РАБОТНА ГРУПА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПО ЧЛЕН 29

17/BG

WP 248 rev. 01

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

Приети на 4 април 2017 г.

Последно преработени и приети на 4 октомври 2017 г.

РАБОТНАТА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

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

като взе предвид членове 29 и 30 от нея,

като взе предвид Правилника за дейността си,

ПРИЕ НАСТОЯЩИТЕ НАСОКИ:

Съдържание

I. Въведение

Регламент 2016/679[1] (ОРЗД) ще се прилага от 25 май 2018 г. С член 35 от ОРЗД се въвежда понятието за оценка на въздействието върху защитата на данните (ОВЗД)[2], което се съдържа и в Директива 2016/680[3].

ОВЗД представлява процес, чиято цел е да опише обработването, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни[4], като ги оцени и определи мерки за справяне с тези рискове. ОВЗД представляват важен инструмент за отчетност, тъй като помагат на администраторите на лични данни не само да спазят изискванията на ОРЗД, но и да демонстрират, че са предприети подходящи мерки за гарантиране на спазването на Регламента (вж. също така член 24)[5]. С други думи **ОВЗД е процес за осигуряване и доказване на спазването на изискванията**.

Съгласно ОРЗД неспазването на изискванията за ОВЗД може да доведе до налагане на глоби от компетентния надзорен орган. Ако не бъде извършена ОВЗД, когато обработването подлежи на ОВЗД (член 35, параграфи 1, 3 и 4), ако ОВЗД бъде извършена неправилно (член 35, параграфи 2, 7 и 9) или ако не бъде проведена консултация с компетентния надзорен орган, когато това се

---

[1] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

[2] Изразът „оценка на въздействието върху неприкосновеността на личния живот“ (ОВНЛЖ) често се използва в други видове контекст за обозначаване на същото понятие.

[3] В член 27 от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни също се посочва, че е необходима оценка на въздействието върху неприкосновеността на личния живот, тъй като съществува вероятност обработването „*да породи висок риск за правата и свободите на физическите лица*“.

[4] ОРЗД не съдържа официално определение на понятието ОВЗД, но

- минималното му съдържание е посочено в член 35, параграф 7, както следва:
  - „*а) системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;*
  - *б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;*
  - *в) оценка на рисковете за правата и свободите на субектите на данни, посочени в параграф 1; и*
  - *г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.“;*
- значението и ролята му са пояснени в съображение 84, както следва: „*За да се подобри спазването на настоящия регламент, когато има вероятност операциите по обработването да доведат до висок риск за правата и свободите на физическите лица, администраторът следва да отговаря за изготвянето на оценка на въздействието върху защитата на личните данни, за да се оценят по-специално произходът, естеството, спецификата и степента на този риск*“.

[5] Вж. също така съображение 84: „*Резултатите от оценката следва да бъдат взети предвид, когато се определят съответните мерки, за да се докаже, че обработването на лични данни отговаря на изискванията на настоящия регламент*“.

изисква (член 36, параграф 3, буква д), това може да доведе до налагането на административна глоба в размер до 10 милиона евро или, в случай на предприятие, до 2 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока.

II. Приложно поле на насоките

В настоящите насоки се вземат предвид:

- Изявлението на работната група за защита на личните данни по член 29 (РГ29), 14/EN WP 218[6];
- Насоките на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243[7];
- Становището на РГ29 относно ограничаването в рамките на целта, 13/EN WP 203[8];
- международни стандарти[9].

В съответствие с основания на анализ на риска подход, залегнал в ОРЗД, извършването на ОВЗД не е задължително за всяка операция по обработване. ОВЗД се изисква само когато съществува вероятност обработването „*да породи висок риск за правата и свободите на физическите лица*“ (член 35, параграф 1). За да се гарантира последователно тълкуване на обстоятелствата, при които е задължително да се извърши ОВЗД (член 35, параграф 3), целта на настоящите насоки на първо място е да се поясни това понятие и да се осигурят критерии за списъците, които трябва да бъдат приети от органите по защита на данните (ОЗД) съгласно член 35, параграф 4.

Съгласно член 70, параграф 1, буква д) Европейският комитет по защита на данните (ЕКЗД) ще може да издава насоки, препоръки и най-добри практики с цел насърчаване на съгласуваното прилагане на ОРЗД. Целта на настоящия документ е да се създаде основа за такава бъдеща работа на ЕКЗД и в тази връзка да се пояснят съответните разпоредби от ОРЗД, за да се помогне на администраторите да спазят правните разпоредби и да се осигури правна сигурност за администраторите, които следва да извършват ОВЗД.

Настоящите насоки също така целят да насърчат разработването на:

- общ списък на операциите по обработване в Европейския съюз, за които е задължително да се извърши ОВЗД (член 35, параграф 4);

---

[6] Изявление на РГ29 относно ролята на основания на анализ на риска подход към правните рамки за защита на данните, 14/EN WP 218, прието на 30 май 2014 г.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Насоки на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243, приети на 13 декември 2016 г.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Становище 03/2013 на РГ 29 относно ограничаването в рамките на целта, 13/EN WP 203, прието на 2 април 2013 г.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Например ISO 31000:2009, *Управление на риска. Принципи и указания*, Международна организация по стандартизация (ISO); ISO/IEC 29134 (проект), *Информационни технологии. Техники за сигурност. Оценка на въздействието върху неприкосновеността на личния живот. Указания*, Международна организация по стандартизация (ISO).

- общ списък на операциите по обработване в ЕС, за които не е задължително да се извърши ОВЗД (член 35, параграф 5);
- общи критерии относно методологията за извършване на ОВЗД (член 35, параграф 5);
- общи критерии за уточняване в кои случаи следва да се провежда консултация с надзорния орган (член 36, параграф 1);
- препоръки, когато е възможно, в които се доразвива опитът, придобит от държавите — членки на ЕС.

III. ОВЗД: обяснение на Регламента

Съгласно ОРЗД администраторите са длъжни да въведат подходящи мерки, за да гарантират и да бъдат в състояние да докажат, че спазват ОРЗД, като вземат предвид, наред с другото, „рисковете с различна вероятност и тежест за правата и свободите на физическите лица“ (член 24, параграф 1). Задължението на администраторите да извършват ОВЗД при определени обстоятелства следва да се разбира в контекста на общото им задължение да управляват по подходящ начин рисковете[10], породени от обработването на лични данни.

