| ЧЛЕН 29  РАБОТНА ГРУПА ЗА ЗАЩИТА НА ДАННИТЕ      Тази работна група е създадена съгласно член 29 от Директива 95/46 / ЕО. Той е независим европейски консултативен орган относно защитата на личните данни и неприкосновеността на личния живот. Неговите задачи са описани в член 30 от Директива 95/46 / ЕО и член 15 от Директива 2002/58 / ЕО.  Секретариатът се осигурява от дирекция C (Основни права и върховенство на закона) на Европейската комисия, Генерална дирекция "Правосъдие и потребители", Б-1049 Брюксел, Белгия, Служба № MO59 05/35 Уебсайт: http://ec.europa.eu /justice/data-protection/index\_en.htm    16 / BG WP 243 rev.01                    Насоки за длъжностните лица по защита на данните ("ДЗД")      Приет на 13 декември 2016 г.  Последно преработен и приет на 5 април 2017 г  Тази работна група е създадена съгласно член 29 от Директива 95/46 / ЕО. Той е независим европейски консултативен орган относно защитата на личните данни и неприкосновеността на личния живот. Неговите задачи са описани в член 30 от Директива 95/46 / ЕО и член 15 от Директива 2002/58 / ЕО.  Секретариатът се осигурява от дирекция C (Основни права и върховенство на закона) на Европейската комисия, Генерална дирекция "Правосъдие и потребители", Б-1049 Брюксел, Белгия, Служба № MO59 05/35 Уебсайт: http://ec.europa.eu /justice/data-protection/index\_en.htm |  |  |  |
| --- | --- | --- | --- |

РАБОТНА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПО ОТНОШЕНИЕ НА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

създаденa с Директива 95/46 / ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г.,

като взе предвид членове 29 и 30 от него,

като взе предвид своя правилник,

ПРИЕ НАСТОЯЩИТЕ НАСОКИ:

Таблица със съдържание

1 ВЪВЕДЕНИЕ ............................................. .................................................. ........................ 4

2 ОПРЕДЕЛЯНЕ НА ДЗП ...... .................................................. ............................................. 5

2.1. ЗАДЪЛЖИТЕЛНО ОПРЕДЕЛЯНЕ ................................................ ................................ 5

2.1.1 "Публичен орган или орган" .......... .................................................. ......................6

2.1.2 "Основни дейности" ..................................... .................................................. .........7

2.1.3 "Големи мащаби "................................................. ................................................ .. 7

2.1.4 "Редовно и систематично наблюдение" .... ..................................................

2.1.5 Специални категории данни и данни, свързани с наказателни присъди и престъпления ............................................................................................................................. 9

2.2. ДПО НА ПРОЦЕСАРА .............................................. .................................................. …9

2.3. ОПРЕДЕЛЯНЕ НА ЕДИННА ОПОР ЗА НОВИ ОРГАНИЗАЦИИ ………….....10

2.4. ДОСТЪПНОСТ И ЛОКАЛИЗАЦИЯ НА ДЗД ............................................ .......... 11

2.5. ЕКСПЕРТИЗИРАНЕ И УМЕНИЯ НА ДПЛ ............................................ ............... 11

2.6. ПУБЛИКУВАНЕ И СЪОБЩЕНИЕ НА ДЕТАЙЛИТЕ

ЗА КОНТАКТИ НА ДЗП ………………………………………………………………..12

3 ПОЗИЦИЯ НА ДЗП ................. .................................................. .......................................... 13

3.1. УЧАСТИЕ НА ДЗД ВЪВ ВСИЧКИ ВЪПРОСИ, СВЪРЗАНИ С ОПАЗВАНЕТО НА ЛИЧНИТЕ ДАННИ .................................... ............................................................................ 13

3.2. НЕОБХОДИМИ РЕСУРСИ ................................................ ............................................ 14

3.3. ИНСТРУКЦИИ И "ИЗВЪРШВАНЕ НА СЛУЧАИТЕ И ЗАДАЧИТЕ В НЕЗАВИСИМИЯ ФАЙН" ..................................... …………………………………………. 15

3.4. ОТСТРАНЯВАНЕ ИЛИ НАКАЗАНИЕ ЗА ИЗПЪЛНЕНИЕ НА ЗАБОЛЯВАНИЯТА ЗА ДПО ........................................... ............................................................................................... 15

3.5 , КОНФЛИКТ НА ИНТЕРЕСИ ............................................... ........................................ 16

4 ЗАДАЧИ НА ДЗП ......... .................................................. .................................................. 17

4.1. МОНИТОРИНГ НА СЪОТВЕТСТВИЕТО С GDPR ............................................. ..... 17

4.2. РОЛЯТА НА ДЗП В ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ЗА ОПАЗВАНЕ НА ДАННИТЕ ........................................ ....................................................................................... 17

4.3. СЪТРУДНИЧЕСТВО С НАДЗОРНИЯ ОРГАН И КАТО КОНТРОЛЕН ТОЧКИ ....................................... ........................................................................................................... 18

4.4. ПОДХОД, ОСНОВАНИ НА РИСКА .............................................. ...............................18

4.5. РОЛЯТА НА ДЗП В ЗАПИСВАНЕ НА ЗАПИСИ .......................................... ………..19

5 ПРИЛОЖЕНИЕ - УКАЗАНИЯ ЗА ДЗП: КАКВО ТРЯБВА ДА ЗНАЕТЕ ОПРЕДЕЛЯНЕ НА ДЗД ........................................... .................................................. ...................................... 20

1 КОИТО ТРЯБВА ДА ОТГОВАРЯТ ОРГАНИЗАЦИИТЕ НАПРАВИТЕ ДПО? ………20

2 КАКВО ПОСОЧВА "ОСНОВНИТЕ ДЕЙНОСТИ"? .................................................. ......20

3 КАКВО ПОКАЗВА "ГОЛЯМ ОБРАЗЕЦ"? .................................................. .................... 21

4 КАКВО МОЖЕ ДА "ПОДГОТВЯНЕ НА ПОДГОТОВКА И СИСТЕМА"? .................. 21

5 МОМИТЕ ОРГАНИЗАЦИИ МОГАТ ДА ОПРЕДЕЛЯТ СЪВМЕСТНО ДПО? АКО ИМАТ, КАКТО УСЛОВИЯ? .................................................. ..... …………………………………...22

6 Къде трябва да бъде разположено DPO? .................................................. ......................... 22

7 МОЖЕ ЛИ ДА НАПОМНЯ ВЪНШЕН ДЗД? ..................................................

8 КАКВИ СА ПРОФЕСИОНАЛНИТЕ КАЧЕСТВА, КОИТО ТРЯБВА ДА БЪДАТ ДПО? .................................................. ............... ……………………………………………………….23

ПОЗИЦИЯ НА ДЗП ........................... .................................................. ………………………23

9 КАКВИ РЕСУРСИ МОГАТ ДА БЪДАТ ПРЕДОСТАВЕНИ НА ДПЛ ОТ КОНТРОЛЯРА ИЛИ ОТ ПРОЦЕСУВАНИЯТА? ................................................................. ………………….23

10 КАКВИ СА ЗАГУБИТЕ, КОИТО ДАВАТ ДА БЪДАТ ДЕЙСТВИЕ НА ДЗП, ЗА ДА ИЗПЪЛНЯТ НЕГО / НЕГОВИТЕ ЗАДАЧИ В НЕЗАВИСИМИЯ ФАЙН? КАКВО МОЖЕ ДА БЪДЕ "СМЪРТ ЗА ИНТЕРЕС"? .................................................. ..............................................24

ЗАДАЧИ НА ДЗП ....................... .................................................. ........................................... 24

11 КАКВО МОЖЕ ДА "МОНИТОРИНГ НА СЪОТВЕТСТВИЕ"? ....................................... 24

12 ДЕЙСТВИТЕЛСТВОТО НА ДЗП Е ЛИЧНО ОТГОВОРЕН ЗА НЕСЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА ЗА ЗАЩИТА НА ДАННИТЕ? .................................................................. 24

13 КАКВО Е РОЛЯТА НА ДЗП ПО ОТНОШЕНИЕ НА ОПАЗВАНЕТО НА ДАННИТЕ ОЦЕНКИ НА ВЪЗДЕЙСТВИЕТО И ДОКЛАДИ ЗА ПРОИЗВОДСТВЕНИ ДЕЙНОСТИ? .................................................. .................................................. .................................................. 25

1 Въведение

Общият регламент за защита на данните ("GDPR") [[1]](#footnote-1), който трябва да влезе в сила на 25 май 2018 г., предвижда модернизирана основаваща се на отчетност рамка за съответствие за защита на данните в Европа. Длъжностните лица по защита на данните (ДЗД) ще бъдат в центъра на тази нова правна рамка за много организации, улесняващи спазването на разпоредбите на ГДРП.

