките на ЕКЗД за оценка на въздействието върху защитата на данните (ОВЗД)“,[12] които се фокусират върху определянето, дали операцията по обработване може да доведе до висок риск за субекта на данни, съдържат и указания за оценяване на рисковете за защитата на данните и за процедурата по извършване на такава оценка. Тези насоки могат да бъдат полезни и във връзка с оценката на риска във всички случаи по споменатите по-горе членове, включително член 25.

32. Подходът, основан на оценката на риска не изключва използването на изходни нива, най-добри практики и стандарти. Те могат да предоставят на разположение на администраторите полезен набор от инструменти за преодоляване на подобни рискове в сходни ситуации (естество, обхват, контекст и цел на обработването). Казаното по-горе не отменя задължението по член 25 (както и по членове 24 и 32 и член 35, параграф 7, буква в) от ОРЗД) да се вземат предвид „*породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица*“. Следователно администраторите, въпреки че използват такива инструменти, трябва да извършват оценка на рисковете за защитата на данните във всеки отделен случай на обработване и да проверяват ефективността на предложените подходящи мерки и гаранции. В резултат на това, може да се наложи извършването и на оценка на въздействието върху защитата на данните (ОВЗД) или актуализация на съществуваща ОВЗД.

2.1.4 Времеви аспект

2.1.4.1 Към момента на определянето на средствата за обработване

33. Защитата на данните на етапа на проектирането се прилага „*към момента на определяне на средствата за обработване*“.

34. „*Средствата за обработване*“ варират от общите до конкретните елементи при проектирането на обработването, включително архитектурата, процедурите, протоколите, оформлението и външния вид.

35. „*Моментът на определяне на средствата за обработване*“ се отнася до периода от време, когато администраторът взема решение относно начина на осъществяване на обработването и механизмите, посредством които ще се осъществи то. Именно в процеса на вземане на тези решения администраторът трябва да оцени подходящите мерки и гаранции за ефективно прилагане на принципите и правата на субектите на данни при обработването и да вземе предвид елементи като достиженията на техническия прогрес, разходите за прилагане, естеството, обхвата, контекста, целта, както и рисковете. Това включва момента на придобиване и въвеждане в експлоатация на софтуер, хардуер и услуги за обработване на данни.

36. Вземането предвид на ЗДЕПП на ранен етап от процеса има определящо значение за успешното прилагане на принципите и за защитата на правата на субектите на данни. Освен това, от гледна точка на съотношението между разходите и ползите в интерес на администраторите е да вземат предвид ЗДЕПП по-рано, отколкото по-късно, тъй като може да се окаже трудно и скъпо да се внасят промени във вече изготвени планове, и в операции по обработване, които вече са разработени.

[12] Работна група по член 29, „Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679“. РД 248, версия 01, 4 октомври 2017 г. ec.europa.eu/newsroom/document.cfm?doc_id=47711 — одобрен от ЕКЗД

2.1.4.2 В момента на осъществяване на обработването (спазване и преглед на изискванията за защита на данните)

37. След като обработването започне, администраторът е обвързан с постоянното задължение да поддържа ЗДЕПП, т.е. с осигуряване на непрекъснато ефективно прилагане на принципите, за да бъдат гарантирани правата, да бъдат спазени достиженията на техническия прогрес, да се извършва преоценка на нивото на риска и т.н. Естеството, обхватът и контекстът на операциите по обработване, както и рискът, подлежат на промени по време на дейността по обработване, което означава, че администраторът трябва да оценява периодично операциите по обработване посредством редовен преглед и оценка на ефективността на определените мерки и гаранции.

38. Задължението за поддържане, преглед и актуализиране при необходимост на операцията по обработване се отнася и до съществуващи системи. Това означава, че заварените системи, които са разработени преди влизането в сила на ОРЗД, трябва да бъдат предмет на прегледи и поддръжка, за да се обезпечи прилагането на мерките и гаранциите, осигуряващи по ефективен начин зачитането на принципите и правата субектите на данни, както е посочено в настоящите насоки.

39. Това задължение обхваща и всяко обработване, извършвано от обработващите данни лица. Операциите на обработващите данни следва да бъдат редовно преглеждани и оценявани от администраторите, за да се гарантира, че те осигуряват непрекъснато зачитане на принципите и позволяват на администратора на данни да изпълнява задълженията си.

2.2 Член 25, параграф 2: Защита на данните по подразбиране

2.2.1 По подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването

40. Понятието „по подразбиране“, както често е определяно в компютърните науки, се отнася до съществуваща или предварително избрана стойност на подлежаща на конфигуриране настройка, която е зададена в рамките на софтуерно приложение, компютърна програма или устройство. Тези настройки се наричат също „предварително зададени настройки“ или „фабрични настройки“, особено по отношение на електронните устройства.

41. От горното следва, че понятието „по подразбиране“ при обработването на лични данни се отнася до определянето на стойности за конфигуриране или функции за обработване, които са зададени или предварително определени в рамките на система за обработване, като например софтуерно приложение, услуга или устройство, или до процедура за ръчно обработване, които оказват въздействие върху обема на събраните лични данни, обхвата на тяхното обработване, периода на тяхното съхранение и тяхната достъпност.

42. Администраторът следва да отговаря за въвеждането на такива настройки и опции по подразбиране, които да позволяват само обработване, което е строго необходимо за постигане на определената законосъобразна цел.. В това отношение, администраторите трябва да се осланят на преценката си относно необходимостта от обработването, като се вземат предвид правните основания, заложени в член 6, параграф 1. Това означава, че по подразбиране, администраторът не може да събира повече данни, отколкото са необходими, не може да извършва обработване на събраните данни, надхвърлящо необходимото за съответните цели, нито да ги съхранява за по-дълъг период. Основното изискване е защитата на данни да бъде включена по подразбиране при извършване на обработване на данните.

43. Администраторът е задължен да определи предварително за кои конкретни, изрични и законосъобразни цели се събират и обработват личните данни.[13] Мерките трябва по подразбиране да бъдат подходящи, за да се гарантира, че се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Насоките на ЕНОЗД за оценка на необходимостта и пропорционалността на мерките, които ограничават правото на защита на личните данни, могат да бъдат полезни и при преценката на вида данни, които трябва да бъдат обработени, за да се постигне конкретната цел.[14] [15] [16]

44. Когато администраторът използва софтуер, доставен от трети лица или стандартни софтуерни продукти, следва да извърши оценка на риска, свързан с използването на продукта и да се увери, че са изключени функциите, за които не е налице правно основание, или не са съвместими с определените цели на обработването.

45. Същите съображения се прилагат и за организационните мерки, подпомагащи операциите по обработване. Те трябва да бъдат по начало проектирани за обработване само на минималното количество лични данни, необходимо за конкретните операции. Това трябва да се има предвид особено във връзка с разпределянето на достъпа до данните между служители с различни роли и различни потребности от достъп.

46. Следователно, понятието за подходящи „технически и организационни мерки“ при защитата на данните по подразбиране се тълкува по същия начин, както беше посочено по-горе в точка 2.1.1, но тези мерки се прилагат конкретно във връзка с изпълнението на принципа на свеждане на данните до минимум.

47. Посоченото по-горе задължение за обработване само на личните данни, които са необходими за постигането на всяка конкретна цел, се прилага за следните елементи:

2.2.2 Параметри на задължението за свеждане на данните до минимум

48. В член 25, параграф 2 са изброени параметрите на задължението за свеждане на данните до минимум във връзка с обработването по подразбиране, като е посочено, че задължението се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.

2.2.2.1 „Обем на събраните лични данни“

49. Администраторите следва да вземат предвид както обема на личните данни, така и видовете, категориите и нивото на детайлност на личните данни, необходими за целите на обработването. Когато събират големи обеми лични данни, на етапа на проектирането те трябва да отчетат увеличения риск за принципите на цялостност и поверителност, свеждане на данните до

[13] Член 5, параграф 1, букви б), в), г) и д) от ОРЗД.
[14] ЕНОЗД. „Насоки за оценка на необходимостта и пропорционалността на мерките, които ограничават правото на защита на данните“. 25 февруари 2019 г. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf
[15] Вж. също ЕНОЗД. „Оценка на необходимостта от мерки, ограничаващи основното право на защита на личните данни: набор от инструменти“ https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
[16] За повече информация относно въпроса за необходимостта, вж. Работна група по член 29, „Становище № 06/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО“. РД 217, 9 април 2014 г. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_bg.pdf

минимум и ограничение на съхранението, и да го сравнят с намаления риск при събиране на намалени обеми и/или не толкова подробна информация за субектите на данни. Във всеки случай настройката по подразбиране не трябва да включва събиране на лични данни, които не са необходими за конкретната цел на обработването. Казано по друг начин, ако определени категории лични данни не са необходими или ако не са необходими подробни данни, тъй като са достатъчни не толкова подробни данни, ненужни лични данни не се събират.

