

## WP243 ПРИЛОЖЕНИЕ — ЧЕСТО ЗАДАВАНИ ВЪПРОСИ

*Целта на настоящото приложение е да се отговори по прост и лесен за четене начин на някои основни въпроси, които може да възникнат в организациите по отношение на новите изисквания съгласно ОРЗД за назначаването на ДЛЗД.*

### Определяне на ДЛЗД (член 37)

---

#### **1 Кои организации са задължени да назначават ДЛЗД? (член 37, параграф 1)**

Според ОРЗД определянето на ДЛЗД се изисква в три конкретни случая:

- когато обработването се извършва от публичен орган или структура (независимо какви данни се обработват);
- когато основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които изискват редовно и систематично мащабно наблюдение на субектите на данни; както и
- когато основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специални категории данни или лични данни, свързани с присъди и нарушения.

Следва да се има предвид, че според правото на Съюза или на държава членка определянето на ДЛЗД може да се изисква и в други случаи. В заключение трябва да се отбележи, че дори назначаването на ДЛЗД да не е задължително, понякога организациите може да сметнат за полезно доброволно да определят ДЛЗД. Работната група за защита на личните данни по член 29 („Работната група по член 29“) насърчава тези доброволни усилия.

*За повече информация вж. раздел 2.1 от Насоките.*

#### **2 Какво означава понятието „основни дейности“? (член 37, параграф 1, букви б) и в)**

За „основни дейности“ може да се считат ключовите операции за постигане на целите на администратора или на обработващия лични данни. Те включват и всички дейности, при които обработването на данни представлява неразривна част от дейността на администратора или на обработващия лични данни. Например обработването на данни за здравословното състояние като здравни досиета на пациенти следва да се счита за една от основните дейности на всяка болница и следователно болниците трябва да определят ДЛЗД.

От друга страна, всички организации извършват определени спомагателни дейности, например плащане на служителите си или осъществяване на стандартни дейности по поддръжка на ИТ. Това са спомагателни функции, които са необходими за основната дейност или основното направление на стопанската дейност на организацията. Въпреки че тези дейности са необходими или дори съществено важни, те обикновено са считани за спомагателни функции, а не за основна дейност.

*За повече информация вж. раздел 2.1.2 от Насоките.*

### **3 Какво означава понятието „машабно обработване“? (член 37, параграф 1, букви б) и в)**

В ОРЗД не е дадено определение на това какво представлява машабно обработване. Работната група по член 29 препоръчва, когато се установява дали се извършва машабно обработване, да се вземат предвид по-специално следните фактори:

- брой на засегнатите субекти на данните или като конкретен брой, или като дял от съответното население;
- обем на данните и/или диапазон от различни елементи на данните, които се обработват;
- продължителност или постоянство на дейността по обработване на данните;
- географски обхват на дейността по обработване.

Примерите за машабно обработване включват:

- обработване на пациентски данни в обичайните условия на осъществяване на дейността на болница;
- обработване на данни за пътувания на физически лица, използващи системата за обществен транспорт на даден град (например проследяване чрез карти за пътуване);
- обработване в реално време на данни за определяне на географското местоположение на клиенти на международна верига за бързо хранене за статистически цели от страна на обработващ лични данни, който е специализиран в тези дейности;
- обработване на клиентски данни от застрахователно дружество или банка в обичайните условия на осъществяване на дейността;
- обработване на лични данни от търсачка с цел поведенческа реклама;
- обработване на данни (съдържание, трафик, местоположение) от доставчици на телефонни или интернет услуги.

Примерите, които не представляват машабно обработване, включват:

- обработване на пациентски данни от отделен лекар;
- обработване на лични данни от отделен адвокат във връзка с присъди и нарушения.

*За повече информация вж. раздел 2.1.3 от Насоките.*

### **4 Какво означава понятието „редовно и систематично наблюдение“? (член 37, параграф 1, буква б)**

Понятието „редовно и систематично наблюдение“ на субектите на данните не е определено в ОРЗД, но ясно включва всички форми на проследяване и профилиране в интернет, включително с цел поведенческа реклама. Все пак понятието „наблюдение“ не е ограничено до онлайн средата.

Според тълкуването на Работната група по член 29 „редовно“ означава едно или повече от следните:

- текущо или възникващо на определени интервали за определен период;
- многократно или повтарящо се на определени интервали;
- случващо се постоянно или периодически.

Според тълкуването на Работната група по член 29 „систематично“ означава едно или повече от следните:

- възникващо по някаква система;
- предварително уредено, организирано или методично;

- случващо се в рамките на общ план за събиране на данни;
- осъществявано в рамките на стратегия.