Съгласно GDPR, някои контролиращи и преработватели трябва задължително да определят ДЗП.[[2]](#footnote-2) Това ще бъде случаят за всички публични органи и органи (независимо от това какви данни обработват) и за други организации, които - като основна дейност - наблюдават лицата систематично и в голям мащаб или обработват специални категории лични данни в голям мащаб.

Дори когато GDPR не изисква специално назначаването на ДЗД, организациите понякога могат да сметнат за полезно да посочат ДЗД на доброволна основа. Работната група по защита на данните по член 29 ("WP29") насърчава тези доброволни усилия.

Концепцията за ДЗД не е нова. Макар че Директива 95/46 / ЕО[[3]](#footnote-3) не изискваше нито една организация да назначи ДЗД, практиката за назначаване на ДЗД все пак се разви в няколко държави-членки през годините.

Преди приемането на ГДРП чл.29 твърди, че ДЗД е крайъгълен камък на отчетността и че назначаването на ДЗД може да улесни спазването и освен това да се превърне в конкурентно предимство за предприятията.[[4]](#footnote-4) В допълнение към улесняването на спазването чрез прилагане на инструменти за отчетност като улесняване на оценките на въздействието за защита на данните и извършването или улесняването на одити), ДЗД действат като посредници между съответните заинтересовани страни (например надзорни органи, субекти на данни и бизнес единици в рамките на една организация).

ДЗД не носят лична отговорност в случай на неспазване на GDPR. GDPR изяснява, че администраторът или преработвателят е длъжен да осигури и да докаже, че обработката се извършва в съответствие с нейните разпоредби (член 24, параграф 1). Зачитането на защитата на данните е отговорност на администратора или на процесора.

 Контролерът или процесорът също играе решаваща роля за ефективното изпълнение на задачите на ДЗД. Определянето на ДЗД е първа стъпка, но длъжностните лица по защита на данните също трябва да получат достатъчна автономност и ресурси, за да изпълняват ефективно своите задачи.

GDPR разпознава ДЗД като ключов играч в новата система за управление на данни и определя условията за неговото назначаване, длъжност и задачи. Целта на тези насоки е да се изяснят съответните разпоредби в ГДРП, за да се помогне на администраторите и преработвателите да се съобразят със закона, но и да подпомогнат длъжностните лица по защита на данните в тяхната роля. Насоките също така предлагат препоръки за най-добри практики, които се основават на опита, придобит в някои държави-членки на ЕС. Работната група 29 ще следи за изпълнението на тези насоки и може да ги допълни, ако е уместно, с допълнителни подробности.

2 Определяне на DPO

2.1. Задължително обозначаване

Член 37, параграф 1 от ГСРД изисква определянето на ДЗД в три конкретни случая[[5]](#footnote-5):

а) когато обработката се извършва от публичен орган или орган[[6]](#footnote-6);

б) когато основните дейности на администратора или преработвателя се състоят от операции по обработка, които изискват редовен и систематичен мониторинг на субектите на данни в голям мащаб; или

в) когато основните дейности на администратора или преработвателя се състоят в обработка на голям брой специални категории данни[[7]](#footnote-7) или [[8]](#footnote-8) лични данни, свързани с осъдителни присъди и престъпления.[[9]](#footnote-9)

В следващите подраздели WP29 дава насоки по отношение на критериите и терминологията, използвани в член 37, параграф 1.

Освен ако не е очевидно, че дадена организация не е длъжна да определи ДЗД, WP29 препоръчва администраторите и преработвателите да документират вътрешния анализ, извършен, за да се определи дали да бъде назначен ДЗД, за да може да докаже, факторите са взети под внимание[[10]](#footnote-10). Този анализ е част от документацията по принципа на отчетност. Тя може да се изисква от надзорния орган и да се актуализира, когато е необходимо, например ако администраторите или преработвателите предприемат нови дейности или предоставят нови услуги, които могат да попаднат в случаите, изброени в член 37, параграф 1.

Когато дадена организация определи ДЗД на доброволна основа, изискванията по членове от 37 до 39 ще се прилагат към неговото или нейното назначаване, длъжност и задачи, сякаш определянето е било задължително.

Нищо не възпрепятства дадена организация, която не е задължена по закон да посочи ДЗД и не желае доброволно да определи ДЗД, за да наеме персонал или външни консултанти със задачи, свързани със защитата на личните данни. В този случай е важно да се гарантира, че няма объркване относно титлата, статута, длъжността и задачите им. Поради това във всяко съобщение в компанията, както и с органите за защита на данните, субектите на данни и широката общественост трябва да бъде ясно, че заглавието на това лице или консултант не е служител по защита на данните.[[11]](#footnote-11)

ДЗД, независимо дали е задължително или доброволно, е предназначен за всички операции по преработка, извършвани от администратора или преработвателя.

2.1.1 "ПУБЛИЧЕН ОРГАН ИЛИ ОРГАН"

GDPR не определя какво представлява "публичен орган или орган". Работната група 29 счита, че подобно понятие трябва да бъде определено съгласно националното законодателство. Съответно, държавните органи и органи включват национални, регионални и местни органи, но понятието, съгласно приложимото национално законодателство, обикновено включва и редица други публичноправни органи.[[12]](#footnote-12) В такива случаи определянето на ДЗД е задължително.

Може да се изпълни публична задача и публична власт може да бъде упражнявана[[13]](#footnote-13) не само от публични органи или органи, но и от други физически или юридически лица, регулирани от публичното или частното право, в сектори като, съгласно националното законодателство на всяка държава-членка, обществените транспортни услуги, водоснабдяването и енергийните доставки, пътната инфраструктура, общественото радиоразпръскване, обществените жилища или дисциплинарните органи за регулираните професии.

В тези случаи субектите на данни могат да се намират в много близко положение, когато данните им се обработват от публичен орган или орган. По-специално, данните могат да бъдат обработвани за сходни цели и хората често имат твърде малко или никакъв избор относно това дали и как ще бъдат обработени техните данни и по този начин могат да изискват допълнителната защита, която може да донесе обозначаването на ДЗД.

Въпреки че в такива случаи няма задължение, РП29 препоръчва като добра практика частните организации, които изпълняват обществени задачи или упражняват публична власт, да определят ДЗД. Тази дейност на ДЗД обхваща всички извършени операции по обработка, включително тези, които не са свързани с изпълнението на обществена задача или упражняване на служебно задължение (например управление на база данни за служителите).

2.1.2 "ОСНОВНИ ДЕЙНОСТИ"

Член 37, параграф 1, букви б) и в) от ГСРП се отнася до "основните дейности на администратора или преработвателя". В съображение 97 се посочва, че основните дейности на администратора се отнасят до "основни дейности и не са свързани с обработката на лични данни като спомагателни дейности". "Основните дейности" могат да се разглеждат като ключови операции, необходими за постигане на целите на контролера или процесора.

Въпреки това "основни дейности" не следва да се тълкуват като изключващи дейности, при които обработването на данни представлява неразделна част от дейността на администратора или преработвателя. Например основната дейност на болницата е да осигурява здравни грижи. Болницата обаче не може да осигури безопасно и ефективно здравеопазване без да обработва данни за здравето, като здравни досиета на пациентите. Поради това обработването на тези данни трябва да се счита за една от основните дейности на болницата, поради което болниците трябва да определят ДЗД.

Като друг пример, частна охранителна фирма извършва наблюдение на редица частни търговски центрове и обществени пространства. Наблюдението е основната дейност на компанията, която от своя страна е неразривно свързана с обработката на лични данни. Следователно, тази фирма трябва да определи и ДЗД.

От друга страна, всички организации извършват определени дейности, например, като плащат своите служители или имат стандартни дейности по ИТ поддръжка. Това са примери за необходимите функции за подпомагане на основната дейност или основната дейност на организацията. Въпреки че тези дейности са необходими или съществени, те обикновено се разглеждат като спомагателни функции, а не като основна дейност.

2.1.3 "Голяма скала"

Член 37, параграф 1, букви б) и в) изисква обработването на лични данни да се извършва в голям мащаб, за да се задейства определянето на ДЗД. GDPR не определя какво представлява широкомащабна обработка, въпреки че в съображение 91 са дадени някои насоки[[14]](#footnote-14)

Всъщност не е възможно да се даде точен номер нито по отношение на обема на обработваните данни, нито по отношение на броя на засегнатите лица, което би било приложимо във всички ситуации. Това обаче не изключва възможността с течение на времето да се развие стандартна практика за по-специфично и / или количествено определяне на това какво представлява "мащабът" по отношение на някои видове общи преработващи дейности. Работната група 29 също така планира да допринесе за това развитие чрез споделяне и публикуване на примери за съответните прагове за определяне на ДЗД.