50. Същите изисквания по подразбиране се прилагат по отношение на услугите, без оглед на използваната платформа или устройство — допуска се събиране само на необходимите лични данни за дадената цел.

2.2.2.2 „Степента на тяхното обработване“

51. Операциите по обработване[17] на лични данни се ограничават само до необходимото. Много операции по обработване могат да допринесат за съответната цел на обработването. Въпреки това фактът, че дадени лични данни са необходими за постигане на дадена цел, не означава, че тези данни могат да бъдат подложени на всякакви видове обработване и с произволна честота. Администраторите трябва също така да внимават да не разширяват границите на „съвместимите цели“ по член 6, параграф 4 и да преценяват кое обработване ще бъде в рамките на разумните очаквания на субектите на данни.

2.2.2.3 „Период на тяхното съхранение“

52. Не се допуска съхранение на събраните лични данни, ако това не е необходимо за целта на обработването и няма друга съвместима цел и правно основание в съответствие с член 6, параграф 4. Всяко запазване трябва да бъде обективно обосновано според случая от администратора на данни в съответствие с принципа на отчетност.

53. Администраторът трябва да ограничи периода на запазване до необходимото за постигането на целта. Когато личните данни вече не са необходими за целта на обработването, те по подразбиране следва да се изтрият или анонимизират. Следователно, продължителността на периода на запазване зависи от целта на конкретната операция по обработване. Това задължение е пряко свързано с принципа на ограничение на съхранението по член 5, параграф 1, буква д), и следва да се изпълнява по подразбиране, т.е. администраторът следва да разполага със систематични процедури за изтриване или анонимизиране на данни в процеса на обработването.

54. Анонимизирането[18] на лични данни е алтернатива на изтриването, при условие, че са взети предвид всички елементи и редовно се прави оценка на вероятността, и тежестта на риска, включително на риска от последващо идентифициране[19].

---

[17] Съгласно член 4, параграф 2 от ОРЗД това включва събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране; ограничаване, изтриване или унищожаване.

[18] Работна група по член 29. „Становище № 05/2014 относно техническите способи за анонимизиране“. РД 216, 10 април 2014 г. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_bg.pdf

[19] Вж. член 4, параграф 1 от ОРЗД, съображение 26 към ОРЗД, Работна група по член 29, „Становище № 05/2014 относно техническите способи за анонимизиране“. Вж. също подраздел „Ограничение на

2.2.2.4 „Тяхната достъпност“

55. Администраторът следва да ограничи обхвата на лицата, които имат достъп и определи видовете достъп до лични данни въз основа на оценка на необходимостта, както и да се увери, че личните данни в действителност са достъпни за лицата, които се нуждаят от тях, когато е необходимо, например в критични ситуации. Контролът върху достъпа следва да бъде налице за целия поток от данни по време на обработването.

56. Освен това в член 25, параграф 2 е посочено, че без намеса от страна на физическото лице, личните данни не трябва да бъдат достъпни за неограничен брой физически лица. По подразбиране, администраторът трябва да ограничи достъпа и да предостави на субекта на данните възможност да се намеси, преди да публикува или по друг начин да предостави лични данни за субекта на данни на неограничен брой физически лица.

57. Предоставянето на достъп до лични данни на неограничен брой физически лица може да доведе до още по-широко разпространение на данните от предвиденото. Това е от особено значение при използването на интернет търсачките. Това означава, че по подразбиране, администраторите следва да предоставят на субектите на данни възможност да се намесят, преди лични данни да бъдат предоставени за свободен достъп в интернет. Това е от особена важност, когато става дума за деца и лица от уязвими групи.

58. В зависимост от правните основания за обработването, може да има различни възможности за намеса в обработването. Например, да се иска съгласие за предоставяне на публичен достъп до личните данни или настройките за поверителност да бъдат заложени по такъв начин, че субектите на данни сами да могат да контролират публичния достъп.

59. Дори когато личните данни са публично достояние с разрешението и знанието на субекта на данните, това не означава, че всеки друг администратор с достъп до личните данни може свободно да ги обработва за собствени цели — той трябва да има отделно правно основание.[20]

3 ПРИЛАГАНЕ НА ПРИНЦИПИТЕ НА ЗАЩИТА НА ДАННИТЕ ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ ЧРЕЗ ИЗПОЛЗВАНЕТО НА ИЗИСКВАНИЯТА ЗА ЗАЩИТА НА ДАННИТЕ НА ЕТАПА НА ПРОЕКТИРАНЕТО И ПО ПОДРАЗБИРАНЕ

60. На всички етапи на проектиране на дейностите по обработване, включително обществени поръчки, тръжни процедури, възлагане на дейности на външни изпълнители, разработване, поддръжка, тестване, съхранение, изтриване и т.н., администраторът следва да взема предвид

съхранението“ от раздел 3 от настоящия документ, където е разгледана необходимостта администраторът да осигури ефективността на прилагания технически способ(и) за анонимизиране.

[20] Вж. решението по дело Satakunnan Markkinapörssi Oy и Satamedia Oy срещу Финландия, № 931/13.

и да разглежда различните елементи на ЗДЕПП, които ще бъдат илюстрирани нагледно с примерите в настоящата глава, свързани с прилагането на принципите.[21] [22] [23]

61. Администраторите трябва да въведат принципите, за да постигнат ЗДЕПП. Тези принципи включват: прозрачност, законосъобразност, добросъвестност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност и поверителност, и отчетност. Те са посочени в член 5 и съображение 39 към ОРЗД. на Осъзнаването на същността на всеки от тези принципи е важно за цялостно разбиране на начина за реализиране на ЗДЕПП.

62. Когато представихме примерите за прилагане на ЗДЕПП, направихме списъци на **основните елементи на ЗДЕПП**, свързани с всеки от принципите. Примерите, макар да обясняват конкретния принцип на защита на данните, могат да се припокриват и с други тясно свързани принципи. ЕКЗД подчертава, че основните елементи и примерите, поместени по-долу, не са нито изчерпателни, нито обвързващи, а служат като насоки, свързани с всеки от принципите. Администраторите трябва да преценяват по какъв начин да гарантират съответствието с принципите при конкретната операция по обработване.

63. Макар че настоящият раздел е посветен на прилагането на принципите, администраторът трябва също така да въведе *подходящи* и *ефективни* начини за защита на правата на субектите на данни, включително в съответствие с глава III от ОРЗД, в случаите, когато това не е изрично предвидено в самите принципи.

64. Принципът на отчетност има първостепенно значение: съгласно този принцип администраторът носи отговорност за избора на необходимите технически и организационни мерки.

3.1 Прозрачност[24]

65. Администраторът трябва да предостави ясна и открита информация на субекта на данните за това как ще събира, използва и споделя лични данни. Прозрачността означава да се даде възможност на субектите на данни да разберат и, ако е необходимо, да се възползват от правата си съгласно членове 15—22. Принципът е заложен в членове 12, 13, 14 и 34. Предвидените мерки и гаранции в подкрепа на принципа на прозрачност следва да гарантират и прилагането на тези разпоредби.

66. Ключовите елементи относно принципа на прозрачност на етапа на проектирането и по подразбиране могат да включват:

- яснота: информацията трябва да е представена на ясен и достъпен език, да бъде кратка и разбираема;
- смисъл: съобщенията следва да имат ясно значение за конкретната аудитория;
- достъпност: информацията трябва да е лесно достъпна за субекта на данните;

[21] Повече примери можете да намерите в: Орган за защита на данните на Норвегия, „Software Development with Data Protection by Design and by Default“ (Разработване на софтуер със защита на данните на етапа на проектирането и по подразбиране), 28 ноември 2017 г. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] Понятието за прозрачност е подробно разгледано в документа на Работната група по член 29: „Насоки относно прозрачността в съответствие с Регламент 2016/679“. РД 260, версия 01, 11 април 2018 г. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 — одобрен от ЕКЗД

- контекст: информацията следва да е предоставена в правилния момент и в подходяща форма;
- уместност: информацията следва да е съотносима и приложима към конкретния субект на данни;
- универсална форма: информацията трябва да бъде достъпна за всички субекти на данни, да включва използване на подлежащи на машинно четене езици, за да се улесни и автоматизира четимостта и яснотата;
- разбираема: субектите на данни трябва да разбират достатъчно добре какво могат да очакват във връзка с обработването на личните им данни, особено когато става дума за деца или членове на други уязвими групи;
- различни комуникационни канали: информацията трябва да се предоставя чрез различни канали и медии, не само чрез писмен текст, за да повиши вероятността за реално достигне на информацията до субекта на данните;
- структурирана в различни нива: информацията следва да бъде структурирана в различни нива по такъв начин, по който да бъде преодоляно противоречието между изисквания за пълнота и разбираемост, като същевременно се вземат предвид разумните очаквания на субектите на данни.