Примери: експлоатация на далекосъобщителна мрежа; предоставяне на далекосъобщителни услуги; пренасочване на електронни съобщения; профилиране и оценяване за целите на оценка на риска (например за определяне на кредитоспособността, изчисляване на застрахователни премии, предотвратяване на измами, откриване на случаи на изпиране на пари); проследяване на местоположението, например чрез мобилни приложения; програми за лоялност; поведенческа реклама; наблюдение на данни за благосъстоянието, тонуса и здравословното състояние чрез носими устройства; вътрешна система за видеонаблюдение; свързани устройства, например интелигентни измервателни устройства, интелигентни автомобили, автоматизация на дома и т.н.

*За повече информация вж. раздел 2.1.4 от Насоките.*

## **5 Могат ли организациите да назначават съвместно ДЛЗД? Ако отговорът е „да“, при какви условия? (членове 37, параграфи 2 и 3)**

В ОРЗД е предвидено, че група предприятия може да определи едно ДЛЗД, при условие че „от всяко предприятие има лесен достъп“ до въпросното лице. Понятието за достъпност се отнася до задачите на ДЛЗД като точка за контакт по отношение на субектите на данните, надзорния орган и също така вътрешно в рамките на организацията. За да се гарантира достъпът до ДЛЗД, независимо дали вътрешен или външен достъп, в съответствие с ОРЗД е важно да се осигури наличието на неговите данни за контакт. ДЛЗД трябва да е в състояние ефективно да общува със субектите на данни и да си сътрудничи със съответните надзорни органи. Това означава, че въпросната комуникация трябва да се осъществява на езика или езиците, използван/и от съответните надзорни органи или субекти на данните. Личното присъствие на ДЛЗД (независимо дали присъства физически в същото помещение като служителите, или чрез гореща линия или други сигурни средства за комуникация) е от съществена важност, за да се гарантира, че субектите на данни ще бъдат в състояние да се свързват с ДЛЗД.

*За повече информация вж. раздел 2.3 от Насоките.*

## **6 Възможно ли е да се назначи външно ДЛЗД (член 37, параграф 6)?**

Да. Според член 37, параграф 6 ДЛЗД може да бъде член на персонала на администратора или обработващия лични данни (вътрешно ДЛЗД) или „да изпълнява задачите въз основа на договор за услуги“. Това означава, че ДЛЗД може да бъде външно лице и в такъв случай неговите функции може да се упражняват на база на договор за услуги, сключен с физическо лице или организация.

Когато ДЛЗД е външно лице, всички изисквания по членове 37—39 са приложими за въпросното ДЛЗД. Както е посочено в Насоките, когато функциите на ДЛЗД се изпълняват от външен доставчик на услуги, екип от физически лица, работещи за съответното предприятие, може ефективно да изпълнява задачите на ДЛЗД като екип, отговорност за който носи определеното лице за контакт и „отговорник“ за клиента. В този случай е съществено важно всеки член на външната организация, който изпълнява функциите на ДЛЗД, да отговаря на всички приложими изисквания по ОРЗД.

В насоките се препоръчва, с оглед на правната яснота и добрата организация, в договора за услуги да се предвиди ясно разпределение на задачите в рамките на външния екип на ДЛЗД и за всеки клиент да бъде определено по едно физическо лице като основно лице за контакт и „отговорник“.

*За повече информация вж. раздели 2.3, 2.4 и 3.5 от Насоките.*

## **7 Какви професионални качества трябва да притежава ДЛЗД (член 37, параграф 5)?**

Според ОРЗД се изисква ДЛЗД да *„се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания в областта на законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите, посочени в член 39“*.

Необходимото ниво на експертни знания следва да се определя в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за обработваните лични данни. Например когато дадена дейност по обработване на данни е особено сложна или когато се касае за голям обем от чувствителни данни, ДЛЗД може да има нужда от повече опит и подкрепа.

Необходимите умения и опит включват:

- опит с национални и европейски закони и практики в областта на защитата на данните, в това число разбиране на ОРЗД в дълбочина;
- разбиране на извършваните операции по обработване;
- разбиране на информационните технологии и сигурността на данните;
- познания за стопанския сектор и организацията;
- способност за насърчаване на културата на защита на данните в рамките на организацията.

*За повече информация вж. раздел 2.4 от Насоките.*

## **Длъжност на ДЛЗД (член 38)**

---

## **8 Какви ресурси трябва да бъдат предоставени на ДЛЗД, за да може да изпълнява своите задачи?**

Според член 38, параграф 2 от ОРЗД се изисква организацияте да подпомагат своите ДЛЗД, като *„осигуряват ресурсите, необходими за изпълнението на [техните] задачи, и достъп до личните данни и операциите по обработване, а така също поддържат [техните] експертни знания“*.