Във всеки случай WP29 препоръчва по-конкретно да се обмислят следните фактори

определяне дали обработката се извършва в голям мащаб:

* Броят на засегнатите субекти на данни - като конкретен брой или като процент от съответната популация
* Обемът на данните и / или обема на различните обработвани данни
* Продължителността или продължителността на дейността по обработка на данните
* Географският обхват на обработващата дейност

**Примери** за мащабна обработка включват:

* обработка на данните за пациентите в нормалния ход на бизнес от болница
* обработка на данни за пътуване на лица, използващи система за обществен транспорт в града (напр. Проследяване чрез туристически карти)
* обработка на данни за географско местоположение в реално време на клиенти на международна заведения за бързо хранене верига за статистически цели от специалист, специализиран в предоставянето на тези услуги
* обработка на данни за клиентите в обичайния ход на дейност от застрахователна компания или банка
* обработка на лични данни за поведенческа реклама от търсачка
* обработка на данни (съдържание, трафик , местоположение) от доставчици на телефонни или интернет услуги

**Примери,** които не представляват мащабна обработка, включват:

* обработка на данни за пациентите от отделен лекар
* обработка на лични данни, свързани с осъдителни присъди и престъпления от отделен адвокат

2.1.4 "Редовен и систематичен мониторинг"

Понятието за редовен и систематичен мониторинг на субектите на данни не е определено в ГДРП, но понятието "наблюдение на поведението на субектите на данни" е споменато в съображение 24[[15]](#footnote-15) и ясно включва всички форми на проследяване и профилиране в интернет, включително за целите на поведенческата реклама.

Понятието за мониторинг обаче не се ограничава до онлайн средата и онлайн проследяването следва да се разглежда само като един пример за мониторинг на поведението на субектите на данни.16

WP29 интерпретира **"редовно"** като едно или няколко от следните[[16]](#footnote-16):

* Текущи или възникващи на определени интервали за определен период от време
* Повтарящи се или повтарящи се в определени срокове
* Постоянно или периодично се провежда

WP29 интерпретира "**систематичен"** като един или повече от следните:

* Възникнали по система
* Предварително организирани, организирани или методични
* Предприети като част от общ план за събиране на данни
* Извършени като част от стратегия

Примери за дейности, които могат да представляват редовен и систематичен мониторинг на субектите на данни: експлоатация на телекомуникационна мрежа; предоставяне на телекомуникационни услуги; пренасочване на имейл; маркетингови дейности, базирани на данни; профилиране и оценяване за целите на оценката на риска (например за целите на кредитния скок, установяване на застрахователни премии, предотвратяване на измами, откриване на пране на пари); проследяване на местоположенията, например от мобилни приложения; програми за лоялност; поведенческа реклама; мониторинг на уелнес, фитнес и здравни данни чрез устройства за носене; затворена телевизионна система; свързани устройства, напр. интелигентни измервателни уреди, интелигентни автомобили, автоматизация на дома и др.

2.1.5 СПЕЦИАЛНИ КАТЕГОРИИ ДАННИ И ДАННИ, СВЪРЗАНИ С НАКАЗАНИЯТА И ПРЕСТЪПЛЕНИЯТА

Член 37, параграф 1, буква в) се отнася до обработката на специални категории данни съгласно член 9 и личните данни, свързани с наказателни присъди и престъпления, посочени в член 10. Въпреки че разпоредбата използва думата "и", няма политическа причина, поради която двата критерия трябва да се прилагат едновременно. Следователно текстът трябва да се чете, за да се каже "или".

2.2. DPO на процесора

Член 37 се прилага както за администраторите[[17]](#footnote-17), така и за преработвателите[[18]](#footnote-18) по отношение на определянето на ДЗД. В зависимост от това кой отговаря на критериите за задължително обозначаване, в някои случаи само администраторът или само преработвателят, в други случаи администраторът и неговият преработвател трябва да назначат ДЗД (който след това трябва да си сътрудничи).

Важно е да се подчертае, че дори ако администраторът изпълни критериите за задължително обозначаване, не е задължително преработвателят да назначи ДЗД. Това обаче може да е добра практика.

Примери:

* Малък семеен бизнес, който се занимава с разпространение на домакински уреди в един град, използва услугите на процесора, чиято основна дейност е да предоставя услуги за анализ на уебсайтове и съдействие при целенасочена реклама и маркетинг. Дейностите на семейния бизнес и неговите клиенти не генерират обработка на данни на "широк мащаб", като се има предвид малкият брой клиенти и относително ограничените дейности. Въпреки това, дейностите на преработвателя, които имат много клиенти като това малко предприятие, взети заедно, извършват мащабна обработка. Следователно преработвателят трябва да определи ДЗД съгласно член 37, параграф 1, буква б). В същото време самият семеен бизнес не е задължен да посочи ДЗД.
* Среден производител на керемиди подразделя своите служби по трудова медицина на външен процесор, който има голям брой подобни клиенти. Преработвателят определя ДЗД съгласно член 37, параграф 1, буква в), при условие че обработката е в голям мащаб. Въпреки това, производителят не е задължително да има задължение да посочи ДЗД.

ДЗД, определен от преработвател, наблюдава също така дейностите, извършвани от организацията на процесора, когато действа като администратор на лични данни (например HR, IT, логистика).

2.3. Определяне на един ДЗД за няколко организации

Член 37, параграф 2 позволява на група от предприятия да определят един служител за защита на данните, при условие че той или тя е "лесно достъпен от всяко предприятие". Понятието за достъпност се отнася до задачите на ДЗД като контактна точка по отношение на субектите на данни[[19]](#footnote-19), надзорния орган[[20]](#footnote-20), но също и вътрешно в рамките на организацията, като се има предвид, че една от задачите на ДЗД е "да информира и консултира администратора и преработвателя и служителите, които извършват обработката на задълженията си съгласно настоящия регламент "[[21]](#footnote-21)

За да се гарантира, че ДЗД, вътрешен или външен, е достъпен, е важно да се уверите, че техните данни за контакт са налице в съответствие с изискванията на GDPR.[[22]](#footnote-22)

Той, ако е необходимо, с помощта на екип трябва да е в състояние ефективно да комуникира с субектите на данни[[23]](#footnote-23) и да сътрудничи[[24]](#footnote-24) с съответните надзорни органи. Това също означава, че това съобщение трябва да се осъществява на езика или езиците, използвани от надзорните органи и съответните субекти на данни. Наличието на ДЗД (физически в същите помещения като служителите, чрез гореща линия или други сигурни средства за комуникация) е от съществено значение, за да се гарантира, че субектите на данни ще могат да се свържат с ДЗД.

2.4. Достъпност и локализация на ДЗД

Съгласно раздел 4 от ГДРП достъпността на ДЗД трябва да бъде ефективна.

За да се гарантира, че ДЗД е достъпен, WP29 препоръчва ДЗД да се намира в рамките на Европейския съюз, независимо дали администраторът или преработвателят е установен в Европейския съюз.

Въпреки това не може да се изключи, че в някои ситуации, когато администраторът или преработвателят няма установяване в рамките на Европейския съюз[[25]](#footnote-25), ДЗД може да може да изпълнява своите дейности по-ефективно, ако се намира извън ЕС.

2.5. Експертиза и умения на ДЗД

В член 37, параграф 5 се предвижда, че ДЗД "се определя въз основа на професионални качества и по-специално на експертни познания в областта на правото и практиките за защита на данните и способността да се изпълняват задачите, посочени в член 39". Съображение 97 предвижда, че необходимото ниво на експертни познания следва да се определи в съответствие с извършените операции по обработка на данните и защитата, необходима за обработката на личните данни.

* Ниво на експертиза

Необходимото ниво на експертиза не е строго дефинирано, но трябва да бъде съизмеримо с чувствителността, сложността и количеството данни, които организацията обработва. Например, когато дейността по обработка на данни е особено сложна или когато има голям брой чувствителни данни, ДЗД може да се нуждае от по-високо ниво на експертиза и подкрепа. Съществува и разлика в зависимост от това дали организацията системно прехвърля лични данни извън Европейския съюз или дали такива трансфери са случайни. Поради това ДЗД трябва да бъде внимателно избран, като надлежно се вземат предвид въпросите, свързани със защитата на данните, които възникват в рамките на организацията.

* Професионални качества

Въпреки че член 37, параграф 5 не уточнява професионалните качества, които следва да бъдат взети предвид при определянето на ДЗД, релевантният елемент е, че длъжностните лица по защита на данните трябва да имат опит в националните и европейските закони и практики за защита на данните и задълбочено разбиране на ГДРП. Също така е полезно, ако надзорните органи насърчават подходящо и редовно обучение за длъжностните лица по защита на данните.