Пример[25]

Администратор на данни разработва политика в областта на неприкосновеността на личния живот във връзка със своя уебсайт, за да изпълни изискванията за прозрачност. Изложението на политиката в областта на неприкосновеността на личния живот не следва да съдържа обемна информация, която е трудна за анализ и разбиране от типичния субект на данни. То трябва да бъде написано ясно и сбито, така че да помогне на потребителите на уебсайта да разберат как се обработват техните лични данни. Следователно, администраторът предоставя информация на различни нива, като са подчертани най-важните елементи. Предоставен е лесен достъп до по-подробна информация. Включени са падащи менюта и връзки към други страници за допълнително разяснение на елементите и понятията, използвани в изложението на политиката. Наред с горното администраторът следва да гарантира, че информацията се предоставя посредством различни канали, като чрез видеоклипове се разясняват най-важните елементи от писмената информация. Координирането на посланията на отделните страници има определящо значение, за да се гарантира, че подходът на предоставяне на информацията по различни начини помага за ориентирането на потребителя, вместо да го обърква.

Политиката в областта на неприкосновеността на личния живот не трябва да е трудно достъпна за субектите на данни. Следователно, тя трябва да е налична и видима на всички страници от съответния уебсайт, така че субектът на данни да може във всеки момент да получи достъп до информацията с едно щракване на мишката. Освен това предоставената информация следва да е разработена в съответствие с най-добрите практики и стандарти за универсално оформление, за да бъде достъпна за всички.

Наред с това необходимата информация трябва да бъде предоставена и в съответния контекст, и в подходящия момент. Тъй като администраторът на данни извършва многобройни операции по обработване, като използва данните, събрани чрез уебсайта, поместването на обща политика в областта на неприкосновеността на личния живот само на уебсайта не е достатъчно, за да се приеме, че администраторът е изпълнил изискванията за прозрачност. С оглед на това,

[25] Френският Орган за защита на данните публикува няколко примера, илюстриращи най-добри практики за информиране на потребителите, както и други принципи на прозрачност: https://design.cnil.fr/en/

администраторът следва да разработи модел за информиране, който да предоставя на субекта на данни подходяща информация с помощта например на фрагменти или изскачащи прозорци. Например, когато приканва физическото лице да въведе личните си данни, администраторът трябва да го информира, как ще бъдат обработени личните му данни и защо те са необходими за обработването.

3.2 Законосъобразност

67. Администраторът следва да определи валидно правно основание за обработването на личните данни. Мерките и гаранциите трябва да гарантират, че цялостният цикъл на обработване е в съответствие с приложимите правни основания за обработването.

68. Ключовите елементи за законосъобразност на етапа на проектирането и по подразбиране могат да включват:
    - уместност: към обработването следва да се приложи правилното правно основание;
    - разграничаване[26]: правното основание, използвано за всяка дейност по обработване, трябва да бъде разграничено.
    - конкретно посочена цел: трябва да е налице ясна връзка между подходящото правно основание и конкретната цел на обработването;[27]
    - необходимост: обработването трябва да е необходимо и безусловно, за да е законосъобразна целта.
    - автономност: субектът на данни трябва да има възможно най-висока степен на автономност по отношение на контрола върху личните данни в рамките на правното основание;
    - получаване на съгласие: съгласието трябва да е свободно изразено, конкретно, информирано и недвусмислено.[28] Особено внимание следва да се отделя на способността на децата и младите хора да предоставят информирано съгласие;
    - оттегляне на съгласието: когато съгласието има функцията на правно основание, процедурата по обработване следва да улеснява оттеглянето на съгласието. Оттеглянето на съгласието трябва да бъде също толкова лесно, колкото и даването му. Ако това не е така, прилаганият от администратора механизъм за даване на съгласие не съответства на изискванията на ОРЗД;[29]
    - претегляне на интересите: когато наличието на законни интереси е използвано като правно основание, администраторът трябва да извърши претегляне на интересите, отделяйки особено внимание на наличието на неравноправни възможности, по-конкретно по отношение на деца до 18-годишна възраст и членове на други уязвими групи. Необходимо е да са налице мерки и гаранции за смекчаване на неблагоприятното въздействие върху субектите на данни;
    - предварително определяне: правното основание следва да бъде определено преди извършването на обработването;

[26] ЕКЗД. „Насоки № 2/2019 относно обработката на лични данни съгласно член 6, параграф 1, буква б) от Общия регламент относно защита на данните при предоставянето на онлайн услуги на субектите на данни“ Версия 2.0, 8 октомври 2019 г. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_bg.pdf

[27] Вж. раздела относно ограничение на целите по-долу.

[28] Вж. Насоки № 05/2020 относно съгласието съгласно Регламент 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_bg

[29] Вж. Насоки № 05/2020 относно съгласието съгласно Регламент 2016/ 679, стр. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_bg

- прекратяване: ако правното основание престане да бъде приложимо, обработването се прекратява;
- коригиране: ако е налице валидна промяна в правното основание за обработването, дейността по обработване следва да бъде коригирана в съответствие с новото правно основание.[30]
- разпределение на отговорностите: когато е предвидено съвместно администриране, страните трябва да разпределят по ясен и прозрачен начин отговорностите си по отношение на субекта на данните и да разработят мерките във връзка с дейностите по обработване.

Пример

Банка планира да предложи услуга за повишаване на ефективността на управлението на заявления за заеми. Идеята на услугата е, че банката трябва да може, след като поиска разрешение от клиента, да получава данни от публичните данъчни органи за него. В този пример не се разглежда обработването на лични данни от други източници.

Получаването на лични данни за финансовото положение на субекта на данните е необходимо, за да се предприемат стъпки по искането му преди сключване на договор за заем.[31] Събирането на данни пряко от данъчната администрация обаче не се счита за необходимо, тъй като клиентът може да сключи договора, предоставяйки лично информацията от данъчната администрация. Макар че банката може да има законен интерес да получи пряко документите от данъчната администрация, например с цел да се гарантира ефективността на разглеждането на искането за заем, предоставянето на такъв пряк достъп на банките до личните данни на заемоискателите поражда рискове, свързани с използването или потенциалната злоупотреба с правата на достъп.

Във връзка с прилагането на принципа на законосъобразност администраторът разбира, че в този случай не може да използва основанието „необходимост за изпълнение на договора“ за частта от обработването, която включва събиране на лични данни пряко от данъчните органи. Фактът, че това конкретно обработване води до риск субектът на данните да участва в по-малка степен в обработването на неговите данни, също е съотносим за оценката на законосъобразността на самото обработване. Банката прави заключението, че тази част от обработването трябва да се опира на друго правно основание. В конкретната държава членка, където администраторът осъществява дейността си, действа национално законодателство, което допуска банката да събира информация пряко от публичните данъчни органи, когато субектът на данните е дал предварително своето съгласие за това.

Поради това банката предоставя информацията за обработването на онлайн платформата си по такъв начин, че да улеснява субектите на данни да разбират кое обработване е задължително и кое не е. По подразбиране, опциите за обработване не допускат извличане на данни пряко от други източници освен от самото физическо лице, а опцията за пряко получаване на информация е представена по начин, който не възпира субекта на данните да оттегли съгласието си. Всяко дадено съгласие за събиране на данни пряко от други администратори, осигурява временно право на достъп до определен набор от информация.

[30] В случаите, когато формата на първоначалното правно основание е съгласие, вж. Насоки № 05/2020 относно съгласието съгласно Регламент 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_bg

[31] Вж. член 6, параграф 1, буква б) от ОРЗД.

Всяко дадено съгласие се обработва по електронен път, така че да може да бъде документирано и на субектите на данни се предоставя лесен начин да контролират съдържанието на даденото от тях съгласие, както и да го оттеглят.

Администраторът е направил предварителна оценка на изискванията за ЗДЕПП и включва всички тези критерии в спецификацията на изискванията си в търга за доставка на платформата. Администраторът разбира, че ако не включи изискванията за ЗДЕПП в предложението, впоследствие може да е твърде късно или да се окаже твърде скъпо да се приложи защита на данните.

3.3 Добросъвестност

69. Добросъвестността е принцип от първостепенно значение, съгласно който личните данни не трябва да се обработват по начин, който е необосновано увреждащ, незаконно дискриминационен, неочакван или подвеждащ за субекта на данните. Мерките и гаранциите за прилагане на принципа на добросъвестност са в подкрепа и на правата, и свободите на субектите на данни, и по-специално на правото на информация (прозрачност), правото на намеса (достъп, изтриване, преносимост на данните, коригиране), и правото на ограничаване на обработването (право да не бъдат обект на автоматизирано индивидуално вземане на решения и право на субектите на данни да не бъдат подложени на дискриминация във връзка с тези процеси).