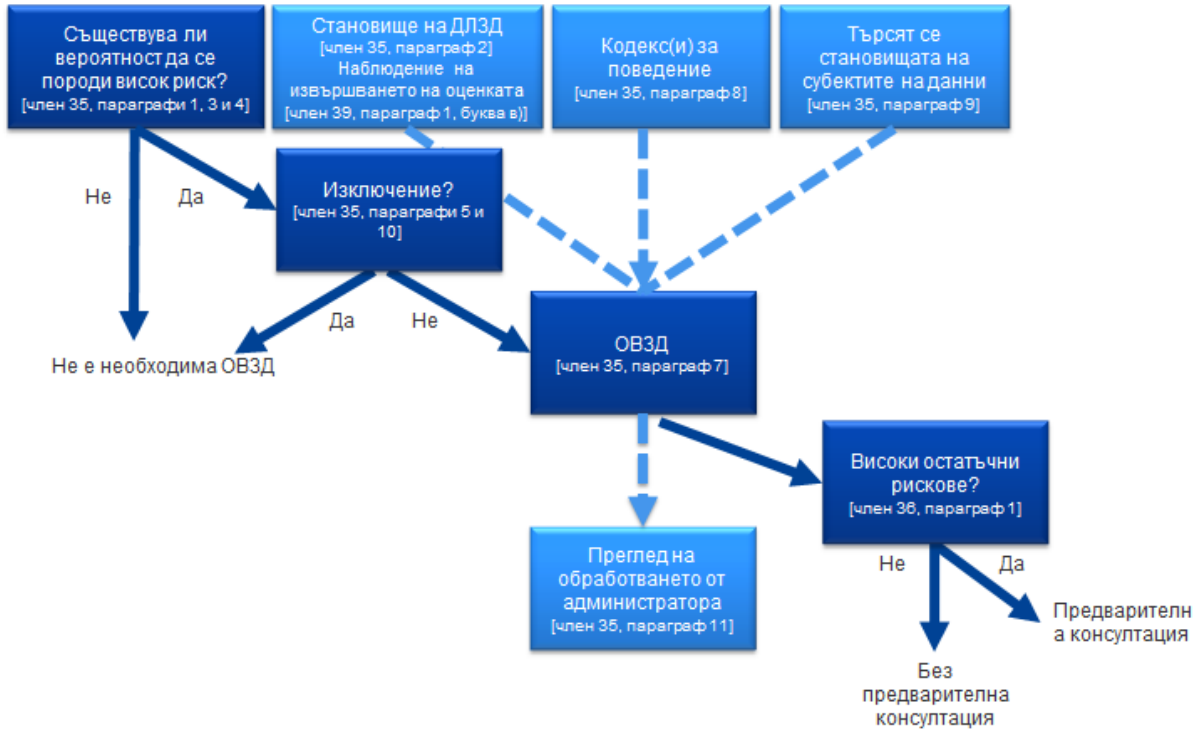
„Риск“ означава сценарий, описващ дадено събитие и неговите последици, оценени от гледна точка на тяхната тежест и вероятност. От друга страна „управление на риска“ може да се определи като координирани дейности за ръководенето и контролирането на дадена организация във връзка с риска.

В член 35 се посочва вероятността от висок риск „за правата и свободите на физическите лица“. Както се посочва в изготвеното от Работната група за защита на личните данни по член 29 изявление относно ролята на основания на анализ на риска подход към правните рамки за защита на данните, посочването на „правата и свободите“ на субектите на данни е свързано най-вече с правата за защитата на личните данни и неприкосновеността на личния живот, но може да включва и други основни права, като например свободата на словото, свободата на мисълта, свободата на движение, забраната за дискриминация, правото на свобода и свободата на съвестта и религията.

В съответствие с основания на анализ на риска подход, залегнал в ОРЗД, извършването на ОВЗД не е задължително за всяка операция по обработване. Вместо това ОВЗД се изисква само когато съществува вероятност определен вид обработване „да породи висок риск за правата и свободите на физическите лица“ (член 35, параграф 1). При все това самият факт, че не са налице условията, при които извършването на ОВЗД е задължително, не намалява общото задължение на администраторите да въведат мерки, за да управляват по подходящ начин рисковете за правата и свободите на субектите на данни. На практика това означава, че администраторите трябва непрекъснато да оценяват рисковете, които се пораждат от техните дейности по обработване, за да идентифицират кога съществува вероятност определен вид обработване „да породи висок риск за правата и свободите на физическите лица“.

[10] Трябва да се подчертае, че с цел управление на рисковете за правата и свободите на физическите лица тези рискове трябва редовно да се идентифицират, анализират, преценяват, оценяват, третират (например като се ограничават...) и преразглеждат. Администраторите не могат да избегнат своята отговорност, като сключват застрахователни полици за покритие на рисковете.

Следната фигура илюстрира основните принципи, свързани с ОВЗД в ОРЗД:



A. Към какво е насочена ОВЗД? Една-единствена операция по обработване или набор от сходни операции по обработване.

ОВЗД може да е свързана с една-единствена операция по обработване на данни. При все това член 35, параграф 1 гласи, че „*в една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове*“. В съображение 92 се добавя, че „*при определени обстоятелства може да бъде разумно и рентабилно предметът на дадена оценка на въздействието върху защитата на данните да обхваща повече от един проект, например когато обществени органи или структури възнамеряват да създадат общо приложение или платформа за обработване на данни или когато няколко администратори планират внедряването на общо приложение или среда за обработване на данните в цял промишлен сектор или сегмент или за широко използвана хоризонтална дейност*“.

Би могла да се използва една-единствена ОВЗД за оценяване на множество операции по обработване, които са сходни по своето естество, обхват, контекст, цел и рискове. В действителност ОВЗД целят систематичното проучване на нови ситуации, които биха могли да доведат до високи рискове за правата и свободите на физическите лица, и не е нужно да се извършва ОВЗД в случаите (т.е. операции по обработване, извършвани в определен контекст и за конкретна цел), които вече са проучени. Такъв може да бъде случаят, когато се използва сходна технология за събирането на един и същ вид данни за едни и същи цели. Например група от общински органи, всеки от които създава сходна система за видеонаблюдение, би могла да извърши една-единствена ОВЗД, която обхваща обработването от отделните администратори, или железопътен оператор (един-единствен администратор) би могъл да обхване видеонаблюдението на всички свои железопътни гари с една ОВЗД. Това може да бъде приложимо и към сходни операции по обработване, извършвани от различни администратори. В такива случаи следва да бъде споделена референтна ОВЗД или да бъде направена публично

достъпна, като описаните в ОВЗД мерки трябва да бъдат изпълнени и трябва да бъде представена обосновка за извършването само на една-единствена ОВЗД.

Когато операцията по обработване включва съвместни администратори, те трябва да определят прецизно своите задължения. В тяхната ОВЗД следва да се посочва коя страна отговаря за различните мерки за третиране на рисковете и за защита на правата и свободите на субектите на данни. Всеки администратор следва да посочи своите потребности и да споделя полезна информация, без да разкрива тайни (например защита на търговски тайни, интелектуална собственост, поверителна търговска информация) или да оповестява слабости.

ОВЗД също така може да бъде полезна за оценяване на въздействието върху защитата на данните на даден технологичен продукт, например хардуер или софтуер, когато има вероятност той да се използва от различни администратори за извършване на различни операции по обработване. Естествено администраторът, който въвежда продукта, продължава да носи отговорност за извършването на своя ОВЗД по отношение на конкретното изпълнение, но при нейното извършване той може да използва като основа изготвена от доставчика на продукта ОВЗД, ако е целесъобразно. Като пример могат да бъдат посочени отношенията между производителите на интелигентни измервателни уреди и дружествата за комунални услуги. Всеки доставчик на продукт или обработващ лични данни следва да споделя полезна информация, без да разкрива тайни или да създава рискове за сигурността, като оповестява слабости.

Б. Кои операции по обработване подлежат на ОВЗД? Освен изключенията, всяка операция, при която съществува вероятност „*да породи висок риск*“.

В настоящия раздел се описва кога ОВЗД е задължителна и кога не е необходимо да се извършва ОВЗД.