Познаването на бизнес сектора и организацията на администратора е полезно. ДЗД трябва също да има добро познаване на извършените операции по обработка, както и на информационните системи, както и на сигурността на данните и нуждите за защита на данните на администратора.

В случай на публичен орган или орган, ДЗД следва да има също така добро познаване на административните правила и процедури на организацията.

* Способност да изпълнява задачите си

Способността да изпълнява задачите, поети от ДЗД, трябва да се тълкува като отнасящи се както до личните им качества и знания, така и до тяхната позиция в организацията. Личните качества трябва да включват например почтеност и висока професионална етика; основната грижа на ДЗД трябва да бъде да позволи спазването на GDPR. ДЗД играе ключова роля в насърчаването на култура на защита на данните в рамките на организацията и помага за осъществяването на съществени елементи от GDPR, като например принципите на обработка на данните[[26]](#footnote-26), правата на субектите на данни[[27]](#footnote-27), защитата на данните по проект и по подразбиране[[28]](#footnote-28), записи на преработвателни дейности [[29]](#footnote-29), сигурност на обработката[[30]](#footnote-30) и уведомяването и съобщаването на нарушенията на данните.[[31]](#footnote-31)

* ДЗД въз основа на договор за услуги

Функцията на ДЗД може да се упражнява и въз основа на договор за услуги, сключен с физическо лице или организация извън организацията на администратора / преработвателя. В последния случай е от съществено значение всеки член на организацията, изпълняващ функциите на ДЗД, да изпълнява всички приложими изисквания на раздел 4 от ГДРП (напр. Е от съществено значение никой да няма конфликт на интереси). Също толкова важно е всеки такъв член да бъде защитен от разпоредбите на GDPR (напр. Не нечестно прекратяване на договора за услуги за дейности като ДЗД, но също и несправедливо уволнение на всеки отделен член на организацията, изпълняващ задачите на ДЗД). В същото време индивидуалните умения и силни страни могат да бъдат комбинирани, така че няколко лица, работещи в екип, да могат по-ефективно да обслужват своите клиенти.

За целите на правната яснота и добрата организация и за предотвратяване на конфликти на интереси за членовете на екипа се препоръчва да има ясно разпределение на задачите в екипа на ДЗД и да се назначи едно лице като водещ контакт и " за всеки клиент. По принцип би било полезно да се посочат тези точки в договора за услуги.

2.6. Публикуване и съобщаване на данните за контакт на ДЗД

Съгласно член 37, параграф 7 от ГПДД администраторът или преработвателят се задължава:

* да публикува данните за връзка с ДЗД и
* да съобщи на съответните надзорни органи данните за контакт на ДЗД.

Целта на тези изисквания е да се гарантира, че субектите на данни (както в организацията, така и извън нея) и надзорните органи могат лесно и пряко да се свържат с ДЗД, без да се налага да се свързват с друга част на организацията. Поверителността е еднакво важна: например, служителите може да не са склонни да се оплачат на ДЗД, ако поверителността на комуникациите им не е гарантирана. ДЗД е обвързан със секретност или поверителност по отношение на изпълнението на неговите задачи в съответствие със законодателството на Съюза или на държавите-членки (член 38, параграф 5).

Данните за връзка с ДЗД трябва да включват информация, която позволява на субектите на данни и надзорните органи да достигнат до ДЗД по лесен начин (пощенски адрес, специален телефонен номер и / или специален електронен адрес). Когато е подходящо, за целите на комуникацията с обществеността биха могли да бъдат осигурени и други средства за комуникация, например специално предназначена гореща линия или специален формуляр за контакт, адресиран до ДЗД на уебсайта на организацията.

Член 37, параграф 7 не изисква публикуваните данни за контакт да съдържат името на ДЗД. Макар че може да е добра практика да се направи това, администраторът, преработвателят и ДЗД трябва да решат дали това е необходимо или полезно при конкретните обстоятелства. [[32]](#footnote-32)

Въпреки това съобщаването на името на ДЗД на надзорния орган е от съществено значение, за да може ДЗД да служи като звено за контакт между организацията и надзорния орган (член 39, параграф 1, буква д).

Като добра практика WP29 също така препоръчва организацията да информира своите служители за името и данните за контакт на ДЗД. Например името и данните за контакт на ДЗП могат да бъдат публикувани вътрешно на интранет на организацията, вътрешна телефонна директория и организационни графики.

3 Позиция на ДЗД

3.1. Участие на ДЗД във всички въпроси, свързани със защитата на личните данни

Член 38 от ГПДП предвижда, че администраторът и преработвателят гарантират, че ДЗД се "участва правилно и своевременно във всички въпроси, свързани със защитата на личните данни".

От решаващо значение е ДЗД или неговият екип да участват възможно най-рано във всички въпроси, свързани със защитата на данните. Във връзка с оценките на въздействието за защита на данните GDPR изрично предвижда ранното участие на ДЗД и уточнява, че администраторът потърси съветите на ДЗД при извършването на такива оценки на въздействието.[[33]](#footnote-33) Гарантиране, че ДЗД е информиран и консултиран от самото начало ще улесни спазването на GDPR, ще насърчи подхода за неприкосновеност на личния живот и следователно трябва да бъде стандартна процедура в рамките на управлението на организацията. Освен това е важно ДЗД да се разглежда като дискусионен партньор в рамките на организацията и да бъде част от съответните работни групи, занимаващи се с дейности по обработка на данни в рамките на организацията.

Следователно организацията трябва да осигури, например, че:

* ДЗД се приканва да участва редовно в срещи на висшето и средното ръководство.
* Неговото / нейното присъствие се препоръчва, когато се вземат решения, свързани със защитата на данните. Цялата релевантна информация трябва да бъде предадена на ДЗД своевременно, за да може той или тя да предостави адекватни съвети.
* В становището на ДЗД винаги трябва да се отдава дължимата тежест. В случай на несъгласие РП29 препоръчва, като добра практика, да се документират причините за неспазване на препоръките на ДЗД.
* ДЗД трябва да бъде консултиран своевременно, след като е настъпило нарушение на данните или друг инцидент.

Където е уместно, администраторът или преработвателят може да разработи указания или програми за защита на данните, които да определят кога трябва да се направи консултация с ДЗД.

3.2. Необходими ресурси

Член 38, параграф 2 от ГДРП изисква от организацията да подкрепя своя ДЗД, като "осигурява необходимите ресурси за изпълнение на [техните] задачи и достъп до лични данни и операции по обработка и да поддържа своите експертни познания". Следва да бъдат разгледани по-специално следните елементи:

* Активна подкрепа на функцията на ДЗД от висшето ръководство (например на ниво управителен съвет).
* Достатъчно време DPO да изпълнява задълженията си. Това е особено важно, когато вътрешен служител по защита на данните се назначава на непълно работно време или когато външният служител по защита на данните извършва защита на данните в допълнение към други задължения. В противен случай противоречивите приоритети могат да доведат до пренебрегване на задълженията на ДЗД. Даването на достатъчно време, за да се посвети на задачите на DPO, е от първостепенно значение. Добра практика е да се установи процент от времето за функцията за ДЗД, когато тя не се изпълнява на пълно работно време. Също така е добра практика да се определи времето, необходимо за изпълнение на задачата, подходящото ниво на приоритетност за задълженията на длъжностните лица по трудови правомощия, а за ДЗД (или организацията) да се изготви работен план.
* Адекватна подкрепа по отношение на финансовите ресурси, инфраструктурата (помещения, съоръжения, оборудване) и персонала, където е уместно.
* Официално уведомяване за определянето на ДЗД на целия персонал, за да се гарантира, че тяхното съществуване и функция са известни в рамките на организацията.
* Необходим достъп до други услуги като човешки ресурси, правни, ИТ, сигурност и т.н., така че ДЗД да могат да получат съществена подкрепа, информация и информация от тези други служби.
* Непрекъснато обучение. На длъжностните лица по защита на данните трябва да бъде дадена възможност да останат актуални относно развитието в областта на защитата на данните. Целта следва да бъде непрекъснато повишаване на нивото на експертиза на ДЗД и те следва да бъдат насърчавани да участват в курсове за обучение по защита на данните и други форми на професионално развитие, като участие в форуми за личен живот, семинари и др.
* Предвид размера и структурата на организацията, може да се наложи да се създаде екип на ДЗД (ДЗД и неговия / нейния персонал). В такива случаи вътрешната структура на екипа и задачите и отговорностите на всеки от неговите членове трябва да бъдат ясно формулирани. По същия начин, когато функцията на ДЗД се упражнява от външен доставчик на услуги, екип от лица, работещи за това лице, може ефективно да изпълнява задачите на ДЗД като екип под отговорността на определен контакт за клиента.

По принцип, колкото по-сложни и / или чувствителни са операциите по обработка, толкова повече ресурси трябва да бъдат предоставени на ДЗД. Функцията за защита на данните трябва да бъде ефективна и достатъчно добре обезпечена във връзка с обработката на данни, която се извършва.