70. Ключовите елементи на добросъвестността на етапа на проектирането и по подразбиране могат да включват:
    - автономност: субектите на данни следва да се ползват с възможно най-висока степен на автономност при определянето на начините, по които да се използват техните лични данни, както и по отношение на обхвата и условията на това използване или обработване;
    - взаимодействие: субектите на данните трябва да могат да съобщават и упражняват своите права по отношение на личните данни, обработвани от администратора;
    - очаквания: обработването трябва да бъде в съответствие с разумните очаквания на субектите на данните;
    - равнопоставеност: администраторът не трябва да дискриминира неоснователно субектите на данни;
    - липса на експлоатация: администраторът не трябва да се възползва от нуждите или уязвимостите на субектите на данни;
    - избор на потребителите: администраторът не трябва да поставя по несправедлив начин потребителите в „обвързано положение“. Когато дадена услуга, която обработва лични данни, използва собствени стандарти е възможно потребителите да бъдат обвързани с нея, като тази практика може да е несправедлива, ако накърнява възможностите на субектите на данни да упражняват правото си на преносимост на данните в съответствие с член 20;
    - баланс на възможностите: поддържането на баланс на възможностите следва да е ключова цел в отношенията между администратора и субекта на данни. Ситуации на неравноправни възможности следва да се избягват. Когато това не е възможно, такива ситуации трябва да се отчитат и да се предприемат подходящи компенсиращи мерки;
    - недопустимост на прехвърляне на рисковете: администраторите не трябва да прехвърлят рисковете на предприятието върху субектите на данни;

- забрана за въвеждане в заблуждение: информацията и опциите относно обработването на данни следва да се предоставят по обективен и неутрален начин, като се избягват заблуждаващи или манипулативни формулировки или представяне;
- зачитане на правата: администраторът трябва да зачита основните права на субектите на данни и да прилага подходящи мерки и гаранции, като не може да накърнява тези права, освен в случаите, изрично предвидени в закона;
- етични съображения: администраторът следва да преценява по-широкия ефект от обработването върху правата и достойнството на физическите лица;
- честност: администраторът трябва да предоставя информация за начина, по който обработва личните данни, да действа по начина, по което е заявил, че ще действа, и да не въвежда в заблуждение субектите на данни;
- човешка намеса: администраторът трябва да осигури *компетентна* човешка намеса, която е в състояние да установи отклонения, въведени в резултат на използването на машини, в съответствие с правото на потребителите да не бъдат обект на автоматизирано вземане на индивидуални решения съгласно член 22.[32]
- справедливи алгоритми: редовно трябва да се оценява дали алгоритмите функционират съобразно приложимите цели и те да се коригират с цел смекчаване на установените отклонения, и да се обезпечи добросъвестността на обработването. Субектите на данни следва да се уведомяват за функционирането на операции по обработване на лични данни въз основа на алгоритми, които анализират или правят прогнози за тях, например по отношение на трудовото изпълнение, икономическото положение, здравословното състояние, личните предпочитания, надеждността или поведението, местоположението или движението им.[33]

Пример 1

Администратор управлява търсачка в интернет, която обработва предимно генерирани от потребители лични данни. Администраторът се възползва от наличието на големи обеми от лични данни и от възможността да ги използва за целеви реклами. Поради това администраторът желае да убеди субектите на данни да разрешат разширено събиране и използване на техните лични данни. Съгласието на субектите на данни ще се получава чрез представяне на опции за обработване.

Във връзка с прилагането на принципа на добросъвестност и предвид естеството, обхвата, контекста и целта на обработването администраторът разбира, че не може да представи опциите по такъв начин, че да мотивира субекта на данните да разреши събиране на повече лични данни, отколкото ако опциите са представени по справедлив и неутрален начин. Това означава, че администраторът не може да представя опциите за обработване по начин, който възпрепятства отказа за споделяне на данни от страна на субектите на данни или възпрепятства коригирането на настройките за поверителност и ограничаването на обработването от страна на лицата. Това са примери за недобросъвестни практики, които противоречат на духа на член 25. Опциите по подразбиране за обработването трябва да бъдат неинвазивни и последващото

[32] Вж. „Насоки относно автоматизирано вземане на индивидуални решения и профилиране за целите на Регламент 2016/679“, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Вж. съображение 71 към ОРЗД.

обработване следва да бъде представено по такъв начин, че да не се оказва натиск върху субектите на данни да предоставят съгласието си. Следователно, администраторът представя възможностите за предоставяне или отказ на съгласие като два еднакви избора, като предоставя точна информация за последствията от всеки избор за субекта на данните.

Пример 2

Друг администратор обработва лични данни с цел предоставяне на стрийминг услуга, при която потребителите могат да избират между обикновен абонамент със стандартно качество и премиум абонамент с по-високо качество. Като част от премиум абонамента абонатите получават приоритетно обслужване.

Във връзка с принципа на добросъвестност приоритетното обслужване на клиенти, предоставяно на абонати на премиум услугата, не трябва да дискриминира възможностите на останалите абонати за достъп за упражняване на правата им в съответствие с член 12 от ОРЗД. Това означава, че въпреки че абонатите на премиум услугата получават приоритетно обслужване, приоритизирането не следва да води до липса на подходящи мерки за удовлетворяване на заявките на редовните абонати без ненужно забавяне и във всеки случай в рамките на един месец от получаване на заявките.

Приоритетните клиенти плащат, за да получат услуга с по-високо качество, но всички субекти на данни разполагат с равни и еднакви възможности за упражняване на своите права и свободи в съответствие с член 12.

3.4 Ограничение на целите[34]

71. Администраторът трябва да събира данни за конкретни, ясни и законни цели и да не обработва допълнително данните по начин, който е несъвместим с целите, за които са били събрани.[35] Следователно основно съображение при проектирането на дейностите по обработване трябва да бъде въпросът какво е необходимо за постигане на целите. Ако трябва да се извърши допълнително обработване, администраторът първо трябва да се увери, че целите на това обработване са съвместими с първоначалните, и да проектира обработването, така че да се съобразява с тях. Съвместимостта на новата цел следва да се оцени въз основа на критериите по член 6, параграф 4.

72. Ключовите елементи на ограничението на целите на етапа на проектирането и по подразбиране могат да включват:
    - предварително определяне: законните цели трябва да бъдат определени преди проектирането на обработването;
    - конкретност: целите следва да бъдат точно определени и да посочват изрично причините за обработването на личните данни;

[34] Работната група по член 29 предостави насоки за разясняване на принципа на ограничение на целите съгласно Директива 95/46/ЕО. Въпреки че становището не е прието от ЕКЗД, то може да е приложимо, тъй като формулировката на принципа е същата, както в ОРЗД. Работна група по член 29, „Становище № 03/2013 относно ограничението на целите“. РД 203, 2 април 2013 г. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Член 5, параграф 1, буква б) от ОРЗД.

- водещ характер на целта: целта на обработването трябва да бъде водеща при проектирането на дейността по обработване и да определя нейните граници;
- необходимост: целта определя какви лични данни са необходими за обработването;
- съвместимост: всяка нова цел трябва да бъде съвместима с първоначалната цел, за която са събрани данните, и да бъде в основата на съответните промени в проектирането;
- ограничение на допълнителното обработване: администраторът не трябва да свързва различни видове данни или да извършва допълнително обработване за нови несъвместими цели;
- технически ограничения за повторно използване: администраторът трябва да използва технически мерки, включително хеширане и криптиране, за да ограничи възможността за използване на личните данни за нова цел. Освен това администраторът следва да е въвел организационни мерки като политики и договорни задължения, които ограничават повторното използване на личните данни;
- преглед: администраторът трябва редовно да преценява дали обработването е необходимо за целите, за които са събрани данните и да тества, дали заложения модел съответства на изискването за ограничението на целите.

Пример

Администратор обработва лични данни на своите клиенти. Обработването се осъществява с цел изпълнение на договор, т.е. доставка на стоки до правилния адрес и получаване на плащане. Съхраняваните лични данни са хронология на покупките, име, адрес, електронна поща и телефонен номер.

Администраторът възнамерява да закупи продукт за управление на взаимоотношенията с клиенти, който обединява на едно място всички данни на клиентите във връзка с продажбите, маркетинга и обслужването. Продуктът дава възможност за запаметяване на всички телефонни обаждания, дейности, документи, електронни писма и маркетингови кампании с цел изготвяне на пълен профил на клиента. Наред с горното софтуерът за управление на взаимоотношенията с клиентите анализира автоматично покупателната способност на клиентите, като използва публична информация. Целта на анализа е постигането на по-голяма ефективност на дейностите по реклама. Тези дейности не са елементи от първоначалната законосъобразна цел на обработването.