Освен ако операцията по обработване не отговаря на едно от изключенията (III.Б.а), трябва да се извърши ОВЗД, когато съществува вероятност операцията по обработване „*да породи висок риск*“ (III.Б.б).

а) Кога задължително се извършва ОВЗД? Когато съществува вероятност обработването „*да породи висок риск*“.

Съгласно ОРЗД не се изисква да се извършва ОВЗД за всяка операция по обработване, която може да породи рискове за правата и свободите на физическите лица. Извършването на ОВЗД е задължително само когато съществува вероятност обработването „*да породи висок риск за правата и свободите на физическите лица*“ (член 35, параграф 1, както е илюстрирано в член 35, параграф 3 и допълнено от член 35, параграф 4). Това е от особено значение, когато се въвежда нова технология за обработване на данни[11].

В случаите, когато не е ясно дали се изисква ОВЗД, РГ29 препоръчва все пак да се извърши ОВЗД, тъй като тя представлява полезен инструмент, който помага на администраторите да спазват законодателството в областта на защитата на данните.

[11] Вж. съображения 89, 91 и член 35, параграфи 1 и 3 за допълнителни примери.

Въпреки че ОВЗД може да се изисква и при други обстоятелства, в член 35, параграф 3 се посочват някои примери кога съществува вероятност операцията по обработване „*да породи висок риск*“:

- „*а) систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице*[12]*;*
- *б) мащабно обработване на специални категории данни, посочени в член 9, параграф 1 или на лични данни за присъди и нарушения по член 10*[13]*; или*
- *в) систематично мащабно наблюдение на публично достъпна зона“*.

Както става ясно от израза „*по-специално*“ в уводното изречение на член 35, параграф 3 от ОРЗД, посоченият списък не е изчерпателен. Възможно е да съществуват „високорискови“ операции по обработване, които да не са включени в този списък, но да пораждат сходен „висок риск“. Такива операции по обработване също следва да подлежат на ОВЗД. Поради тази причина в някои случаи изложените по-долу критерии са нещо повече от просто обяснение на това, което следва да се разбира от трите примера, дадени в член 35, параграф 3 от ОРЗД.

С оглед да се представи по-конкретен набор от операции по обработване, при които трябва да се извърши ОВЗД поради присъщия за тях висок риск, като се вземат предвид конкретните елементи на член 35, параграф 1 и член 35, параграф 3, букви а)—в), списъкът, който следва да бъде приет на национално равнище съгласно член 35, параграф 4, и съображения 71, 75 и 91, както и други препратки в ОРЗД към операции по обработване, които „*има вероятност да доведат до висок риск*“[14], следва да се вземат под внимание следните девет критерия.

1. Оценка или точкуване, включително профилиране и прогнозиране, по-специално от *„аспекти, имащи отношение към резултатите в работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението, местоположението или движенията“* (съображения 71 и 91). Примерите за това биха могли да включват финансови институции, които извършват справки за своите клиенти в референтна база данни за кредити, в база данни за борба срещу изпирането на пари или финансирането на тероризма или в база данни за борба с измамите, биотехнологични компании, които предлагат генетични тестове директно на клиенти, за да оценят и прогнозират рисковете от заболявания/здравните рискове, или компании, които създават поведенчески или маркетингови профили въз основа на използването на техния уебсайт или навигацията в него.
2. Автоматизирано вземане на решения с правни последици или подобни сериозни последици: обработване с цел вземане на засягащи субектите на данни решения, които

[12] Вж. съображение 75: „*по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили*“.

[13] Вж. съображение 75: „*когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност*“.

[14] Вж. например съображения 75, 76, 92, 116.

имат „*правни последици за физическото лице*“ или „*по подобен начин сериозно засягат физическото лице*“ (член 35, параграф 3, буква а). Например обработването може да доведе до изключване или дискриминация на физически лица. Обработването с незначителни последици или без последици за физическите лица не отговаря на този конкретен критерий. Допълнителни обяснения за тези понятия ще бъдат дадени в предстоящите Насоки на РГ29 относно профилирането.

3. Систематично наблюдение: обработване, което се използва за наблюдение, мониторинг или контрол на субектите на данни, включително данни, които се събират чрез мрежи, или „*систематично мащабно наблюдение на публично достъпна зона*“ (член 35, параграф 3, буква в))[15]. Този вид наблюдение е включен като критерий, защото е възможно да се събират лични данни при обстоятелства, когато субектите на данни може да не осъзнават кой събира техните данни и как ще бъдат използвани. Освен това за физическите лица може да е невъзможно да избегнат подлагането на такова обработване в публична (или публично достъпна) зона.
4. Чувствителни данни или данни от изключително лично естество: това включва специални категории лични данни, определени в член 9 (например информация относно политическите възгледи на физическите лица), както и лични данни, свързани с присъди и нарушения по смисъла на член 10. Пример за това биха били обществени болници, които съхраняват медицинските досиета на пациентите, или частни детективи, които съхраняват данните на нарушителите. Отвъд тези разпоредби на ОРЗД, за някои категории данни може да се счита, че увеличават евентуалния риск за правата и свободите на физическите лица. Тези лични данни се считат за чувствителни (по начина, по който се възприема обикновено този термин), защото са свързани с домашни и лични занимания (като например електронни съобщения, чиято поверителност следва да бъде защитена) или защото засягат упражняването на основно право (като например данни за местонахождението, събирането на които поставя под въпрос свободата на движение), или защото нарушенията във връзка с тях очевидно биха довели до сериозно въздействие върху ежедневието на субекта на данни (като например финансови данни, които могат да се използват за измами при плащания). В тази връзка може да е от значение дали данните вече са обявени публично от съответното физическо лице или от трети страни. Фактът, че личните данни са публично достъпни, може да се разгледа като фактор в оценката, ако се е очаквало данните да се използват допълнително за определени цели. Този критерий също така може да включва данни, като например лични документи, електронни писма, дневници, бележки от електронни четци, които позволяват водене на бележки, и изключително личната информация, записвана от приложения, в които се отбелязват събития от живота.
5. Мащабно обработване на данни: в ОРЗД не се определя какво означава мащабно, въпреки че съображение 91 съдържа известни насоки. Във всеки случай РГ29

[15] Съгласно тълкуването на РГ29 *„систематично“* е наблюдението, което отговаря на един или повече от следните критерии (вж. Насоки на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243):

- извършва се в съответствие с дадена система;
- предварително установено е, организирано е или е методично;
- извършва се като част от общ план за събиране на данни;
- извършва се като част от стратегия.

Съгласно тълкуването на РГ29 *„публично достъпна зона“* е всяко място, достъпно за гражданите, например площад, търговски център, улица, пазар, железопътна гара или обществена библиотека.

препоръчва да се проучат по-специално следните фактори, когато се определя дали извършваното обработване е мащабно[16]:

а. броят на засегнатите субекти на данни като конкретна цифра или като дял от съответното население;
б. обемът на данните и/или обхватът на различните видове данни, които се обработват;
в. продължителността или непрекъснатостта на дейността по обработване на данните;
г. географският обхват на дейността по обработване.