3.3. Инструкции и "изпълнение на задълженията и задачите по независим начин"

Член 38, параграф 3 установява някои основни гаранции, за да гарантира, че длъжностните лица по защита на данните са в състояние да изпълняват задачите си с достатъчна степен на автономност в рамките на своята организация. По-специално, администраторите / преработвателите са длъжни да гарантират, че ДЗД "не получава никакви инструкции относно упражняването на неговите задачи". Съображение 97 добавя, че длъжностните лица, отговарящи за закрила, "независимо дали са служители на администратора или не, да бъде в състояние да изпълнява задълженията и задачите си по независим начин ".

Това означава, че при изпълнение на техните задачи по член 39, длъжностните лица за защита на данните не трябва да бъдат инструктирани как да се занимават с въпрос, например какъв резултат трябва да бъде постигнат, как да разследва жалба или дали да се консултира с надзорния орган. Освен това, те не трябва да бъдат инструктирани да приемат определено мнение за проблем, свързан със закона за защита на данните, например конкретно тълкуване на закона.

Автономията на ДЗД обаче не означава, че те имат правомощия за вземане на решения, които надхвърлят техните задачи съгласно член 39.

Контрольорът или преработвателят остава отговорен за спазването на законодателството за защита на данните и трябва да може да доказва съответствие.[[34]](#footnote-34) Ако администраторът или преработвателят вземат решения, които са несъвместими с препоръките на ГДРП и ДЗД, на ДЗД следва да бъде дадена възможност да направи своето или нейното несъгласие, ясно до най-висшето управленско ниво и до тези, които взимат решенията. В това отношение член 38, параграф 3 предвижда, че ДЗД "докладва директно на най-високото ниво на управление на администратора или преработвателя". Такова директно отчитане гарантира, че висшето ръководство (напр. Бордът на директорите) е наясно с препоръките и препоръките на ДЗД като част от мисията на ДЗД да информира и съветва администратора или преработвателя. Друг пример за директно отчитане е изготвянето на годишен доклад за дейностите на ДЗД, предоставени на най-високо управленско ниво.

3.4. Уволнение или наказание за изпълнение на задачи по DPO

В член 38, параграф 3 се изисква длъжностните лица по защита на данните да не бъдат "отхвърляни или санкционирани от администратора или преработвателя за изпълнение на [техните] задачи".

Това изискване укрепва автономията на ДЗД и помага да се гарантира, че те действат самостоятелно и се ползват с достатъчна защита при изпълнение на задачите си за защита на данните.

Санкциите са забранени само съгласно GDPR, ако се налагат в резултат на това, че ДЗД изпълнява задълженията си като ДЗД. Например ДЗД може да сметне, че определена обработка е вероятно да доведе до висок риск и да посъветва администратора или преработвателя да извърши оценка на въздействието върху защитата на данните, но администраторът или преработвателят не са съгласни с оценката на ДЗД. В такава ситуация ДЗД не може да бъде отхвърлен за предоставянето на този съвет.

Санкциите могат да приемат различни форми и могат да бъдат преки или косвени. Те могат да се състоят например в отсъствие или забавяне на повишението; предотвратяване на професионалното развитие; отричане от обезщетения, които получават други служители. Не е необходимо тези санкции действително да се изпълняват, а само заплахата е достатъчна, стига те да бъдат използвани за санкциониране на ДЗД на основания, свързани с неговите дейности по ДЗД.

Като нормално правило за управление и какъвто би бил случаят с всеки друг служител или изпълнител съгласно и съгласно приложимото национално договорно или трудово и наказателно право, ДЗД би могъл да бъде уволнен законно поради причини, различни от изпълнението на неговите задачи като ДЗД (например, в случай на кражба, физически, психологически или сексуален тормоз или подобно грубо неправомерно поведение).

В този контекст следва да се отбележи, че ГСРП не уточнява как и кога ДЗД може да бъде освободен или заменен от друго лице. Въпреки това, колкото по-стабилен е договорът на ДЗД и колкото повече гаранции съществуват срещу неправомерно уволнение, толкова по-голяма е вероятността те да могат да действат по независим начин. Следователно WP29 би приветствал усилията на организациите в тази насока.

3.5. Конфликт на интереси

Член 38, параграф 6 позволява на длъжностните лица по защита на данните да "изпълняват други задачи и задължения". Той обаче изисква организацията да гарантира, че "такива задачи и задължения не водят до конфликт на интереси".

Липсата на конфликт на интереси е тясно свързана с изискването за действие по независим начин. Въпреки че на ДЗП се разрешава да изпълняват други функции, те могат да бъдат натоварени само с други задачи и задължения, при условие че те не водят до конфликт на интереси. Това по-специално означава, че ДЗД не може да заема позиция в организацията, която го кара да определя целите и средствата за обработка на лични данни. Поради специфичната организационна структура във всяка организация, това трябва да се разглежда поотделно.

Като правило, противоречивите позиции в организацията могат да включват висши ръководни длъжности (като главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, ръководител на отдела по маркетинг, ръководител на отдел "Човешки ресурси" или ръководител на отделите за информационни технологии) ролите са по-ниски в организационната структура, ако тези позиции или роли водят до определяне на целите и средствата за обработка. Освен това може да възникне конфликт на интереси, например, ако от външен служител по защита на данните се изисква да представлява администратора или преработвателя пред съдилищата в случаи, засягащи въпроси, свързани със защитата на данните.

В зависимост от дейностите, размера и структурата на организацията, може да бъде добра практика за администраторите или преработвателите:

 да се определят позициите, които биха били несъвместими с функциите на ДЗД  да се изготвят вътрешни правила за това, за да се избегнат конфликтите на интереси  да се включи по-общо обяснение за конфликтите на интереси  да се обяви, че техният ДЗД няма конфликт на интересите по отношение на неговата функция на ДЗД като начин за повишаване на осведомеността относно това изискване  да включи предпазни мерки във вътрешните правила на организацията и да гарантира, че обявата за свободна длъжност за длъжността на ДЗД или договора за услуги е достатъчно точна и подробно, за да се избегне конфликт на интереси. В този контекст следва също така да се има предвид, че конфликтите на интереси могат да приемат различни форми в зависимост от това дали ДЗД се набират вътрешно или външно

4 Задачи на ДЗД

4.1. Мониторинг на спазването на GDPR

Член 39, параграф 1, буква б) възлага на длъжностните лица по защита на данните, наред с другите задължения, задължението да контролират спазването на ГДРП. В съображение 97 допълнително се уточнява, че ДЗД "следва да съдейства на администратора или на преработвателя да наблюдава вътрешното съответствие с настоящия регламент".

Като част от тези задължения за наблюдение на спазването, ДЗД могат по-специално:

* да събира информация за идентифициране на дейностите по обработката
* да анализира и да проверява съответствието на обработващите дейности
* да информира, съветва и издава препоръки на администратора или процесора

Мониторингът на спазването не означава, че DPO е лично отговорен, когато има несъответствие. ГДРП изяснява, че администраторът, а не ДЗД, трябва да "прилага подходящи технически и организационни мерки, за да гарантира и да може да докаже, че обработката се извършва в съответствие с настоящия регламент" (член 24, параграф 1) ). Зачитането на защитата на данните е корпоративна отговорност на администратора на данни, а не на ДЗД.

4.2. Ролята на ДЗД при оценката на въздействието върху защитата на данните

Съгласно член 35, параграф 1 задача на администратора, а не на ДЗД, е да извърши, при необходимост, оценка на въздействието върху защитата на данните ("DPIA"). Въпреки това, ДЗД може да играе много важна и полезна роля в подпомагането на администратора. В съответствие с принципа за защита на данните от разработката, член 35, параграф 2 конкретно изисква администраторът да "потърси съвет" от ДЗД при извършването на DPIA. Член 39, параграф 1, буква в) на свой ред задължава ДЗД да изпълнява задължението да "предоставя консултации при поискване по отношение на [DPIA] и да следи неговото изпълнение съгласно член 35".

РП29 препоръчва администраторът да потърси съвет от ДЗД по следните въпроси, наред с други [[35]](#footnote-35):

* дали да се извърши DPIA
* каква да бъде методологията, която трябва да се следва при извършване на DPIA
* дали да се извърши вътрешнофирмената оценка на въздействието върху околната среда (DPIA) или дали тя да бъде възложена на външни изпълнители
* какви гаранции (включително технически и организационни мерки) да се прилагат за смекчаване на рисковете на правата и интересите на субектите на данни
* дали оценката на въздействието за защита на данните е била извършена правилно и дали нейните заключения (дали да се извърши или не обработката и какви предпазни мерки да се прилагат) са в съответствие с ГПЧП

Ако администраторът не е съгласен със съветите, предоставени от ДЗД, документацията за DPIA трябва да обоснове конкретно в писмена форма защо не са взети предвид съветите[[36]](#footnote-36).