За да приложи принципа на ограничение на целите, администраторът изисква от доставчика на продукта да отбележи различните дейности по обработване, при които се използват лични данни съобразно целите на администратора.

След като получава резултата, администраторът оценява дали новата цел, свързана с маркетинговите дейности и тази, отнасяща се до насочената реклама са съвместими с първоначалните цели, определени на етапа на събиране на данните, и дали е налице достатъчно правно основание за съответната дейност по обработване. Ако резултатът от оценката не е положителен, администраторът не следва да използва съответните функции. Алтернативно администраторът може да се откаже от тази оценка и просто да не използва описаните функции на продукта.

3.5 Свеждане на данните до минимум

73. Обработват се само лични данни, които са подходящи, свързани със и ограничени до **необходимото** във връзка с целите, за които се обработват.[36] Поради това администраторът трябва предварително да определи кои характеристики и параметри на системите за обработване и техните поддържащи функции са допустими. Свеждането на данните до минимум обосновава и изпълнява принципа на необходимост. При допълнителното обработване администраторът следва периодично да преценява дали обработваните лични данни продължават да са подходящи, уместни и необходими или дали те трябва да бъдат изтрити или анонимизирани.

74. На първо място администраторите трябва да определят дали е необходимо да обработват лични данни за постигането на съответните цели. Администраторът проверява дали съответните цели могат да бъдат постигнати посредством обработване на по-малък обем лични данни или на по-малко подробни или на обобщени лични данни, или без изобщо да се прибягва до обработване на лични данни[37]. Тази проверка следва да се предприеме, преди да се пристъпи към обработване, но тя може също така да бъде извършена на всеки етап на цикъла на обработване. Този подход е в съответствие и с член 11.

75. Свеждането на данните до минимум може да се отнася и до степента на идентифициране. Ако целта на обработването не предполага окончателният набор от данни да посочва идентифицирано или подлежащо на идентифициране физическо лице (например- за статистическа цел), но за първоначалното обработване това е необходимо (например- преди обобщаване на данните), администраторът следва да анонимизира личните данни, веднага щом идентифицирането престане да бъде необходимо. Алтернативно, ако идентифицирането е необходимо за други дейности по обработване, личните данни трябва да бъдат псевдонимизирани, за да се намалят рисковете за правата на субектите на данни.

76. Ключовите елементи, свързани със свеждането на данните до минимум на етапа на проектирането и по подразбиране, могат да включват:
    - избягване на обработването на данни: обработването на лични данни трябва да се избягва винаги, когато това е възможно с оглед постигането на съответната цел;
    - ограничение: обемът на събираните лични данни трябва да се ограничава до необходимото за постигането на целта;
    - ограничение на достъпа: дейността по обработване на данни трябва да се планира по такъв начин, че минимален брой лица да се нуждаят от достъп до личните данни, за да могат да изпълняват задълженията си, като достъпът трябва да се ограничи;
    - уместност: личните данни трябва да бъдат съотносими към конкретната дейност по обработване и администраторът следва да може да докаже тази съотносимост;
    - необходимост: всяка категория лични данни трябва да е необходима за постигане на посочените цели и следва да се обработва, само ако не е възможно тези цели да се постигнат по друг начин;
    - обобщаване: обобщени данни трябва да се използват винаги, когато това е възможно;
    - псевдонимизиране: личните данни трябва да бъдат псевдонимизирани веднага, щом отпадне необходимостта от лични данни, пряко идентифициращи лицата, а ключовете за идентифициране трябва да се съхраняват отделно;
    - анонимизиране и изтриване: когато личните данни вече не са необходими за постигането на целта, те трябва да бъдат анонимизирани или изтрити;

[36] Член 5, параграф 1, буква в) от ОРЗД.

[37] Съображение 39 към ОРЗД гласи: „...Личните данни следва да се обработват, единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства.“

- поток от данни: потокът от данни следва да бъде достатъчно ефикасен, за да не се създават повече копия, отколкото е необходимо;
- „достижения на техническия прогрес“: администраторът трябва да прилага съвременни и подходящи технологии за избягване на обработването и свеждане до минимум на данните.

Пример 1

Книжарница иска да увеличи приходите си, като продава книги онлайн. Собственикът на книжарницата иска да създаде стандартизиран формуляр за поръчки. За да е сигурен, че клиентите ще въвеждат цялата необходима информация, собственикът на книжарницата прави всички полета във формуляра задължителни за попълване (ако не попълни всички полета, клиентът не може да направи поръчка). Първоначално собственикът на уебмагазина използва стандартен формуляр за контакти, в който клиентът трябва да въведе датата си на раждане, телефонния си номер и домашния си адрес. Все пак не всички полета във формуляра са необходими за закупуването и доставката на книгите. В този конкретен случай, ако субектът на данните заплати продукта предварително, неговата дата на раждане и телефонен номер не са задължителни за закупуването на продукта. Това означава, че не е допустимо тези полета в уебформуляра да са задължителни за попълване, за да може клиентът да поръча продукта, освен ако администраторът може да докаже убедително, че тези данни са необходими на друго основание и да обоснове необходимостта от попълването на полетата. Освен това в някои случаи предоставянето на адрес не е необходимо. Например когато клиентът поръчва електронна книга, той може да изтегли продукта пряко на своето устройство.

Поради това собственикът на уебмагазина решава да направи два уебформуляра: един за поръчка на книги с поле за адреса на клиента и един за поръчка на електронни книги без поле за адреса на клиента.

Пример 2

Дружество за обществен транспорт желае да събира статистически данни за маршрутите на пътниците. Това е полезно във връзка с въвеждането на целесъобразни промени в разписанията на обществения транспорт и точните маршрути на влаковете. Пътниците трябва да поставят билета си в четец всеки път, когато влизат или излизат от транспортно средство. След като извършва оценка на риска, свързан с правата и свободите на пътниците по отношение на събирането на данни за маршрутите на пътуване, администраторът установява, че е възможно да се идентифицират пътниците в случаите, когато те живеят в рядко населени райони, въз основа на единен идентификатор на маршрута с помощта на номера на билета. Поради това администраторът не съхранява идентификаторите на билетите, тъй като те не са необходими за оптимизиране на разписанията на обществения транспорт и маршрутите на влаковете. След приключването на пътуването администраторът съхранява само отделните маршрути на пътуване, за да не могат да се идентифицират пътувания, свързани с един билет, като запазва само информацията за отделните маршрути.

В случаите, когато въпреки горното е налице риск да се идентифицира дадено лице единствено въз основа на маршрута му, администраторът прилага статистически мерки, за да намали риска, като например заличаване на информацията за началната и крайната точка на маршрута.

Пример 3

Куриерска фирма желае да оцени ефективността на извършваните от нея доставки във връзка със сроковете за доставка, планирането на работното натоварване и разхода на гориво. За да постигне тази цел, куриерската фирма трябва да обработи съвкупност от лични данни, свързани както със служителите (водачи), така и с клиенти (адреси, стоки, които трябва да бъдат доставени и др.). Тази операция по обработване крие рискове във връзка както с наблюдението на служителите, за което са необходими конкретни правни гаранции, така и със събирането на информация за потребителските навици на клиентите въз основа на доставените стоки. Тези рискове могат да бъдат значително намалени посредством подходящо псевдонимизиране на данните за служителите и клиентите. По-специално, ако ключовете за псевдонимизиране се сменят често и се използват по-големи зони, вместо конкретни адреси, се постига ефективно свеждане на данните до минимум и администраторът може да се концентрира единствено върху процеса на доставка и целта за оптимизиране на ресурсите, без да прекрачва границата с наблюдение на поведението на лицата (клиентите или служителите).

Пример 4

Болница събира данни за своите пациенти в болнична информационна система (електронно здравно досие). Служителите на болницата се нуждаят от достъп до картоните на пациентите, за да могат да вземат информирани решения относно грижите и лечението им, както и за да документират всички предприети действия за диагностициране, грижи и лечение. По подразбиране такъв достъп се предоставя само на тези членове на медицинския персонал, които са ангажирани с лечението на съответния пациент в отделението, където се лекува той или тя. Групата на лицата, които имат достъп до картона на пациента, се разширява, когато в лечението участват други отделения или диагностични звена. След изписването на пациента и изготвянето на съответните документи достъпът се ограничава до малка група служители от специален отдел, които отговарят на запитвания за здравна информация или консултации, направени или поискани от други доставчици на здравни услуги с разрешението на съответния пациент.

3.6 Точност

77. Личните данни следва да са точни и поддържани в актуален вид, като трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.[38]

78. Изискванията трябва да се разглеждат във връзка с рисковете и последиците от конкретното използване на данните. Неточните лични данни могат да представляват риск за правата и

[38] Член 5, параграф 1, буква г) от ОРЗД.