6. Търсене на съвпадение или съчетаване на набори от данни, например с произход от две или повече операции по обработване на данни, извършени за различни цели и/или от различни администратори, по начин, който надхвърля разумните очаквания на субекта на данни[17].
7. Данни относно уязвими субекти на данни (съображение 75): обработването на този вид данни е включено като критерий поради увеличената неравнопоставеност на правомощията между субектите на данни и администратора, което означава, че физическите лица може да не са в състояние лесно да се съгласят или да възразят срещу обработването на техните данни, или да упражнят своите права. Уязвимите субекти на данни могат да включват деца (може да се счита, че те не са в състояние съзнателно и мотивирано да възразят срещу или да се съгласят с обработването на техните данни), служители, по-уязвими сегменти от населението, които се нуждаят от специална защита (психично болни лица, търсещи убежище лица или възрастни лица, пациенти и др.) и субекти на данни във всички случаи, при които може да се установи неравнопоставеност в отношенията с оглед на положението на субекта на данни и това на администратора.
8. Иновативно използване или прилагане на нови технологични или организационни решения, като например съчетаване на използването на пръстови отпечатъци и разпознаване на лица с цел подобряване на контрола на физическия достъп и др. В ОРЗД ясно се посочва (член 35, параграф 1 и съображения 89 и 91), че използването на нова технология, определена „*в съответствие с постигнатото ниво на технически познания*“ (съображение 91), може да доведе до необходимост от извършване на ОВЗД. Причината за това е, че използването на такава технология може да включва нови форми на събиране и използване на данни, което евентуално води до висок риск за правата и свободите на физическите лица. В действителност личните и социалните последици от внедряването на нова технология може да не са известни. ОВЗД ще помогне на администратора да разбере и да третира тези рискове. Например някои приложения, свързани с „интернет на предметите“, биха могли да окажат значително въздействие върху ежедневния живот на физическите лица и неговата неприкосновеност; и поради това изискват ОВЗД.
9. Когато операциите по обработванет сами по себе си „*възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор*“ (член 22 и съображение 91). Това включва операции по обработване, чиято цел е да се позволи, измени или откаже достъпът на субектите на данни до услуга или сключването на договор. Пример за това са банки, които извършват справки за своите клиенти в референтна база данни за кредити, за да решат дали да им предложат кредит.

В повечето случаи администраторът може да заключи, че ако обработването отговаря на два критерия, ще се изисква извършването на ОВЗД. Като цяло РГ29 счита, че на колкото повече критерии отговаря обработването, толкова по-вероятно е да поражда висок риск за правата и

[16] Вж. Насоки на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243.
[17] Вж. обяснението в становището на РГ29 относно ограничаването в рамките на целта, 13/EN WP 203, стр. 24.

свободите на субектите на данни, поради което ще изисква ОВЗД независимо от мерките, които администраторът планира да въведе.

При все това в някои случаи **администраторът може да заключи, че обработване, което отговаря само на един от тези критерии, изисква ОВЗД.**

Следните примери илюстрират как следва да се използват критериите, за да се оцени дали конкретна операция по обработване изисква ОВЗД:

Примери за обработване	**Евентуално приложими критерии**	**Има ли вероятност да се изисква ОВЗД?**
Болница, която обработва генетичните и здравните данни на своите пациенти (информационна система на болницата).	- Чувствителни данни или данни от изключително лично естество. - Данни относно уязвими субекти на данни. - Мащабно обработване на данни.	Да
Използване на система от камери за наблюдение на поведението на шофьорите на магистралите. Администраторът предвижда да използва интелигентна система за видеоанализ за идентифициране на отделни автомобили и автоматично разпознаване на регистрационни номера.	- Систематично наблюдение. - Иновативно използване или прилагане на технологични или организационни решения.	
Дружество, което осъществява систематично наблюдение на дейностите на своите служители, включително наблюдение на работните станции на служителите, дейността им в интернет и др.	- Систематично наблюдение. - Данни относно уязвими субекти на данни.	
Събиране на публични данни от социални мрежи с цел изготвяне на профили.	- Оценка или точкуване. - Мащабно обработване на данни. - Търсене на съвпадение или съчетаване на набори от данни. - Чувствителни данни или данни от изключително лично естество:	
Институция, която създава база данни за кредитен рейтинг или за борба с измамите на национално равнище.	- Оценка или точкуване. - Автоматизирано вземане на решения с правни последици или подобни сериозни последици. - Възпрепятства субект на данни да упражнява дадено право или да използва някоя услуга или договор. - Чувствителни данни или данни от изключително лично естество:	
Съхранение с цел архивиране на псевдонимизирани чувствителни лични данни относно уязвими субекти на данни, които са	- Чувствителни данни. - Данни относно уязвими субекти на данни. - Възпрепятства субекти на данни да	

Примери за обработване	Евентуално приложими критерии	Има ли вероятност да се изисква ОВЗД?
участвали в научноизследователски проекти или клинични изпитвания	упражняват дадено право или да използват някоя услуга или договор.	
Обработване на „лични данни на пациенти или клиенти на отделен лекар, друг здравен работник или адвокат“ (съображение 91).	- Чувствителни данни или данни от изключително лично естество. - Данни относно уязвими субекти на данни.	Не
Онлайн списание, което използва списък с адресати, за да изпраща общо резюме с информация на своите абонати.	- Мащабно обработване на данни.	
Уебсайт за електронна търговия, на който се показват реклами за части за стари модели автомобили, което включва ограничено профилиране въз основа на разглежданите или закупените артикули на самия уебсайт.	- Оценка или точкуване.	

От друга страна, дадена операция по обработване може да отговаря на горепосочените случаи и все пак администраторът да заключи, че не „съществува вероятност да породи висок риск“. В такива случаи администраторът следва да обоснове и документира причините, поради които не извършва ОВЗД, и да включи/отбележи възгледите на длъжностното лице по защита на данните.

Освен това като част от принципа на отчетност всеки администратор „*поддържа регистър на дейностите по обработване, за които отговаря*“, включително, наред с другото, целите на обработването, описание на категориите данни и получателите на данните, както и „*когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 32, параграф 1*“ (член 30, параграф 1), и трябва да оцени дали съществува вероятност да се породи висок риск, дори ако в крайна сметка реши да не извърши ОВЗД.

Забележка: надзорните органи са длъжни да съставят, оповестят публично и да съобщят списък на операциите по обработване, за които се изисква ОВЗД, на Европейския комитет по защита на данните (ЕКЗД) (член 35, параграф 4)[18]. Горепосочените критерии могат да помогнат на надзорните органи да съставят този списък, като по целесъобразност с времето ще се добавя по-конкретно съдържание. Например обработването на всички видове биометрични данни или данни на деца също би могло да се счита за подходящо за съставянето на списък в съответствие с член 35, параграф 4.

б) Кога не се изисква ОВЗД? Когато не съществува вероятност обработването „*да породи висок риск*“ или вече съществува сходна ОВЗД, или обработването е

[18] В този контекст „*компетентният надзорен орган прилага посочения в член 63 механизъм за съгласуваност, ако тези списъци включват дейности за обработване, свързани с предлагането на стоки или услуги на субекти на данни или с наблюдението на тяхното поведение в няколко държави членки или могат съществено да засегнат свободното движение на лични данни в рамките на Съюза*“ (член 35, параграф 6).