Работната група 29 освен това препоръчва администраторът да посочи ясно, например в договора за закрила на потребителите, но също така и в информацията, предоставена на служителите, ръководството (и други заинтересовани страни, където е приложимо), точните задачи на ДЗД и техния обхват, по-специално по отношение на извършване на DPIA.

4.3. Сътрудничество с надзорния орган и действащо като звено за контакт

Съгласно член 39, параграф 1, букви г) и д) ДЗД следва да "сътрудничи на надзорния орган" и да "действа като звено за контакт на надзорния орган по въпроси, свързани със обработването, включително предварителната консултация, чл. 36 и да се консултира, по целесъобразност, по отношение на всеки друг въпрос ".

Тези задачи се отнасят до ролята на "посредник" на ДЗД, посочен в уводната част на настоящите насоки. ДЗД действа като звено за контакт, което улеснява достъпа на надзорния орган до документите и информацията за изпълнението на задачите, посочени в член 57, както и за упражняването на своите правомощия за разследване, коригиране, упълномощаване и консултиране, посочени в член 58. Както вече беше споменато, ДЗД е обвързан от тайна или поверителност по отношение на изпълнението на неговите или нейните задачи в съответствие със законодателството на Съюза или на държавите-членки (член 38, параграф 5). Въпреки това задължението за поверителност / поверителност не забранява на ДЗД да се свързва и да търси съвети от надзорния орган. Член 39, параграф 1, буква д) предвижда, че ДЗД може да се консултира с надзорния орган по всеки друг въпрос, когато е уместно.

4.4. Подход, базиран на риска

В член 39, параграф 2 се изисква длъжностното лице за защита на данните "да отчита надлежно риска, свързан с операциите по обработка, като взема предвид естеството, обхвата, контекста и целите на обработката".

Тази статия напомня за общия принцип и принципа на здравия разум, който може да е от значение за много аспекти на ежедневната работа на ДЗД. По същество той изисква от организациите за защита на данните да дават приоритет на своите дейности и да съсредоточат усилията си върху въпроси, които представляват по-високи рискове за защита на данните. Това не означава, че те трябва да пренебрегнат следеността на мониторинга на операциите по обработка на данни, които имат сравнително по-ниско ниво на рискове, но това показва, че те трябва да се съсредоточат главно върху по-рисковите райони.

Този селективен и прагматичен подход трябва да помогне на ДЗД да информират администратора относно методологията, която да се използва при извършване на ПДИ, кои области трябва да подлежат на вътрешен или външен одит за защита на данните, какви вътрешни дейности за обучение да предоставят на персонала или ръководството, , и кои операции за обработка да отделят повече от своето време и ресурси.

4.5. Ролята на ДЗД в воденето на отчети

Съгласно член 30, параграфи 1 и 2, администраторът или преработвателят, а не ДЗД, трябва да "води отчет за операциите по обработка, които са под негова отговорност" или "да води отчет за всички категории преработвателни дейности, които се извършват от името на администратор ".

На практика ДЗД често създават инвентаризации и поддържат регистър на операциите по обработка въз основа на информацията, предоставена им от различните отдели в своята организация, отговарящи за обработката на лични данни. Тази практика е установена в много действащи национални закони и съгласно правилата за защита на данните, приложими за институциите и органите на ЕС.[[37]](#footnote-37)

Член 39, параграф 1 предвижда списък на задачите, които ДЗД трябва да имат като минимум. Следователно нищо не възпрепятства контролера или процесора да възложат на ДЗД задачата да поддържат запис на операциите по обработка под отговорността на контролера или процесора. Такъв запис трябва да се разглежда като един от инструментите, позволяващи на ДЗД да изпълнява задачите си за наблюдение на спазването, информиране и консултиране на администратора или преработвателя.

Във всички случаи регистърът, който се изисква да бъде съхраняван съгласно член 30, следва също да се разглежда като инструмент, който позволява на контролиращия орган и на надзорния орган да получат при поискване преглед на всички дейности по обработка на лични данни, които организацията извършва. Това е предпоставка за спазването и като такава е ефективна мярка за отчетност.

**5 ПРИЛОЖЕНИЕ - УКАЗАНИЯ ЗА ДЗП:** КАКВО ТРЯБВА ДА ЗНАЕТЕ

Целта на това приложение е да отговорите, в опростен и лесен за разглеждане формат, на някои от ключовите въпроси, които организациите могат да имат по отношение на новите изисквания съгласно Общия регламент за защита на данните (GDPR) да назначи ДЗД.

Определяне на ДЗД

1 Кои организации трябва да назначат ДЗД?

Определянето на ДЗД е задължение:

* ако обработката се извършва от публичен орган или орган (независимо от това какви данни се обработват)
* ако основните дейности на администратора или преработвателя се състоят от операции по обработка, които изискват редовно и систематичен мониторинг на субектите на данни в широк мащаб
* ако основните дейности на администратора или преработвателя се състоят в обработка на голям мащаб на специални категории данни или лични данни, свързани с наказателни присъди и престъпления

Имайте предвид, че правото на Съюза или на държавите-членки може да изисква определянето на длъжностни лица по защита на данните и в други ситуации. Накрая, дори ако определянето на ДЗД не е задължително, организациите понякога могат да сметнат за полезно да посочат доброволно ДЗД. Работната група по защита на данните по член 29 ("WP29") насърчава тези доброволни усилия. Когато дадена организация определи ДЗД на доброволна основа, същите изисквания ще се прилагат към нейното назначаване, длъжност и задачи, сякаш определянето е било задължително.

Източник: Член 37, параграф 1 от GDPR

2 Какво означава "основни дейности"?

"Основните дейности" могат да се разглеждат като ключови операции за постигане на целите на администратора или процесора. Те включват и всички дейности, при които обработката на данни представлява неделима част от дейността на администратора или преработвателя. Например, обработването на здравни данни, като например здравните досиета на пациентите, трябва да се разглежда като една от основните дейности на болницата, поради което болниците трябва да определят ДЗД.

От друга страна, всички организации извършват определени спомагателни дейности, като например да плащат на служителите си или да имат стандартни дейности по ИТ поддръжка. Това са примери за необходимите функции за подпомагане на основната дейност или основната дейност на организацията. Въпреки че тези дейности са необходими или съществени, те обикновено се разглеждат като спомагателни функции, а не като основна дейност.

Източник: член 37, параграф 1, букви б) и в) от GDPR

3 Какво означава "голям мащаб"?

GDPR не определя какво представлява мащабна обработка. РП29 препоръчва по-специално да се вземат предвид следните фактори, когато се определя дали обработката се извършва в голям мащаб:

* броя на засегнатите субекти на данни - или като конкретен брой или като процент от съответната популация,
* обема на данните и / или обхвата на различните обработвани данни
* продължителността или постоянството на дейността по обработка на данните
* географския обхват на обработващата дейност

Примери за широкомащабна обработка включват:

* обработка на данни за пациентите в нормалния ход на бизнеса от болница
* обработка на данни за пътувания на лица, използващи градска система за обществен транспорт (напр. Проследяване чрез туристически карти)
* обработка на данни за географско местоположение в реално време от клиенти на международна верига за бързо хранене за статистически цели от специалист, специализиран в тези дейности
* обработка на данни за клиентите в обичайния ход на дейност от застрахователна компания или банка
* обработка на лични данни за поведенческа реклама от търсачка
* обработка на данни (съдържание, трафик, местоположение) от доставчици на телефонни или интернет услуги

Примери, **които не представляват** мащабна обработка, включват:

* обработка на данни за пациентите от отделен лекар;
* обработка на лични данни, свързани с осъдителни присъди и престъпления от отделен адвокат

Източник: член 37, параграф 1, букви б) и в) от GDPR

4 Какво означава "редовен и систематичен мониторинг"?

Понятието за редовен и систематичен мониторинг на субектите на данни не е определено в GDPR, но ясно включва всички форми на проследяване и профилиране в интернет, включително за целите на поведенческата реклама. Понятието за мониторинг обаче не се ограничава до онлайн средата.

Примери за дейности, които могат да представляват редовен и систематичен мониторинг на субектите на данни: експлоатация на телекомуникационна мрежа; предоставяне на телекомуникационни услуги; пренасочване на имейл; маркетингови дейности, базирани на данни; профилиране и оценяване за целите на оценката на риска (например за целите на кредитния скок, установяване на застрахователни премии, предотвратяване на измами, откриване на пране на пари); проследяване на местоположенията, например от мобилни приложения; програми за лоялност; поведенческа реклама; мониторинг на уелнес, фитнес и здравни данни чрез устройства за носене; затворена телевизионна система; свързани устройства, напр. интелигентни измервателни уреди, интелигентни автомобили, автоматизация на дома и др.

