|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Версия** | **Дата** | **Описание** | **Автор** | **Одобрил** |
|  |  |  |  |  |

1. Предназначение на процедурата

Всички дейности и проекти, осъществявани от ПАТО ЕООД, които предвиждат обработка на лични данни, са предмет на предварителна оценка на риска. Когато тази оценка покаже, че съществува вероятност обработването да породи висок риск за правата и свободите на субектите на данни, преди да извърши обработването, ПАТО ЕООД извършва също и оценка на въздействието върху защитата на данните (ОВЗД) съгласно изискванията на тази процедура.

Освен при идентифициране на висок риск, ОВЗД се извършва задължително и в изброените в [член 35, параграф 3 от ОРЗД](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art35) случаи:

* когато се извършва 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;
* при мащабно обработване на „чувствителни“ лични данни или на лични данни за присъди и нарушения;
* при систематично мащабно наблюдение на публично достъпна зона.

ОВЗД е задължителна също и за видовете операции по обработване, посочени в списък, приет и оповестен от националния надзорен орган ([чл. 35, пар. 4 от ОРЗД](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art35)).

1. Нормативна уредба

* [Член 35](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art35) и [член 36](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art36) от Общия регламент за защита на данните (ОРЗД)
* [Насоки](https://web.apis.bg/e.php?i=651194) 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[[1]](#footnote-2)

1. Задължения и роли

Длъжностното лице по защита на данните / Отговорникът по защита на данните отговаря за извършването на необходимите проверки[[2]](#footnote-3) на личните данни, чиято цел е да се установи нуждата от провеждане на ОВЗД.

Управителят, който е длъжностното лице, което отговаря за управление на риска заедно с Длъжностното лице по защита на данните / Отговорникът по защита на данните споделят отговорността за вземането на подходящи мерки за ограничаване на всички рискове, идентифицирани в процеса на оценка на въздействието, и за вземането на последващо решение за започване, респ. продължаване на обработката.

Лицата, ръководещи отделните процеси по обработка на данните в организацията- , Главният счетоводител, Началник складовете, Отговорникът по здравословни и безопасни условия на труд, служителите по обработка на данни на контрагенти , са отговорни за своевременното известяване на Управителя и Длъжностното лице по защита на данните / Отговорника по защита на данните и за съвместното вземане на решения във връзка с възникнали рискове за сигурността на личните данни.

1. Ход на процедурата
2. **Анализ на рисковете и оценка на въздействието**

При започването на всяка дейност или проект Длъжностното лице по защита на данните / Отговорникът по защита на данните или Ръководителят на съответната дейност извършва оценка на риска съгласно изискванията на приетата в организацията на ПАТО ЕООД методология за ОВЗД[[3]](#footnote-4), като взема предвид вида на личните данни и начините за обработването им.

Администраторът въвежда методологична рамка, която допълва съществуващите му работни практики, при условие че в нея се отчитат елементите, описани в [член 35, параграф 7 от ОРЗД](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art35).  Администраторът сам избира методология, но тази методология следва да бъде в съответствие с критериите, посочени в Приложение 2 от [Насоките](https://web.apis.bg/e.php?i=651194). Тези критерии се използват от администратора, за да оцени дали извършената от него ОВЗД, респ. използваната от него методология за извършване на ОВЗД е достатъчно всеобхватна, така че да отговаря на [ОРЗД](https://web.apis.bg/e.php?celex=32016R0679).

Въпреки че все още не е приведена в съответствие с ОРЗД, приетата от българския надзорен орган – Комисията за защита на личните данни, [Наредба № 1](https://web.apis.bg/p.php?Base=NARH&DocCode=83626) от 30.01.2013 г. [[4]](#footnote-5), е добра основа за разработването на методология за ОВЗД от администратора. Съгласно [Наредба № 1](https://web.apis.bg/p.php?Base=NARH&DocCode=83626), администраторът извършва ОВЗД с цел определяне на адекватно ниво на технически и организационни мерки за защита на личните данни, което отговаря на обработваните от него лични данни и въздействието при нарушаване на защитата им.