било разрешено преди май 2018 г., или за него има правно основание, или е включено в списъка с операции по обработване, за които не се изисква ОВЗД.

РГ29 счита, че не се изисква ОВЗД в следните случаи:

- **когато не съществува вероятност обработването „*да породи висок риск за правата и свободите на физическите лица*“** (член 35, параграф 1);
- **когато естеството, обхватът, контекстът и целите на обработването са много сходни с тези на обработването, за което е извършена ОВЗД**. В тези случаи могат да се използват резултатите от ОВЗД за сходни операции по обработване (член 35, параграф 1[19]);
- когато операциите по обработване са били проверени от надзорен орган преди май 2018 г. при конкретни условия, които не са се променили[20] (вж. III.B);
- **когато операция по обработване** съгласно член 6, параграф 1, буква в) или д) **има правно основание** в правото на Съюза или в правото на държавата членка, когато това право регулира конкретната операция по обработване **и когато вече е извършена ОВЗД** като част от установяването на това правно основание (член 35, параграф 10)[21], освен ако държавата членка не сметне за необходимо да извърши ОВЗД преди започването на дейностите за обработване;
- **когато обработването е включено в незадължителния списък (съставен от надзорния орган) с операции по обработване**, за които не се изисква ОВЗД (член 35, параграф 5). Този списък може да включва дейности по обработване, които отговарят на условията, посочени от този орган, по-специално чрез насоки, конкретни решения или разрешения, правила за спазване и други (например във Франция — разрешения, изключения, опростени правила, набори от правила за спазване...). В тези случаи и съгласно повторната оценка от компетентния надзорен орган не се изисква ОВЗД, но само ако обработването попада изцяло в обхвата на съответната процедура, посочена в списъка, и продължава да отговаря напълно на всички съответни изисквания на ОРЗД.

B. <u>Как се процедира при вече съществуващи операции по обработване? При определени обстоятелства се изисква ОВЗД.</u>

Изискването за извършване на ОВЗД се прилага към съществуващи операции по обработване, при които съществува вероятност да породят висок риск за правата и свободите на физическите лица и по отношение на които е настъпила промяна в рисковете, като се вземат предвид естеството, обхватът, контекстът и целите на обработването.

ОВЗД не е необходима за операции по обработване, които са били проверени от надзорен орган или от длъжностното лице по защита на данните в съответствие с член 20 от Директива

[19] „*В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове*“.

[20] „*Приетите от Комисията решения и разрешенията на надзорните органи въз основа на Директива 95/46/ЕО остават в сила, докато не бъдат изменени, заменени или отменени*“ (съображение 171).

[21] Когато ОВЗД се извършва на етапа на изготвяне на законодателството, което включва правното основание за обработване, съществува вероятност да се наложи преразглеждане на оценката преди започването на операциите, тъй като приетото законодателство може да се различава от предложението по начин, който оказва въздействие върху въпросите относно неприкосновеността на личния живот и защитата на данните. Освен това към момента на приемане на законодателството е възможно да не са налични достатъчни технически подробности по отношение на действителното обработване, дори ако се придружава от ОВЗД. В такива случаи може все пак да е необходимо да се извърши конкретна ОВЗД преди осъществяването на действителните дейности по обработване.

95/46/ЕО и които се извършват по начин, който не се е променил след предишната проверка. В действителност „*приетите от Комисията решения и разрешенията на надзорните органи въз основа на Директива 95/46/ЕО остават в сила, докато не бъдат изменени, заменени или отменени*“ (съображение 171).

От друга страна това означава, че на ОВЗД следва да подлежи всяко обработване на данни, чиито условия за изпълнение (обхват, цел, събрани лични данни, самоличност на администраторите или получателите, срок на задържане на данните, технически и организационни мерки и др.) са се променили след предишната проверка, извършена от надзорния орган или от длъжностното лице по защита на данните, и при което съществува вероятност да породи висок риск.

Освен това би могла да се изисква ОВЗД след промяна в рисковете, породени от операциите по обработване[22], например защото започва да се използва нова технология или защото личните данни се използват за различна цел. Операциите по обработване на данни могат да се развият бързо и могат да възникнат нови слабости. Поради това следва да се отбележи, че преразглеждането на ОВЗД не само е от полза за постигането на постоянни подобрения, но е от решаващо значение за поддържането на същото равнище на защита на данните в условията на променяща се с времето среда. ОВЗД може да стане необходима и поради промяна в организационния или обществения контекст за дейността по обработване, например защото последиците от определени автоматизирани решения са станали по-сериозни или защото нови категории субекти на данни са станали уязвими на дискриминация. Всеки от тези примери би могъл да представлява елемент, който води до промяна на риска, произтичащ от съответната дейност по обработване.

От друга страна някои промени също така биха могли да понижат риска. Например дадена операция по обработване може да се развие по такъв начин, че решенията вече да не са автоматизирани или, в случай на дейност по наблюдение, то вече да не е систематично. В такъв случай преразглеждането на извършения анализ на риска може да покаже, че вече не се изисква извършване на ОВЗД.

Съгласно добрата практика **ОВЗД следва постоянно да се преразглежда и да подлежи на редовна повторна оценка.** Поради това дори ако към 25 май 2018 г. не се изисква ОВЗД, в подходящ момент администраторът ще трябва да извърши такава ОВЗД като част от общите си задължения за отчетност.

Г. <u>Как следва да бъде извършена ОВЗД?</u>

а) В кой момент следва да бъде извършена ОВЗД? Преди да бъде извършено обработването.

[22] От гледна точка на контекста, събраните данни, целите, функциите, обработените лични данни, получателите, комбинациите от данни, рисковете (помощни елементи, източници на риск, потенциални въздействия, заплахи и др.), мерките за сигурност и международното предаване на данни.

ОВЗД следва да бъде извършена „*преди да бъде извършено обработването*“ (член 35, параграфи 1 и 10, съображения 90 и 93)[23]. Това съответства на принципите за защита на данните на етапа на проектирането и по подразбиране (член 25 и съображение 78). ОВЗД следва да се разглежда като инструмент, който подпомага вземането на решения относно обработването.

Извършването на ОВЗД следва да започне на възможно най-ранен етап от проектирането на операцията по обработване, дори ако някои от операциите по обработване все още не са известни. Актуализирането на ОВЗД през целия жизнен цикъл на проекта ще гарантира, че се отчитат защитата на данните и неприкосновеността на личния живот, което ще стимулира създаването на решения, с които се насърчава спазването. Освен това е възможно да бъде необходимо да се повторят отделните стъпки от оценката с напредването на процеса по разработване, защото подборът на определени технически или организационни мерки може да окаже въздействие върху тежестта и вероятността на рисковете, породени от обработването.

Фактът, че може да се наложи актуализиране на ОВЗД след реалното започване на обработването, не е основателна причина да се отложи или да не се извърши ОВЗД. ОВЗД е текущ процес, особено когато операцията по обработване е динамична и подлежи на текущи промени. **Извършването на ОВЗД е постоянен процес, а не еднократно действие**.

б) Кой е длъжен да извърши ОВЗД? Администраторът, заедно с длъжностното лице по защита на данните и обработващите лични данни.

Администраторът носи отговорност да гарантира, че се извършва ОВЗД (член 35, параграф 2). ОВЗД може да бъде извършена от друго лице в рамките на организацията или извън нея, но администраторът продължава да носи крайната отговорност за тази задача.