WP29 интерпретира "редовно" като едно или няколко от следните:

* продължаващо или възникващо на определени интервали за определен период от време
* повтарящо се или повтарящо се в определени периоди от време
* постоянно или периодично

WP29 интерпретира "систематичен" като един или повече от следните:

* възникващ по система
* предварително организирани, организирани или методически
* извършвани като част от общ план за събиране на данни
* извършвани като част от стратегия

Източник: член 37, параграф 1, буква б) от ГДРП

5 Могат ли организациите да назначат съвместно ДЗД?

Ако е така, при какви условия? Да. Група предприятия може да определи един ДЗД, при условие че той е "леснодостъпен от всяко предприятие". Понятието за достъпност се отнася до задачите на ДЗД като звено за контакт по отношение на субектите на данни, надзорния орган и също вътрешно в рамките на организацията. За да се гарантира, че ДЗД е достъпен, вътрешен или външен, е важно да се уверите, че са налице данните за контакт. ДЗД, ако е необходимо, с помощта на екип, трябва да бъде в състояние да комуникира ефикасно с субектите на данни и да си сътрудничи със съответните надзорни органи. Това означава, че това съобщение трябва да се извършва на езика или езиците, използвани от надзорните органи и съответните субекти на данни. Наличието на ДЗД (физически в същите помещения като служителите, чрез гореща линия или други сигурни средства за комуникация) е от съществено значение, за да се гарантира, че субектите на данни ще могат да се свържат с ДЗД.

Един единствен ДЗД може да бъде определен за няколко държавни органи или органи, като се отчита тяхната организационна структура и размер. Същите съображения по отношение на ресурсите и комуникацията се прилагат. Като се има предвид, че ДЗД отговаря за различни задачи, администраторът или преработвателят трябва да гарантира, че един ДЗД с помощта на екип, ако е необходимо, може да ги изпълнява ефикасно, въпреки че е определен за няколко публични органи и органи.

Източник: член 37, параграфи 2 и 3 от GDPR

6 Къде трябва да се намира ДЗД?

За да се гарантира, че ДЗД е достъпен, WP29 препоръчва ДЗД да се намира в рамките на Европейския съюз, независимо дали администраторът или преработвателят е установен в Европейския съюз. Въпреки това не може да се изключи, че в някои ситуации, когато администраторът или преработвателят няма установяване в рамките на Европейския съюз, ДЗД може да може да изпълнява своите дейности по-ефективно, ако се намира извън ЕС.

7 Възможно ли е да се назначи външен ДЗД?

Да. ДЗД може да бъде член на персонала на администратора или преработвателя (вътрешен ДЗД) или да изпълнява задачите въз основа на договор за услуга. Това означава, че ДЗД може да бъде външен и в този случай неговата / нейната функция може да бъде упражнявана въз основа на договор за услуги, сключен с физическо лице или организация.

Когато функцията на ДЗД се упражнява от външен доставчик на услуги, екип от лица, работещи за това лице, може ефективно да изпълнява задачите на ДЗД като екип под отговорността на определен ръководител и "отговорно лице" на клиента , В този случай е от съществено значение всеки член на външната организация, изпълняващ функциите на ДЗД, да изпълнява всички приложими изисквания на ГДРП.

За целите на правната яснота и добра организация и за предотвратяване на конфликтите на интереси за членовете на екипа, Насоките препоръчват в договора за услуги да има ясно разпределение на задачите в рамките на външния екип на ДЗД и да се определи едно лице като лидер контакт и лице, отговарящо за клиента.

Източник: член 37, параграф 6 от GDPR

8 Какви са професионалните качества, които трябва да притежава ДЗД?

ДЗД се определя въз основа на професионални качества и по-специално на експертни познания в областта на законодателството и практиките за защита на данните и способността да изпълнява своите задачи.

Необходимото ниво на експертни знания следва да се определи в съответствие с извършените операции по обработка на данните и необходимата защита за обработката на личните данни. Например, когато дейността по обработка на данни е особено сложна или когато има голям брой чувствителни данни, ДЗД може да се нуждае от по-високо ниво на експертиза и подкрепа.

Съответните умения и опит включват:

* опит в националните и европейските закони и практики за защита на данните, включително задълбочено разбиране на ГДРП;
* разбиране на извършените операции по обработка;
* разбиране на информационните технологии и сигурността на данните;
* познаване на бизнес сектора и организацията; културата за защита на данните в организацията

Източник: член 37, параграф 5 от GDPR

Позиция на ДЗД

9 Какви ресурси трябва да се предоставят на ДЗД от администратора или от процесора?

ДЗД трябва да разполага с необходимите ресурси, за да може да изпълнява своите задачи.

В зависимост от естеството на операциите по преработка и дейностите и размера на организацията, на ДЗД следва да бъдат предоставени следните ресурси:

* Активна подкрепа за функциите на ДЗД от висшето ръководство
* Време на ДЗД да изпълни задачите си
* Адекватна подкрепа по отношение на финансовите ресурси, инфраструктурата (помещения, съоръжения, оборудване) и персонала, когато е уместно
* Официално уведомяване за определянето на ДЗД целия персонал
* достъп до други услуги в рамките на организацията, така че организациите за закрила на половете да могат да получат съществена подкрепа, принос или информация от тези други услуги
* непрекъснато обучение

Източник: Член 38, параграф 2 от GDPR

10 Какви са гаранциите, които позволяват на ДЗД да изпълнява задачите си по независим начин? Какво означава "конфликт на интереси"?

Има няколко гаранции, за да може ДЗД да действа по независим начин:

* никакви инструкции от страна на администраторите или преработвателите относно упражняването на задачите на ДЗД
* липса на уволнение или наказание от страна на администратора за изпълнението на задачите на ДЗД
* липса на конфликт на интереси с възможни други задачи и задължения

Другите задачи и задължения на ДЗД не трябва да водят до конфликт на интереси. Това означава, от една страна, че ДЗД не може да заема позиция в организацията, която да го накара да определи целите и средствата за обработка на лични данни. Поради специфичната организационна структура във всяка организация, това трябва да се разглежда поотделно.

Като правило, противоречивите позиции в организацията могат да включват висши ръководни длъжности (като главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, ръководител на отдела по маркетинг, ръководител на отдел "Човешки ресурси" или ръководител на отделите за информационни технологии) ролите са по-ниски в организационната структура, ако тези позиции или роли водят до определяне на целите и средствата за обработка. Освен това може да възникне конфликт на интереси, например, ако от външен служител по защита на данните се изисква да представлява администратора или преработвателя пред съдилищата в случаи, засягащи въпроси, свързани със защитата на данните.

Източник: член 38, параграф 3 и член 38, параграф 6 от GDPR

Задачи на ДЗД

11 Какво означава "мониторинг на спазването"?

Като част от тези задължения за наблюдение на спазването, ДЗД могат по-специално:

* да събира информация за идентифициране на дейностите по обработката
* да анализира и да проверява съответствието на обработващите дейности
* да информира, съветва и издава препоръки на администратора или процесора

Източник: член 39, параграф 1, буква б) от ГДРП

12 ДП отговаря лично за неспазването на изискванията за защита на данните?

**Не.** ДЗД не са лично отговорни за неспазването на изискванията за защита на данните. Операторът или преработвателят е длъжен да осигури и да демонстрира тази обработка се извършва в съответствие с настоящия регламент. Зачитането на защитата на данните е отговорност на администратора или преработвателя.

13 Каква е ролята на ДЗД по отношение на оценките на въздействието върху защитата на данните и записите на обработващите дейности?

Що се отнася до оценката на въздействието за защита на данните, администраторът или преработвателят следва да потърси съвет от ДЗД по следните въпроси, наред с другото:

* дали да се извърши оценката на въздействието върху защитата на данните - DPIA
* каква трябва да бъде методологията, която трябва да се спазва при извършване на DPIA
* дали да се извърши вътрешна DPIA или дали тя да се възложи на външни изпълнители
* какви гаранции (включително технически и организационни мерки) да се прилагат за смекчаване на рисковете на правата и интересите на субектите на данни
* дали оценката на въздействието върху защитата на данните е извършена правилно и дали нейните заключения (дали да се продължи обработката и какви предпазни мерки да се прилагат) са в съответствие с изискванията за защита на данните

Що се отнася до регистрите на обработващите дейности, от оператора или от обработващия, а не от ДЗД, се изисква да води отчети за операциите по обработка. Нищо обаче не възпрепятства контролера или процесора да възложат на ДЗД задачата да поддържат записите на операциите по обработка под отговорността на контролера или процесора. Тези записи следва да се разглеждат като един от инструментите, позволяващи на ДЗД да изпълнява задачите си за наблюдение на спазването, информиране и съветване на администратора или на процесора.