Оценката на въздействието е процес, при който администраторът преценява нивата на рисковете за правата и свободите на субектите на данни. Водещ критерий при тази преценка е степента (нивото) на въздействие, което нарушаването на поверителността, цялостността или наличността на личните данни би оказало върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица ([чл. 11, ал. 2 от Наредба № 1](https://web.apis.bg/p.php?Base=NARH&DocCode=83626&ToPar=Art11)).

В съответствие с това, администратора анализира вероятността за възникване на нарушение на сигурността на данните и да определи 4 нива на въздействие – ниско, средно, високо и изключително високо.

При извършването на ОВЗД, администраторът използва следната матрица за степенуване на въздействието (риска), отчитаща вероятността за настъпване на съответното нарушение на сигурността на данните и величината на потенциалните неблагоприятни последици (вреди):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Последици** | | | |
| **Ограничени** | **Средни** | **Тежки** | **Много тежки** |
| **Вероятност** | **Малка** | **Ниско**  **- 1 -** | **Средно**  **- 4 -** | **Средно**  **- 6 -** | **Високо**  **- 10 -** |
| **Средна** | **Ниско**  **- 2 -** | **Средно**  **- 5 -** | **Високо**  **- 8 -** | **Изключително високо**  **- 11 -** |
| **Висока** | **Средно**  **- 3 -** | **Високо**  **- 7 -** | **Високо**  **- 9 -** | **Изключително високо**  **- 12 -** |

При определянето на степента на риска ПАТО ЕООД се ръководи от критериите за вероятен „висок риск“ на [член 35, параграф 3 от ОРЗД](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art35) и [Насоките[[5]](#footnote-6)](https://web.apis.bg/e.php?i=651194). Наред с преките рискове за правата и свободите на физическите лица, произтичащи от обработката на лични данни, организацията отчита също и рисковете за бизнеса (репутационни, правни и т.н.), както и целите и задълженията на самата организация (регулаторни и договорни).

В зависимост от определеното ниво на въздействие, администраторът извършва

1) приоритизация на идентифицираните рискове,

2) определя адекватно ниво на защита, включващо техническите и организационни мерки, които трябва да предприеме за тяхното ограничаване.

Редът на приоритет на идентифицираните рискове е, както следва:

1. Рисковете с висока тежест на последиците и вероятност за настъпване (8, 9, 11 и 12) трябва да бъдат напълно избегнати или ограничени чрез прилагане на мерки за сигурност, които намаляват както тежестта им, така и тяхната вероятност. В плана за управление на рисковете следва да се предвидят както мерки за предотвратяване (действия, предприети преди вредно събитие), така и за защита (действия, предприети по време на вредно събитие) и възстановяване (действия, предприети след вредно събитие).
2. Рисковете с висока тежест, но с малка вероятност (6, 10) трябва да се избягват или ограничават чрез прилагане на мерки за сигурност, които намаляват тежестта на последиците или вероятността за настъпването им. Приоритет следва да имат преди всичко на мерките за предотвратяване (превантивните мерки).
3. Рисковете с малка тежест, но с голяма вероятност за настъпване (3, 7), трябва да бъдат ограничавани чрез прилагане на мерки за сигурност, които намаляват тяхната вероятност. Трябва да се наблегне обаче на мерките за възстановяване.
4. Рискове с ниска тежест и вероятност (1, 2, 4, 5) могат да бъдат третирани на по-късен етап, още повече че прилагането на мерките спрямо рисковете с по-висок приоритет може да доведе до тяхното елиминиране или значително ограничаване.

В зависимост от приоритизацията на рисковете и идентифицираното ниво на въздействие, ПАТО ЕООД определя съответно ниво на защита – ниско, средно, високо или изключително високо, както и организационните и технически мерки, адекватни на така определеното ниво.

Минимално необходимото съдържание на ОВЗД е:

* системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
* оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
* оценка на рисковете за правата и свободите на субектите на данни; и
* 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 ОРЗД.

Заедно с определянето на мерки за елиминирането или ограничаването на съществуващите рискове, ПАТО ЕООД посочва лице, което отговаря за изпълнението на мерките и определя срок за изпълнението.