Администраторът също така трябва да поиска становището на длъжностното лице по защита на данните (ДЛЗД), когато такова е определено (член 35, параграф 2), като това становище и взетите от администратора решения следва да се документират в ОВЗД. ДЛЗД също така следва да наблюдава извършването на ОВЗД (член 39, параграф 1, буква в). Насоките на РГ29 относно длъжностните лица по защита на данните, 16/EN WP 243, съдържат допълнителни указания.

Ако обработването се извършва изцяло или частично от обработващ лични данни, **обработващият лични данни следва да подпомага администратора при извършването на ОВЗД** и да предостави цялата необходима информация (в съответствие с член 28, параграф 3, буква е).

Администраторът трябва да „*се обръща към субектите на данните или техните представители за становище*“ (член 35, параграф 9), „*когато е целесъобразно*“. РГ29 счита, че:

- тези становища биха могли да се потърсят по редица начини в зависимост от контекста (например общо проучване, свързано с целта и средствата на операцията по обработване, отправяне на въпрос към представителите на персонала или обичайните анкети, които се изпращат на бъдещите клиенти на администратора), за да се гарантира,

[23] Освен когато става въпрос за вече съществуващо обработване, което е било проверено преди това от надзорния орган, като в този случай ОВЗД следва да бъде извършена преди осъществяването на значителни промени.

че администраторът разполага със законно основание да обработва личните данни, с които е свързано търсенето на такива становища. Въпреки това следва да се отбележи, че съгласието за обработване на данните очевидно не представлява начин да се потърсят становищата на субектите на данни;
- ако окончателното решение на администратора се различава от становищата на субектите на данни, неговите причини да обработи данните или не следва да бъдат документирани;
- администраторът също така следва да документира своята обосновка да не потърси становищата на субектите на данни, ако реши, че това не е целесъобразно, например ако това би изложило на риск поверителността на бизнес плановете на дружеството или би било непропорционално или непрактично.

На последно място, добра практика представлява определянето и документирането на други специфични роли и отговорности в зависимост от вътрешната политика, процеси и правила, например:

- когато конкретни звена на дружеството могат да предлагат извършването на ОВЗД, тези звена следва впоследствие да предоставят данни за ОВЗД и да участват в процеса по валидиране на ОВЗД;
- по целесъобразност се препоръчва да се поиска становището на независими експерти от различни области[24] (адвокати, ИТ експерти, експерти по сигурността, социолози, експерти по етични стандарти и др.);
- ролите и отговорностите на обработващите лични данни трябва да бъдат определени в договор; и ОВЗД трябва да бъде извършена с помощта на обработващия лични данни, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни (член 28, параграф 3, буква е);
- главният служител по сигурността на информацията (ГССИ), ако е назначен такъв, и ДЛЗД биха могли да предложат на администратора да извърши ОВЗД по отношение на конкретна операция по обработване и следва да помогнат на заинтересовани страни с методологията, да подпомогнат оценяването на качеството на оценката на риска и на въпроса дали остатъчният риск е приемлив, както и да се стремят към развиване на специфични познания за контекста, в който работи администраторът;
- главният служител по сигурността на информацията (ГССИ), ако е назначен такъв, и/или ИТ отделът следва да съдействат на администратора и биха могли да предложат извършването на ОВЗД по отношение на конкретна операция по обработване в зависимост от свързаните със сигурността или оперативните потребности.

в) Каква е методологията за извършване на ОВЗД? Различни методологии, но общи критерии.

В ОРЗД се определят минималните характеристики на ОВЗД (член 35, параграф 7 и съображения 84 и 90):

- *„опис на предвидените операции по обработване и целите на обработването“;*
- „*оценка на необходимостта и пропорционалността на операциите по обработване*“;
- „*оценка на рисковете за правата и свободите на субектите на данни*“;
- *мерките, предвидени за:*

[24] *Recommendations for a privacy impact assessment framework for the European Union (Препоръки за рамка на Европейския съюз за оценка на въздействието върху неприкосновеността на личния живот), документ D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

- „*справяне с рисковете*“;
- „*демонстриране на спазването на настоящия регламент*“.

Следната фигура илюстрира общия повтарящ се процес за извършване на ОВЗД[25]:

Спазването на кодекс за поведение (член 40) трябва да се вземе предвид (член 35, параграф 8), когато се оценява въздействието на дадена операция по обработване на данни. Това може да бъде от полза, за да се демонстрира, че са избрани или въведени подходящи мерки, при условие че кодексът за поведение е подходящ за операцията по обработване. Под внимание следва да се вземат и сертификатите, печатите и маркировките с цел да се демонстрира спазването на ОРЗД при операциите по обработване от страна на администраторите и обработващите лични данни (член 42), както и задължителните фирмени правила (ЗФП).

Всички съответни изисквания, определени в ОРЗД, осигуряват широка и обща рамка за планиране и извършване на ОВЗД. Практическото извършване на ОВЗД ще зависи от

[25] Следва да се подчертае, че описаният тук процес се повтаря: на практика съществува вероятност всеки от етапите да се повтори многократно преди приключването на ОВЗД.

изискванията, определени в ОРЗД, които могат да бъдат допълнени от по-подробни практически насоки. Поради това извършването на ОВЗД е с променлив мащаб. Това означава, че дори администратор на малък обем данни може да планира и извърши ОВЗД, която е подходяща за неговите операции по обработване.

В съображение 90 от ОРЗД се описват редица елементи на ОВЗД, които се припокриват с добре определени елементи от управлението на риска (например ISO 31000[26]). От гледна точка на управлението на риска ОВЗД е насочена към „управление на рисковете“ за правата и свободите на физическите лица, като се използват следните процеси:

- установяване на контекста: „*като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска*“;
- оценка на рисковете: „*за да се оценят конкретната вероятност и тежестта на високия риск*“;
- третиране на рисковете: „*ограничаване на този риск*“ и „*с които се осигурява защитата на личните данни*“ и „*се доказва съответствието с настоящия регламент*“.

Забележка: ОВЗД съгласно ОРЗД представлява инструмент за управление на рисковете за правата на субектите на данни и поради това отразява тяхната гледна точка, какъвто е случаят в определени области (например сигурност на обществото). От друга страна управлението на риска в други области (например информационната сигурност) е насочено към организацията.

ОРЗД осигурява гъвкавост на администраторите да определят конкретната структура и форма на ОВЗД, за да може тя да съответства на съществуващите работни практики. В рамките на ЕС и по света са установени редица различни процеси, при които се отчитат елементите, описани в съображение 90. При все това независимо от формата ОВЗД трябва да представлява действителна оценка на рисковете, която позволява на администраторите да въведат мерки за справяне с тях.

Биха могли да се използват различни методологии (вж. приложение 1 за примери за методологии за оценка на въздействието върху защитата на данни и неприкосновеността на личния живот), които да подпомогнат изпълнението на основните изисквания, определени в ОРЗД. За да се позволи съществуването на тези различни подходи и същевременно да се позволи на администраторите да спазват ОРЗД, са определени общи критерии (вж. приложение 2). Те поясняват основните изисквания на Регламента, но осигуряват достатъчно широк обхват за различни форми на изпълнение. Тези критерии могат да се използват, за да се демонстрира, че дадена методология за ОВЗД отговаря на стандартите, изисквани съгласно ОРЗД. **Администраторът сам избира методология, но тази методология следва да бъде в съответствие с критериите, посочени в приложение 2**.