Източник: член 39, параграф 1, буква в) и член 30 от ГДРП

Съставено в Брюксел на 13 декември 2016 г.

За работната група председателят

Изабел Фалк-Пиеротин

Последно преработен и приет на 05 април 2017 г.

За работната група Председателят

Изабел Фалк-Пиеротин

1. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни и за отмяна на Директива 95/46 / ЕО (Общ регламент за защита на данните) (ОВ L 119, 4.5.2016 г.). GDPR е от значение за ЕИП и ще се прилага след включването му в Споразумението за ЕИП. [↑](#footnote-ref-1)
2. Назначаването на ДЗД е задължително и за компетентните органи съгласно член 32 от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица по отношение на обработката на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и за свободното движение на такива данни и за отмяна на Рамково решение 2008/977 / ПВР на Съвета (ОВ L 119, 4.5.2016 г. , стр. 89- 131) и национално законодателство за прилагане. Въпреки че тези насоки се съсредоточават върху ДЗД в рамките на ГДРП, указанията също са от значение по отношение на ДЗД съгласно Директива 2016/680 по отношение на техните подобни разпоредби. [↑](#footnote-ref-2)
3. Директива 95/46 / ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни (ОВ L 281, 23.11.1995 г., стр. 1). 31). [↑](#footnote-ref-3)
4. Виж http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150617\_appendix\_core\_issues\_plenary\_en.pdf [↑](#footnote-ref-4)
5. Имайте предвид, че съгласно член 37, параграф 4, правото на Съюза или на държавите-членки може да изисква определянето на длъжностни лица по защита на данните и в други ситуации. [↑](#footnote-ref-5)
6. С изключение на съдилищата, които действат в качеството си на съдебни служители. Виж член 32 от Директива (ЕС) 2016/680 [↑](#footnote-ref-6)
7. Съгласно член 9 те включват лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации и обработка на генетични данни, биометрични данни с цел еднозначно идентифициране на физическо лице, данни относно здравето или данни относно сексуалния живот или сексуалната ориентация на физическо лице [↑](#footnote-ref-7)
8. В член 37, параграф 1, буква в) се използват думите "и". Вижте раздел 2.1.5 по-долу за обяснение относно използването на "или" вместо "и". [↑](#footnote-ref-8)
9. Член 10

   [↑](#footnote-ref-9)
10. Вж. Член 24, параграф 1. [↑](#footnote-ref-10)
11. Това важи и за главните служители за защита на личния живот ("CPO") или други специалисти по защита на личните данни, които вече съществуват днес в някои компании, които не винаги отговарят на критериите за GDPR, например от гледна точка на наличните ресурси или гаранции за независимост. не, те не могат да бъдат разглеждани и посочени като ДЗД. [↑](#footnote-ref-11)
12. Виж напр. определението за "орган на публичния сектор" и "орган, управляван от публичното право" в член 2, параграфи 1 и 2 от Директива 2003/98 / ЕО на Европейския парламент и на Съвета от 17 ноември 2003 г. относно повторната употреба на обществения сектор (ОВ L 345, 31.12.2003 г., стр. 90). [↑](#footnote-ref-12)
13. Член 6, параграф 1, буква д). [↑](#footnote-ref-13)
14. Съгласно съображението "мащабни операции по обработка, които имат за цел да обработват значителни количества лични данни на регионално, национално или наднационално равнище и които биха могли да засегнат голям брой субекти на данни и които вероятно ще доведат до висок риск" да бъдат включени, по-специално. От друга страна съобщението изрично предвижда, че "обработването на лични данни не следва да се разглежда като широкомащабно, ако обработката се отнася до лични данни от пациенти или клиенти от отделен лекар, друг медицински специалист или адвокат". Важно е да се има предвид, че докато в съображението са дадени примери в крайните размери (обработка от отделен лекар срещу обработка на данни за цялата страна или в цяла Европа); между тези крайности има голяма сива зона. Освен това следва да се има предвид, че това съображение се позовава на оценки на въздействието върху защитата на данните. Това означава, че някои елементи може да са специфични за този контекст и не се отнасят задължително до определянето на ДЗД по абсолютно същия начин. [↑](#footnote-ref-14)
15. "За да се определи дали дадена обработваща дейност може да се разглежда като наблюдение на поведението на субектите на данни, следва да се провери дали физическите лица са проследени в интернет, включително потенциална последваща употреба на техники за обработка на лични данни, които се състоят в профилиране на физическо лице, за да взема решения относно нея или за анализиране или предсказване на личните му предпочитания, поведения и нагласи " [↑](#footnote-ref-15)
16. Обърнете внимание, че съображение 24 се съсредоточава върху извънтериториалното прилагане на ГДРП. В допълнение, съществува също така разлика между текста "наблюдение на тяхното поведение" (член 3, параграф 2, буква б)) и "редовен и систематичен мониторинг на субектите на данни" (член 37, параграф 1, буква б)), да се разглежда като различно понятие [↑](#footnote-ref-16)
17. Контрольорът се определя от член 4, параграф 7 като лице или орган, който определя целите и средствата на обработката. [↑](#footnote-ref-17)
18. Преработвателят се определя от член 4, параграф 8 като лице или орган, който обработва данни от името на администратора. [↑](#footnote-ref-18)
19. Член 38, параграф 4: "субектите на данни могат да се свържат с служителя по защита на данните по всички въпроси, свързани с обработката на техните лични данни и с упражняването на техните права съгласно настоящия регламент". [↑](#footnote-ref-19)
20. Член 39, параграф 1, буква д): "действа като звено за контакт на надзорния орган по въпроси, свързани с обработката, включително предварителната консултация, посочена в член 36, и да се консултира по целесъобразност по отношение на всеки друг въпрос". [↑](#footnote-ref-20)
21. Член 39, параграф 1, буква а). [↑](#footnote-ref-21)
22. Вижте също Раздел 2.6 по-долу. [↑](#footnote-ref-22)
23. Съгласно член 37, параграф 3 може да бъде определен един ДЗД за няколко публични органи или органи, като се вземе предвид тяхната организационна структура и размер. Същите съображения по отношение на ресурсите и комуникацията се прилагат. Като се има предвид, че ДЗД отговаря за различни задачи, администраторът или преработвателят трябва да гарантира, че един ДЗД с помощта на екип, ако е необходимо, може да ги изпълнява ефикасно, въпреки че е определен за няколко публични органи и органи.

    Член 12, параграф 1: "Контролерът предприема подходящи мерки, за да предостави всяка информация, посочена в членове 13 и 14, и всякакви съобщения по членове 15-22 и 34, свързани с обработката на данните на субекта на данните в кратка, прозрачна, разбираема и лесно достъпна форма, използвайки ясен и ясен език, по-специално за всякаква информация, адресирана специално до дете. " [↑](#footnote-ref-23)
24. Член 39, параграф 1, буква г):" да си сътрудничи с надзорния орган " [↑](#footnote-ref-24)
25. Вж. Член 3 от ГДРСР относно териториалния обхват. [↑](#footnote-ref-25)
26. Глава II. [↑](#footnote-ref-26)
27. Глава III. 31 [↑](#footnote-ref-27)
28. Член 25. [↑](#footnote-ref-28)
29. Член 30 [↑](#footnote-ref-29)
30. Член 32 [↑](#footnote-ref-30)
31. Членове 33 и 34 [↑](#footnote-ref-31)
32. трябва да се отбележи, че член 33, параграф 3, буква б), който описва информацията, която трябва да се предостави на надзорния орган и на субектите на данни в случай на нарушение на лични данни, за разлика от член 37, параграф 7, (и не само данните за контакт) на ДЗД, които трябва да бъдат съобщени [↑](#footnote-ref-32)
33. Член 35, параграф 2. [↑](#footnote-ref-33)
34. Член 5, параграф 2. [↑](#footnote-ref-34)
35. В член 39, параграф 1 се споменават задачите на ДЗД и се посочва, че ДЗД трябва да има "най-малко" следните задачи. Следователно нищо не възпрепятства администратора да възлага на ДЗД други задачи, различни от тези, изрично упоменати в член 39, параграф 1, или да конкретизира тези задачи по-подробно. [↑](#footnote-ref-35)
36. Член 24, параграф 1 предвижда, че "като се вземат предвид естеството, обхватът, контекстът и целите на обработката, както и рисковете от различна вероятност и сериозност на правата и свободите на физическите лица, администраторът прилага подходящи технически и организационни мерки да осигури и да може да докаже, че обработката се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и актуализират, когато е необходимо. " [↑](#footnote-ref-36)
37. Член 24, параграф 1, буква г), Регламент (ЕО) № 45/2001 [↑](#footnote-ref-37)