свободите на субектите на данни: например, когато водят до неправилна диагноза или неправилно обработване на здравен протокол или когато неправилно изграденият образ на даден човек може да доведе до вземане на решения на грешна основа, ръчно, чрез автоматизирано вземане на решения или чрез изкуствен интелект.

79. Ключовите елементи на точността на етапа на проектирането и по подразбиране могат да включват:
    - източник на данни: източниците на данни трябва да бъдат надеждни по отношение на точността на данните;
    - степен на точност: всеки елемент от личните данни трябва да бъде толкова точен, колкото е необходимо за постигането на конкретните цели;
    - измерима степен на точност: намаляване на броя на фалшивите положителни или отрицателни резултати, като например отклонения при автоматизирано вземане на решения и използване на изкуствен интелект;
    - проверка: в зависимост от естеството на данните и от това колко често се променя то администраторът следва да се консултира със субекта на данните относно тяхната точност преди и по време на различните етапи на обработването;
    - изтриване / коригиране: администраторът е длъжен да изтрие или коригира незабавно неточни данни. Той е задължен да улесни изтриването или коригирането на данните, когато субектите на данни са или са били деца, които по-късно желаят да премахнат такива лични данни;[39]
    - избягване на разпространението на грешки: администраторите трябва да смекчат ефекта от натрупване на грешки във веригата на обработване;
    - достъп: на субектите на данни трябва да бъде предоставена информация за, и лесен достъп до личните данни в съответствие с членове 12—15 от ОРЗД, за да се контролира дали са точни и да се коригират при необходимост;
    - текуща точност: личните данни трябва да бъдат точни на всички етапи от обработването, като при критични ситуации трябва да се извършват тестове за точност;
    - актуалност: личните данни трябва да се актуализират, ако това е необходимо за постигането на целта;
    - проектиране на данните: трябва да се използват технологични и организационни характеристики за намаляване на неточностите, например да се предоставят кратки, предварително формулирани отговори с възможност за избор, вместо полета за вписване на свободен текст.

Пример 1

Застрахователно дружество желае да използва решение за изкуствен интелект (ИИ), за да изготви профили на клиентите си, които купуват застраховки, които да използва като основа за своя процес на вземане на решения относно изчисляването на застрахователния риск. Когато определят как трябва да се разработят решенията за изкуствен интелект, представителите на дружеството определят и средствата за обработване, и трябва да вземат предвид изискванията за защита на данните на етапа на проектирането, при избора на приложение за изкуствен интелект и когато решават как да го обучат.

Когато определя как да функционира решението за изкуствен интелект, администраторът трябва да разполага с точни данни, за да постигне прецизни резултати. Следователно, администраторът

[39] Вж. съображение 65.

трябва да е сигурен, че данните, които се използват за обучение на решението за изкуствен интелект, са точни.

При условие че разполага с валидно правно основание за обучение на решението въз основа на личните данни на голяма група от клиентите на дружеството, администраторът избира група клиенти, която е представителна, за да избегне възможни отклонения.

На следващия етап с помощта на съответната система за обработване на данни се събират данните на клиентите, включващи данни за вида на застраховките, като например: здравна застраховка, застраховка на жилище, пътна застраховка и т.н., както и данни от публични регистри, до които администраторът има законосъобразен достъп. Всички данни се псевдонимизират преди прехвърлянето в системата, предназначена за обучение на модела, основан на изкуствен интелект.

За да гарантира, че данните, използвани за обучение за решението за изкуствен интелект, са възможно най-точни, администраторът събира данни само от източници, съдържащи точна и актуална информация.

Застрахователното дружество проверява дали решението за изкуствен интелект е надеждно и дава недискриминационни резултати както по време на неговото разработване, така и при пускането на продукта на пазара. Когато решението за изкуствен интелект е напълно обучено и в експлоатационна готовност, застрахователното дружество използва резултатите, за да подпомага оценките на застрахователните рискове, но без да се осланя изцяло на решението за изкуствен интелект за вземането на решения за сключване на застраховки, освен когато решението се взема на основание на изключенията, предвидени в член 22, параграф 2 от ОРЗД.

Наред с горното застрахователното дружество извършва редовен преглед на резултатите от функционирането на решението за изкуствен интелект, за да обезпечи неговата надеждност и при необходимост да внася изменения в алгоритъма.

Пример 2

Администраторът е здравно заведение, което се стреми да открие методи, позволяващи му да гарантира цялостността и точността на личните данни в регистрите за неговите пациенти.

В случаите, когато две лица са приети в заведението по едно и също време и получават еднакво лечение, съществува риск от грешка, ако единственият параметър за разграничаването им е по име. За да се гарантира точността, администраторът се нуждае от уникален идентификатор за всяко лице и от повече информация, а не само от името на пациента.

Заведението използва няколко системи, съдържащи лична информация на пациенти, и трябва да гарантира, че информацията, свързана с пациентите, е правилна, точна и последователна във всички системи във всеки един момент. Заведението е идентифицирало няколко риска, които могат да възникнат, ако информацията бъде променена в една от системите, но не и в останалите.

Администраторът решава да смекчи риска с помощта на техника за хеширане, която може да се използва за гарантиране на цялостността на данните в дневниците за лечение. Създават се неподлежащи на промяна криптографски времеви печати за записите в дневниците за лечение и пациента, свързан с тях, за да може всяка промяна да бъде отчетена, свързана и проследена, ако е необходимо.

3.7 Ограничение на съхранението

80. Администраторът трябва да гарантира, че личните данни се съхраняват във форма, която позволява идентифицирането на субектите на данните за период не по-дълъг от необходимия за целите, за които се обработват личните данни.[40]
От ключово значение е администраторът да знае точно какви лични данни обработва дружеството и защо. Целта на обработването е основният критерий за това колко дълго ще се съхраняват личните данни.

81. Мерките и гаранциите, чрез които се прилага принципът за ограничение на съхранението, следва да допълват правата и свободите на субектите на данни, и по-специално правото на изтриване и правото на възражение.

82. Ключовите елементи на ограничението на съхранението на етапа на проектирането и по подразбиране могат да включват:
- изтриване и анонимизиране: администраторът следва да разполага с ясни вътрешни процедури и функции за изтриване и/или анонимизиране на данни;
- ефективност на анонимизирането /изтриването: администраторът трябва да се увери, че не е възможно да се идентифицират повторно анонимизираните данни или да се възстановят изтритите данни, като трябва да проведе тестове за проверка дали това е възможно;
- автоматизиране: изтриването на определени лични данни трябва да бъде автоматизирано;
- критерии за съхранение: администраторът трябва да определи какви данни и каква продължителност на съхранение са необходими за постигането на целта;
- обосновка: администраторът трябва да може да обоснове защо периода на съхранение е необходим за постигането на целта и за съответните лични данни, както и да може да разкрие обосновката и правните основания за определения период на запазване;
- прилагане на политиките за запазване: администраторът трябва да прилага вътрешни политики за запазване на данни и да провежда тестове, за да провери дали организацията ги изпълнява на практика;
- резервни копия/регистрационни файлове: администраторите трябва да определят личните данни и периодите на съхранение по отношение на резервните копия и регистрационните файлове;
- поток от данни: администраторите трябва да познават потока от лични данни и съхранението на копия на тези данни, като се стремят да ограничават тяхното „временно“ съхранение.

Пример

Администраторът събира лични данни, като целта на обработването е администриране на членство на субекта на данни. Личните данни подлежат на изтриване при прекратяване на членството и липса на правно основание за по-нататъшно съхранение на данните.

Администраторът първо изготвя вътрешна процедура за запазване и изтриване на данни. Съгласно тази процедура служителите трябва да изтрият ръчно личните данни след изтичането

[40] Член 5, параграф 1, буква в) от ОРЗД.

на периода на запазване. Служителят спазва процедурата, предвиждаща редовно изтриване и коригиране на данни от всички устройства, от резервни копия, регистрационни файлове, електронни писма и други подходящи носители за съхранение.

За да направи изтриването по-ефективно и защитено от грешки, администраторът решава да внедри автоматична система, обезпечаваща автоматично, надеждно и редовно изтриване на данните. Системата е конфигурирана да следва съответната процедура за изтриване на данни, която се изпълнява през предварително определени редовни интервали с цел премахване на лични данни от всички носители за съхранение на дружеството. Администраторът проверява и тества редовно процедурата за запазване, като осигурява нейното съответствие с актуализираната политика за запазване на данни.

3.8 Цялостност и поверителност

83. Принципът на цялостност и поверителност включва защита от неразрешено или незаконосъобразно обработване и случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. За обезпечаване на сигурността на личните данни са необходими подходящи мерки за предотвратяване и управление на нарушения на сигурността на данните, гарантиране на правилното изпълнение на задачите за обработване на данните и осигуряване на съответствието с други принципи, и за улесняване на ефективното упражняване на правата на физическите лица.