РГ29 насърчава разработването на специфични за отделните сектори рамки за ОВЗД. Причината за това е, че тези рамки могат да се основават на специфични знания в отделните сектори, което означава, че ОВЗД може да бъде насочена към специфичните особености на конкретен вид операция по обработване (например конкретни видове данни, корпоративни активи, потенциални въздействия, заплахи, мерки). Това означава, че ОВЗД може да бъде насочена към въпроси, които

[26] Процедури за управление на риска: комуникация и консултация, установяване на контекста, управление на риска, третиране на риска, наблюдение и преглед (вж. терминологията и определенията, както и съдържанието в предварителния преглед на ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

възникват в конкретен икономически сектор или при използването на конкретни технологии или извършването на конкретни видове операции по обработване.

На последно място, при необходимост „*администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване*“ (член 35, параграф 11[27]).

г) Има ли задължение за публикуване на ОВЗД? Не, но публикуването на резюме би могло да повиши доверието, а пълната ОВЗД трябва да бъде съобщена на надзорния орган в случай на предварителна консултация или ако бъде поискана от ОЗД.

ОРЗД не включва правно изискване за публикуването на ОВЗД, администраторът сам решава дали да направи това. При все това администраторите следва да обмислят публикуването най-малкото на части от оценката, например на резюме или на заключението от своята ОВЗД.

Целта на този процес е да се подпомогне изграждането на доверие в извършваните от администратора операции по обработване и да се демонстрира отчетност и прозрачност. Особено добра практика е да се публикува ОВЗД, когато гражданите са засегнати от операцията по обработване. Такъв би могъл да бъде случаят по-специално когато публичен орган извършва ОВЗД.

Не е нужно публикуваната ОВЗД да съдържа цялата оценка, особено когато в ОВЗД се представя специфична информация, свързана с рисковете за сигурността на администратора, или когато по този начин биха могли да се разкрият търговски тайни или търговска информация с чувствителен характер. В тези обстоятелства публикуваната версия би могла да се състои просто от резюме на основните констатации на ОВЗД или дори само от изявление, че е извършена ОВЗД.

Освен това, когато ОВЗД покаже високи остатъчни рискове, администраторът ще бъде задължен да се консултира предварително с надзорния орган по отношение на обработването (член 36, параграф 1). Като част от тази процедура трябва да се предостави пълната версия на ОВЗД (член 36, параграф 3, буква д). Надзорният орган може да предостави становище[28], без да разкрива тайни или да оповестява слабости по отношение на сигурността, съгласно приложимите в съответната държава членка принципи относно публичния достъп до официални документи.

Д. <u>Кога се осъществява консултация с надзорния орган? Когато остатъчните рискове са високи.</u>

Както е обяснено по-горе:

- ОВЗД се изисква, когато съществува вероятност обработването „*да породи висок риск за правата и свободите на физическите лица*“ (член 35, параграф 1, вж. III.Б.а). Например се счита, че съществува вероятност мащабното обработване на здравни данни да породи висок риск и при него се изисква ОВЗД;
- в такъв случай администраторът носи отговорност за оценка на рисковете за правата и свободите на субектите на данни и да определи мерки[29], предвидени за намаляване на тези

[27] В член 35, параграф 10 изрично се изключва единствено прилагането на член 35, параграфи 1—7.

[28] Даването на писмено становище на администратора е необходимо само когато надзорният орган е на мнение, че планираното обработване не е в съответствие с разпоредбите, посочени в член 36, параграф 2.

[29] Включително като взема предвид съществуващите насоки от ЕКЗД и надзорните органи и като взема предвид достиженията на техническия прогрес и разходите за прилагане, както е определено в член 35, параграф 1.

рискове до приемливо равнище и за демонстриране на спазването на ОРЗД (член 35, параграф 7, вж. III.В.в). Пример за това би било при съхранението на лични данни на преносими компютри да се прилагат подходящи технически и организационни мерки за сигурност (пълно криптиране на диска, надеждно управление на ключове, подходящ контрол на достъпа, резервни копия на сигурно място и др.) в допълнение към съществуващите политики (известие, съгласие, право на достъп, право на възражение и др.).

Ако в примера с преносимите компютри по-горе е било счетено, че администраторът е намалил рисковете в достатъчна степен, и след отчитане на член 36, параграф 1 и съображения 84 и 94 обработването може да започне без консултация с надзорния орган. Администраторът трябва да се консултира с надзорния орган именно в случаите, когато администраторът не може да намали идентифицираните рискове в достатъчна степен (т.е. остатъчните рискове продължават да бъдат високи).

Примерите за неприемливо висок остатъчен риск включват случаи, в които за субектите на данни могат да настъпят значителни или дори необратими последици, които те не могат да преодолеят (например незаконен достъп до данни, който води до заплаха за живота на субектите на данни, съкращение, финансов риск), и/или когато изглежда очевидно, че рискът ще се материализира (например при невъзможност да се намали броят на лицата, които осъществяват достъп до данните, в резултат на начините на споделяне, използване или разпространение или когато не се отстрани известна слабост).

Консултация с надзорния орган се изисква всеки път, когато администраторът не може да установи достатъчни мерки за намаляване на рисковете до приемливо равнище (т.е. остатъчните рискове продължават да бъдат високи)[30].

Освен това администраторът ще трябва да се консултира с надзорния орган всеки път, когато правото на държавите членки изисква от администраторите да се консултират с надзорния орган и/или да получават предварително разрешение от него във връзка с обработването от администратор за изпълнението на задача, осъществявана от администратора в полза на обществения интерес, включително обработване във връзка със социалната закрила и общественото здраве (член 36, параграф 5).

Следва обаче да се посочи, че независимо дали се изисква консултация с надзорния орган въз основа на равнището на остатъчния риск или не, продължават да важат задълженията да се поддържа документация за ОВЗД и своевременно да се актуализира ОВЗД.

IV. Заключения и препоръки

ОВЗД представляват полезен начин за администраторите да прилагат системи за обработване на данни, които са в съответствие с ОВЗД, и могат да бъдат задължителни за някои видове операции по обработване. Те са с променлив мащаб и могат да приемат различна форма, но в ОРЗД се определят основните изисквания за ефективна ОВЗД. Администраторите следва да

[30] Забележка: „*псевдонимизирането и криптирането на лични данни*“ (както и свеждането до минимум на данните, механизмите за надзор и др.) не представляват непременно подходящи мерки. Това са само примери. Подходящите мерки зависят от конкретния контекст и рисковете във връзка с операциите по обработване.

гледат на извършването на ОВЗД като на полезна и положителна дейност, която подпомага спазването на законовите разпоредби.

В член 24, параграф 1 се определя основната отговорност на администратора от гледна точка на спазването на ОРЗД: „*Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират.“*

ОВЗД представлява ключова част от спазването на Регламента, когато се планира или се извършва обработване с висок риск. Това означава, че администраторите следва да използват критериите, определени в настоящия документ, за да определят дали трябва да се извърши ОВЗД или не. Съгласно вътрешната политика на администратора този списък би могъл да се разшири отвъд правните изисквания на ОРЗД. Това следва да доведе до повишено доверие и увереност от страна на субектите на данни и другите администратори на данни.