Накрая, след консултация с Длъжностното лице по защита на данните / Отговорника по защита на данните, ПАТО ЕООД одобрява и подписва ОВЗД за всяка подлежаща на оценка на въздействието дейност/проект по обработка на лични данни.

Освен при започване на нова дейност/проект, ПАТО ЕООД прави преглед за необходимостта от извършване на оценка на въздействието и при всяка промяна в риска, с който са свързани вече съществуващи операции по обработване

ОВЗД следва постоянно да се преразглежда и да подлежи на редовна повторна оценка.

Пълният цикъл на повтарящия се процес на извършване на ОВЗД е онагледен със следната илюстрация:



1. **Записи в Регистъра на дейностите по обработване**

ПАТО ЕООД записва информация за всички лични данни, включително разпознатите като „рискови“, обработвани в рамките на всяка отделна дейност/проект, и за всички процеси, свързани с тази дейност/проект в Регистъра на дейностите по обработване.

Това включва описание на обработката и целите за които се извършва, законоустановените интереси, преследвани от администратора, оценка на необходимостта и пропорционалността на обработката на данните, категорията на данните (общи, специални, отнасящи се до дете), формáта на данните, оценка на рисковете за правата и свободите на субектите на данни (съгласно схемата и определенията за нивото на въздействие, посочени по-горе). В Регистъра на дейностите по обработване се вписват също така всички видове операции по обработката на данните – събиране, прехвърляне, съхранение, достъп, изтриване. След извършването на ОВЗД, в Регистъра на дейностите по обработване са вписват данни и за определеното адекватно ниво на защита и набелязаните организационни и технически мерки за елиминиране или ограничаване на рисковете.

С оглед на идентифицираното основание за обработка на данните, ПАТО ЕООД определя и записва в Регистъра на дейностите по обработване съответния период на съхранение (в съответствие с Процедура за съхраняване и унищожаване на данните (GDPR\_PROC\_07)).

Организацията определя и посочва в Регистъра на дейностите по обработване кои лица имат достъп до данните (физически лица, работни екипи, организационни звена, трети лица) и/или кои лица участват в обработката на личните данни, включително географското местоположение на мястото на извършване на обработката, както и дали се извършва трансгранична обработка.

1. **Предварителна консултация**

Когато в резултат на извършена ОВЗД преди започването на обработката на лични данни ПАТО ЕООЕустанови, че обработката им ще доведе до висок риск за субектите на данни и че не е могъл да идентифицира адекватни мерки за ограничаване и контрол на риска, организацията се консултира с надзорния орган (за България КЗЛД) съгласно изискванията на [чл. 36 от ОРЗД](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art36).

Когато поиска консултация от надзорния орган, ПАТО ЕООД му предоставя следната информация:

* информация за съответните отговорности на администратора, съвместните администратори и обработващите лични данни, които се занимават с обработването
* целите на планираното обработване и средствата за него;
* предвидените мерки и гаранции за защита на правата и свободите на субектите на данни;
* (доколкото е приложимо) координатите за връзка на длъжностното лице по защита на данните;
* копие от ОВЗД, както и
* всякаква друга информация, поискана от надзорния орган.

1. Приети от Работната група по член 29 на 04.04.2017 г. По-нататък се реферират за краткост само като „Насоки“. [↑](#footnote-ref-2)
2. В зависимост от използваната в организацията методология за оценка на въздействието (методология за ОВЗД). [↑](#footnote-ref-3)
3. Общият регламент за защита на данните и Насоките разглеждат ОВЗД изцяло в контекста на общото задължение на администраторите да управляват по подходящ начин рисковете, породени от обработването на данни. С оглед на това, методологията за оценка на риска е неразделна част от методологията за ОВЗД. [↑](#footnote-ref-4)
4. Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, издадена от КЗЛД, обн., ДВ, бр. 14 от 12.02.2013 г. [↑](#footnote-ref-5)
5. В Насоките да дадени примери за начина на използване на критериите, за да се оцени дали конкретна операция по обработване изисква ОВЗД. [↑](#footnote-ref-6)