84. В съображение 78 е посочено, че една от мерките за ЗДЕПП може да се състои от осигуряване на възможност за администратора *„да създава и подобрява елементите на сигурността“*. Наред с други мерки за ЗДЕПП, със съображение 78 се въвежда задължение за администраторите да извършват текущо оценка дали използват подходящите средства за обработване във всеки момент и дали избраните мерки реално противодействат на съществуващите слаби места. Освен това администраторите следва да извършват редовни прегледи на мерките за сигурност на информацията, които са свързани и защитават личните данни, както и на процедурите за справяне с нарушения на сигурността на данните.

85. Ключовите елементи за цялостност и поверителност на етапа на проектирането и по подразбиране могат да включват:
    - система за управление на сигурността на информацията (СУСИ): наличие на оперативно средство за управление на политики и процедури за сигурност на информацията;
    - анализ на риска: оценка на рисковете за сигурността на личните данни посредством отчитане на въздействието върху правата на физическите лица и предприемане на мерки за противодействие на идентифицираните рискове; за използване във връзка с оценката на риска: разработване и поддържане на всеобхватно, систематично и реалистично „моделиране на заплахите“ и анализ за устойчивост на атаки на разработения софтуер с цел ограничаване на елементите и възможностите за атаки, насочени към използване на слаби и уязвими елементи;
    - сигурност на етапа на проектирането: вземане предвид на изискванията за сигурност на възможно най-ранен етап в процеса на проектиране и разработване на системата, и текущо интегриране, и изпълнение на съответни тестове;
    - поддръжка: редовен преглед и тестване на софтуера, хардуера, системите и услугите, и др., с цел откриване на уязвими елементи на системите, обезпечаващи дейността по обработване;

- управление на контрола на достъпа: само оправомощените служители, които се нуждаят от достъп, следва да имат достъп до личните данни, необходими за изпълнението на техните служебни задачи по обработване, а администраторът трябва да разграничава нивата на разрешен достъп на отделните служители;
    - ограничение на достъпа (действащи лица): дейността по обработване на данни трябва да се планира и ограничи по такъв начин, че минимален брой лица да се нуждаят от достъп до личните данни, за да могат да изпълняват задълженията си;
    - ограничение на достъпа (съдържание): при всяка операция по обработване достъпът трябва да е ограничен само до атрибутите на отделните набори от данни, които са необходими за изпълнението на съответната операция. Освен това достъпът трябва да е ограничен до данните, отнасящи се до физическите лица, които попадат в обхвата на работата на съответния служител;
    - разделяне на достъпа: дейността по обработване на данни трябва да се планира по такъв начин, че нито едно лице да няма нужда от пълен достъп до всички събрани данни за даден субект на данни и в още по-голяма степен до всички лични данни за определена категория субектите на данни;
- защитени прехвърляния: прехвърлянията трябва да бъдат защитени от неразрешен и случаен достъп и промени;
- сигурно съхранение: съхраняваните данни трябва да бъдат защитени от неразрешен достъп и промени. Следва да са налице процедури за оценка на риска, свързан с централизираното или децентрализираното съхранение, и за кои категории лични данни се отнася този риск. По отношение на някои данни може да са необходими допълнителни мерки за сигурност или тези данни да бъдат изолирани от други данни;
- псевдонимизиране: личните данни и резервните копия/регистрационните файлове трябва да бъдат псевдонимизирани като мярка за сигурност, за да се сведе до минимум рискът от потенциални нарушения на сигурността на данните, например посредством хеширане или криптиране;
- резервни копия/регистрационни файлове: съхранение на резервни копия и регистрационни файлове, доколкото това е необходимо за обезпечаване на сигурността на информацията, използване на информацията за извършени проверки и мониторинг на събития като рутинна мярка за контрол на сигурността. Тези копия следва да бъдат защитени от неразрешен или случаен достъп и промени, да подлежат на редовен преглед и да се предприемат необходимите мерки в случаи на инциденти;
- възстановяване на дейността при бедствие/непрекъснатост на дейността: предприемане на мерки в отговор на изискванията за възстановяване на информационните системи при бедствие и осигуряване на непрекъснатостта на дейността с цел възстановяване на достъпността на личните данни след тежки инциденти;
- защита съобразно нивото на риск: всички категории лични данни следва да бъдат защитени с мерки, които са подходящи с оглед на риска от нарушение на сигурността. Данните, които са съпроводени с особен риск, следва при възможност да се съхраняват отделно от останалите лични данни;
- управление на реакцията при инциденти, свързани със сигурността: наличие на протоколи, процедури и ресурси за откриване, ограничаване, преодоляване, докладване и извличане на поуки от нарушенията на сигурността на данните;
- управление на инциденти: администраторът следва да има въведени процедури за действие в случаи на нарушения и инциденти, свързани със сигурността, с цел постигане на по-устойчива системата за обработване. Това включва процедури за уведомяване,

като например за управление на уведомяването (пред надзорния орган) и предоставянето на информация (на субектите на данни).

Пример

Администратор на данни желае да извлече големи обеми лични данни от медицинска база данни, съдържаща електронни (пациентски) здравни досиета, които да прехвърли в специален сървър с база данни в помещение на дружеството, за да може да извърши обработване на извлечените данни за целите на дейността по осигуряване на качеството. Дружеството е оценило риска от насочване на извлечените данни към сървър, който е достъпен за всичките му служители, като висок по отношение на правата и свободите на субектите на данни. Тъй като само едно звено в дружеството се нуждае да извърши обработване на извлеченията от данните на пациентите, администраторът решава да ограничи достъпа до специалния сървър само за служителите на това звено. Освен това, данните ще бъдат псевдонимизирани преди прехвърлянето им с цел допълнително намаляване на риска.

За да регулира достъпа и да намали евентуалните щети от зловреден софтуер, дружеството решава да отдели мрежата и да въведе мерки за контрол на достъпа до сървъра. Освен това дружеството въвежда мониторинг на сигурността и внедрява система за откриване и предотвратяване на прониквания, а също така изолира сървъра от ежедневна употреба. Въведена е автоматизирана одитна система за наблюдение на достъпа и промените. Тази система генерира отчети и автоматизирани сигнали, когато се конфигурират определени събития, свързани с употребата. Администраторът ще гарантира, че потребителите имат достъп при необходимост и с подходящо ниво на достъп. Неправилната употреба се установява бързо и лесно.

Някои от извлеченията трябва да се сравняват с новите версии, поради което трябва да се съхраняват за срок от три месеца. Администраторът взема решение да запише тези извлечения в отделни бази данни на същия сървър и да приложи както прозрачно криптиране, така и криптиране на колоните при записването на данните. Ключовете за декриптиране на данните в колоните са съхранени в специални модули за сигурност, които могат да се използват само от упълномощени служители, но не могат да се извличат.

Мерките за подготовка за справяне с бъдещи инциденти повишава устойчивостта и надеждността на системата. Администраторът на данни стига до заключението, че превантивни и ефективни мерки и гаранции трябва да бъдат интегрирани във всички предприемани действия за обработване на лични данни сега, и в бъдеще, и че това може да помогне да се предотвратят бъдещи нарушения на сигурността на данните.

Администраторът определя тези мерки за сигурност, както за да гарантира точността, цялостността и поверителността, така и за да предотврати разпространението на зловреден софтуер чрез кибератаки и да направи решението устойчиво. Наличието на надеждни мерки за сигурност способства за изграждане на доверие със субектите на данни.

3.9 Отчетност[41]

86. Съгласно принципа за отчетност администраторът следва да носи отговорност и да може да докаже спазването на всички посочени по-горе принципи.

[41] Вж. съображение 74, съдържащо изискване към администраторите да докажат ефективността на предприетите от тях мерки.

87. Администраторът трябва да е в състояние да докаже съответствие с принципите. За тази цел администраторът може да докаже резултатността на предприетите мерки за защита на правата на субектите на данни и защо счита, че мерките са подходящи и ефективни. Той може например да покаже причината, поради която дадена мярка е подходяща за ефективното спазването на принципа за ограничение на съхранението.

88. Администраторът следва да притежава необходимите знания и умения за прилагане на защита на данните, за да може да осъществява отговорно обработване на лични данни. Това предполага, че администраторът следва да разбира своите задължения във връзка със защитата на данните, произтичащи от ОРЗД, както и да има капацитет да изпълнява тези задължения.