Когато се планира обработване с вероятност от висок риск, администраторът трябва:

- да избере методология за ОВЗД (в приложение 1 са дадени примери), която отговаря на критериите в приложение 2, или да определи и изпълнява систематичен процес за ОВЗД, който:
  - отговаря на критериите в приложение 2;
  - е интегриран в съществуващите процеси във връзка с планирането, разработването, промените, риска и оперативния преглед в съответствие с вътрешните процеси, контекста и културата;
  - включва съответните заинтересовани страни и ясно определя техните отговорности (администратор, ГССИ, субекти на данни или техни представители, бизнес, техническо обслужване, обработващи лични данни, служител по сигурността на информацията и др.);
- да предостави доклада от ОВЗД на компетентния надзорен орган, когато е длъжен;
- да се консултира с надзорния орган, когато не успее да определи достатъчни мерки за ограничаване на високите рискове;
- да извършва периодичен преглед на ОВЗД и на обработването, което се оценява чрез нея, най-малкото когато настъпи промяна на риска, породен от операцията по обработване;
- да документира взетите решения.

Приложение 1 — Примери за съществуващи рамки за ОВЗД в ЕС

В ОРЗД не се уточнява какъв процес за ОВЗД трябва да се следва, а вместо това на администраторите се позволява да въведат рамка, която допълва съществуващите им работни практики, при условие че в нея се отчитат елементите, описани в член 35, параграф 7. Тази рамка може да бъде съобразена със специфичните нужди на администратора или да е обща за съответния сектор. Публикуваните преди това рамки, разработени от ОЗД в ЕС, и рамките на специфични сектори в ЕС включват (но не са ограничени до):

Примери за общи рамки в ЕС:

- Германия: стандартен модел за защита на данните, V.1.0 — пробна версия, 2016 г.[31] https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- Испания: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014 г. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- Франция: *Оценка на въздействието върху неприкосновеността на личния живот (ОВНЛЖ)*, Commission nationale de l'informatique et des libertés (CNIL), 2015 г. https://www.cnil.fr/fr/node/15798
- Обединено кралство: *Кодекс на практиката за провеждане на оценка на въздействието върху неприкосновеността на личния живот*, Служба на комисаря по информацията (ICO), 2014 г. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Примери за специфични за отделните сектори рамки в ЕС:

- Рамка за оценка на въздействието върху защитата на данни и неприкосновеността на личния живот за приложения, използващи радиочестотна идентификация[32]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Модел за оценка на въздействието върху защитата на данните за интелигентни електроенергийни мрежи и интелигентни измервателни системи[33]. http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Освен това ще бъде изготвен международен стандарт, който също ще осигурява насоки за методологиите, използвани при извършването на ОВЗД (ISO/IEC 29134[34]).

---

[31] Единодушно приет и утвърден (Бавария гласува „въздържал се“) с 92 гласа. Конференция на независимите органи за защита на данните на федерално и провинциално ниво в Кюлунгсборн на 9—10 ноември 2016 г.

[32] Вж. също:

- Препоръка на Комисията от 12 май 2009 г. относно спазването на принципите за неприкосновеност на личния живот и защита на данните в приложения, използващи радиочестотна идентификация. https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Становище 9/2011 относно преработеното предложение на индустрията за Рамка за оценка на въздействието на приложения с радиочестотна идентификация върху неприкосновеността на личния живот и защитата на данните. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_bg.pdf

[33] Вж. също така Становище 07/2013 относно модела за оценка на въздействието върху защитата на данните за интелигентни електроенергийни мрежи и интелигентни измервателни системи („модела за ОВЗД“), изготвен от Експертна група 2 на Работната група на Комисията за интелигентни електроенергийни мрежи. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_bg.pdf

Приложение 2 — Критерии за приемлива ОВЗД

РГ29 предлага следните критерии, които администраторите могат да използват, за да оценят дали ОВЗД или методология за извършване на ОВЗД е достатъчно всеобхватна, така че да отговаря на ОРЗД:

- ☐ осигурен е системен опис на обработването (член 35, параграф 7, буква а):
  - ☐ вземат се предвид естеството, обхватът, контекстът и целите на обработването (съображение 90);
  - ☐ поддържа се регистър на личните данни, получателите и срока, за който ще се съхраняват личните данни;
  - ☐ осигурено е функционално описание на операцията по обработване;
  - ☐ определени са елементите, свързани с личните данни (хардуер, софтуер, мрежи, лица, хартиен носител или канали за предаване на хартиен носител);
  - ☐ взема се предвид спазването на одобрени кодекси за поведение (член 35, параграф 8);
- ☐ оценяват се необходимостта и пропорционалността (член 35, параграф 7, буква б)):
  - ☐ определени са мерки за спазване на Регламента (член 35, параграф 7, буква г) и съображение 90), като се вземат предвид:
    - ☐ мерки, допринасящи за пропорционалността и необходимостта на обработването въз основа на:
      - ☐ конкретна, изрично указана и легитимна цел или цели (член 5, параграф 1, буква б);
      - ☐ законосъобразност на обработването (член 6);
      - ☐ подходящи, свързани със и ограничени до необходимото данни (член 5, параграф 1, буква в);
      - ☐ ограничена продължителност на съхранението (член 5, параграф 1, буква д);
    - ☐ мерки, допринасящи за правата на субектите на данни:
      - ☐ информиране на субекта на данни (членове 12, 13 и 14);
      - ☐ право на достъп и на преносимост на данните (членове 15 и 20);
      - ☐ право на коригиране и на изтриване (членове 16, 17 и 19);
      - ☐ право на възражение и на ограничаване на обработването (членове 18, 19 и 21);
      - ☐ взаимоотношения с обработващите лични данни (член 28);
      - ☐ гаранции при международно предаване на данни (глава V);
      - ☐ предварителна консултация (член 36).
- ☐ управляват се рисковете за правата и свободите на субектите на данни (член 35, параграф 7, буква в)):
  - ☐ оценяват се произходът, естеството, спецификата и степента на рисковете (вж. съображение 84), или по-конкретно за всеки риск, (незаконен достъп, нежелани изменения и изчезване на данни) от гледна точка на субектите на данни:
    - ☐ вземат се предвид източниците на риска (съображение 90);
    - ☐ определят се потенциалните въздействия върху правата и свободите на субектите на данни в случай на определени събития, включително незаконен достъп, нежелани изменения и изчезване на данни;
    - ☐ определят се заплахи, които биха могли да доведат до незаконен достъп, нежелани изменения и изчезване на данни;
    - ☐ изчисляват се вероятността и тежестта (съображение 90);

[34] ISO/IEC 29134 (проект), *Информационни технологии. Техники за сигурност. Оценка на въздействието върху неприкосновеността на личния живот. Указания*, Международна организация по стандартизация (ISO).

- ☐ определят са мерки за третиране на тези рискове (член 35, параграф 7, буква г) и съображение 90);
- ☐ заинтересованите страни участват:
  - ☐ иска се становището на ГССИ (член 35, параграф 2);
  - ☐ по целесъобразност се търсят становищата на субектите на данни или техните представители (член 35, параграф 9).