В зависимост от естеството на операциите по обработване и от дейностите и големината на организацията, на ДЛЗД трябва да бъдат предоставени следните ресурси:

- активно подпомагане на функциите на ДЛЗД от страна на висшето ръководство;
- достатъчно време за изпълнението на задачите на ДЛЗД;
- подходящо подпомагане от гледна точка на финансови ресурси, инфраструктура (помещения, съоръжения, оборудване) и персонал, когато е целесъобразно;
- официално съобщаване на назначаването на ДЛЗД пред целия персонал;
- достъп до други отдели в рамките на организацията, за да могат ДЛЗД да получават съществено важно подпомагане, ресурси или информация от въпросните други отдели;
- продължаващо обучение.

*За повече информация вж. раздел 3.2 от Насоките.*

## **9 Какви гаранции дават възможност на ДЛЗД да изпълнява задачите си по независим начин (член 38, параграф 3)?**

Предвидени са няколко гаранции, с които се дава възможност на ДЛЗД да действа „независимо“, както е посочено в съображение 97:

- не се дават указания от страна на администраторите или обработващите лични данни по отношение на изпълнението на задачите на ДЛЗД;
- не се допуска освобождаване от длъжност от страна на администратора във връзка с изпълнението на задачите на ДЛЗД;
- не се допуска конфликт на интереси с евентуални други задачи и задължения.

*За повече информация вж. раздели 3.3—3.5 от Насоките.*

## **10 Кои са „другите задачи и задължения“ на ДЛЗД, които може да доведат до конфликт на интереси (член 38, параграф 6)?**

ДЛЗД не може да заема длъжност в рамките на организацията, която ще го задължава да определя целите и средствата за обработването на лични данни. Поради специфичната организационна структура във всяка организация, този аспект трябва да се разглежда на база конкретен случай.

Длъжностите в рамките на организацията, които влизат в противоречие, по общо правило може да включват длъжности във висшето ръководство (като главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, ръководител на маркетингов отдел, ръководител на отдел „Човешки ресурси“ или ръководител на ИТ отдела), но също така и други функции по-надолу в организационната структура, ако въпросните длъжности или функции са свързани с определяне на целите и средствата за обработване.

*За повече информация вж. раздел 3.5 от Насоките.*

## **Задачи на ДЛЗД (член 39)**

---

## **11 Какво обхваща понятието „наблюдение на спазването“ на ОРЗД (член 39, параграф 1, буква б)?**

В рамките на задълженията за наблюдение на спазването ДЛЗД може по-специално:

- да събира информация за определяне на дейностите по обработване;
- да анализира и проверява спазването на дейностите по обработване; както и
- да информира, съветва и отправя препоръки към администратора или обработващия лични данни.

*За повече информация вж. раздел 4.1 от Насоките.*

## **12 Носи ли ДЛЗД лична отговорност за неспазване на ОРЗД?**

Не, ДЛЗД не носят лична отговорност за неспазването на ОРЗД. В ОРЗД ясно е посочено, че администраторът или обработващият лични данни е този, който е длъжен да гарантира и да бъде в състояние да докаже, че обработването се извършва в съответствие с този регламент (член 24, параграф 1). Спазването на разпоредбите за защита на данните е отговорност на администратора или на обработващия лични данни.

## **13 Каква е ролята на ДЛЗД във връзка с оценката на въздействието върху защитата на данните (член 37, параграф 1, буква в) и регистъра на дейностите по обработване (член 30)?**

Що се отнася до оценката на въздействието върху защитата на данните, администраторът или обработващият лични данни следва да иска становището на ДЛЗД по следните въпроси, наред с други:

- дали на извърши ОВЗД или не;
- каква методика да използва при извършването на ОВЗД;
- дали да извърши ОВЗД вътрешно или да я възложи на външен изпълнител;
- какви гаранции (включително технически и организационни мерки) да приложи, за да намали всички рискове за правата и интересите на субектите на данните;
- дали оценката на въздействието върху защитата на данните е извършена правилно и дали заключенията от нея (дали да се продължи с обработването и какви гаранции да се приложат) съответстват на ОРЗД.

*За повече информация вж. раздел 4.2 от Насоките.*

Що се отнася до регистъра на дейностите по обработване, администраторът или обработващият лични данни, а не ДЛЗД, е този, който следва да поддържа регистър на операциите по обработване. Нищо обаче не пречи на администратора или обработващия лични данни да възложи на ДЛЗД задачата да води регистъра на операциите по обработване, за които отговаря администраторът или обработващият лични данни. Този регистър следва да се счита за един от инструментите, даващи възможност на ДЛЗД да изпълнява своите задачи по наблюдение на спазването, информиране и съветване на администратора или обработващия лични данни.

*За повече информация вж. раздел 4.4 от Насоките.*