4 ЧЛЕН 25, ПАРАГРАФ 3, СЕРТИФИЦИРАНЕ

89. Съгласно член 25, параграф 3 сертифицирането на защитата на данните на етапа на проектирането по член 42 може да се използва като елемент за доказване на съответствие със ЗДЕПП. И обратно, документи, доказващи съответствие със ЗДЕПП, може да се използват в процеса на сертифициране. Това означава, че когато дадена операция по обработване, осъществявана от администратор или обработващ данни, е сертифицирана в съответствие с член 42, надзорните органи вземат това предвид в своята оценка на спазването на ОРЗД, по-специално по отношение на ЗДЕПП.

90. Когато операция по обработване, осъществявана от администратор или от обработващ данни, е сертифицирана в съответствие с член 42, елементите които допринасят за доказването на съответствие с изискванията на член 25, параграфи 1 и 2, са процесите, свързани с проектиране, т.е. определяне на средствата за осъществяване на обработването, управленските и техническите, и организационни мерки, предприети с цел прилагане на принципите на защита на данните. Критериите за сертифициране на защитата на данните се определят от сертифициращите органи или от собствениците на схемите за сертифициране, след което се одобряват от компетентния надзорен орган или от ЕКЗД. Повече информация относно механизмите за сертифициране може да бъде намерена в издаденото от ЕКЗД Ръководство по сертифициране[42] и други документи в тази област, публикувани на уебсайта на ЕКЗД.

91. Дори в случаите, когато дадена операция по обработване бъде сертифицирана в съответствие с член 42, администраторът остава задължен да наблюдава и подобрява текущо съответствието съгласно критериите за ЗДЕПП, предвидени в член 25.

5 ПРИЛАГАНЕ НА ЧЛЕН 25 И ПОСЛЕДИЦИ

92. Надзорните органи могат да оценяват съответствието с изискванията по член 25 въз основа на процедурите, посочени в член 58. Корективните правомощия са посочени в член 58, параграф 2 и включват отправяне на предупреждения, официални предупреждения, разпореждания за спазване на правата на субектите на данни, ограничения или забрани за обработване, административни глоби и т.н.

[42] ЕКЗД. „Насоки № 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламента“. Версия 3.0, 4 юни 2019 г. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_bg.pdf

93. Наред с това ЗДЕПП е фактор за определяне на нивото на паричните санкции за нарушения на ОРЗД, вж. член 83, параграф 4.[43] [44]

6 ПРЕПОРЪКИ

94. Макар че не са пряко посочени в член 25, обработващите лични данни и производителите също се приемат за ключови лица по отношение на ЗДЕПП и те следва да разбират, че администраторите са задължени да извършват обработване на лични данни само посредством системи и технологии, които имат вградени мерки за защита на данните.

95. Когато извършват обработване от името на администраторите или предлагат решения на администраторите, обработващите лични данни и производителите следва да използват своя експертен капацитет, за да изграждат доверие и да насочват клиентите си, включително МСП, при проектирането/възлагането на решения, които включват мерки за защита на данните в процеса на обработване. Това на свой ред означава, че проектирането на продукти и услуги следва да улеснява изпълнението на задълженията на администраторите.

96. При прилагането на член 25 трябва да се има предвид, че основната цел на проектирането е *ефективното въвеждане* на принципите и *защита* на правата на субектите на данни в подходящите мерки, които следва да се предприемат при обработване. С цел улесняване и подпомагане на процеса на въвеждане на ЗДЕПП, отправяме следните препоръки към администраторите, производителите и обработващите лични данни:
    - Администраторите следва да помислят върху аспектите на защитата на данните още в *началните етапи* от планирането на операциите по обработване, дори преди момента на определяне на средствата за обработване.
    - В случаите, когато администраторът има назначено длъжностно лице по защита на данните (ДЛЗД), ЕКЗД насърчава активното участие на ДЛЗД в интегрирането на ЗДЕПП в процедурите за обществени поръчки и разработване, както и във всички етапи на цикъла на обработване.
    - Операциите по обработване могат да бъдат *сертифицирани*. Възможността за сертифициране на дадена операция по обработване създава добавена стойност за администратора в процеса на избор на софтуер, хардуер, услуги и/или системи за обработване, предлагани от производители или обработващи лични данни. Следователно, производителите следва да стремят да докажат изпълнението на изискванията за ЗДЕПП в рамките на техния цикъл на разработване на решение за обработване. Наличието на маркировка за сертифициране може също така да ориентира избора на субектите на данни между различни стоки и услуги. Възможността за сертифициране на дейността по обработване може да служи като конкурентно предимство за производителите, обработващите лични данни и администраторите и дори може да повиши доверието на субектите на данни в процеса на обработване на техните лични данни. Когато не се предлага възможност за сертифициране,

[43] В член 83, параграф 2, буква г) от ОРЗД е предвидено, че при определяне на налагането на глоби за нарушения на ОРЗД *„надлежно“ се разглеждат „степента на отговорност на администратора или обработващия лични данни, като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с членове 25 и 32“.*

[44] Повече информация за глобите може да бъде намерена в публикацията на Работна група по член 29, „Насоки за прилагане и определяне на административни глоби за целите на Регламент 2016/679“. РД 253, 3 октомври 2017 г. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 — одобрени от ЕКЗД.

администраторите трябва да се стремят да предоставят други *гаранции*, че производителите или обработващите лични данни спазват изискванията за ЗДЕПП.

- Администраторите, обработващите лични данни и производителите следва да изпълняват своите задължения да предоставят на деца до 18-годишна възраст и членове на други уязвими групи специална защита в съответствие със ЗДЕПП.
- Производителите и обработващите лични данни следва да се стремят да улесняват прилагането на ЗДЕПП, за да подпомагат изпълнението от администратора на задълженията по член 25. Администраторите, от друга страна, не следва да избират производители или обработващи лични данни, които не предлагат системи, даващи възможност на администратора да спазва изискванията на член 25, тъй като администраторите ще носят отговорност за неприлагането на тези разпоредби.
- Производителите и обработващите лични данни трябва да играят активна роля в усилията за гарантиране на спазването на критериите за „достижения на техническия прогрес“ и да уведомяват администраторите за всички промени в „достиженията на техническия прогрес“, които могат да повлияят на ефективността на установените мерки. Администраторите трябва да включват това изискване като договорна клауза, за да са сигурни, че се изпълнява.
- ЕКЗД препоръчва на администраторите да изискват от производителите и обработващите лични данни да демонстрират как предлаганият от тях хардуер, софтуер, услуги или системи дават възможност на администратора да изпълнява изискванията за отчетност в съответствие със ЗДЕПП, например, като използват ключови показатели за ефективност, за да докажат ефективността на мерките и гаранциите за прилагане на принципите, и правата.
- ЕКЗД изтъква необходимостта от хармонизиран подход за ефективно прилагане на принципите и правата и насърчава сдруженията или органите, изготвящи кодекси за поведение в съответствие с член 40, да включват, и секторни насоки за ЗДЕПП.
- Администраторите трябва да действат добросъвестно по отношение на субектите на данни и прозрачно по отношение на начина, по който оценяват, и доказват ефективното прилагане на ЗДЕПП, по същия начин, по който показват спазването на ОРЗД съгласно принципа за отчетност.
- Технологиите за подобряване на защитата на личния живот, които са достигнали ниво на технологична зрялост, могат да се прилагат, ако е уместно, като мярка в съответствие с изискванията за ЗДЕПП, в рамките на подход, основан на риска. Технологиите за подобряване на защитата на личния живот от своя страна не изпълняват непременно задълженията по член 25. Администраторите следва да оценяват дали дадена мярка е подходяща и ефективна по отношение на прилагането на принципите на защита на данните и правата на субектите на данни.
- По отношение на заварените системи се прилагат същите задълженията за ЗДЕПП, както към новите системи. Когато заварени системи не отговарят на задълженията за ЗДЕПП и не е възможно да бъдат внесени изменения, обезпечаващи тяхното съответствие със задълженията, се приема, че съответната заварена система не отговаря на задълженията по ОРЗД и не може да се използва за обработване на лични данни.
- Член 25 не предвижда по-нисък праг за изпълнение на изискванията за МСП. Изпълнението на следните препоръки може да улесни МСП в постигането на съответствие с член 25:

- Извършвайте оценка на риска на ранен етап;
- Започнете с обработване в малък мащаб, като на по-късен етап можете да разширите обхвата и да повишите сложността на дейността;
- Изисквайте гаранции от производителите и обработващите лични данни за ЗДЕПП, като например сертифициране и спазване на кодекси за поведение;
- Работете с партньори, които имат доказани добри резултати в тази област;
- Свързвайте се с органите за защита на данните (ОЗД);
- Четете указанията на ОЗД и ЕКЗД;
- Спазвайте кодексите за поведение, когато са налице такива;
- Търсете професионална помощ и консултации.

За Европейския комитет по защита на данните

Председател

(Andrea Jelinek)