**УТВЪРЖДАВАМ:**
*/ утвърдени със Заповед № РД-14-103 /21.06.2021 г./*

**ЛАЗАР МИЧЕВ**
**АДМИНИСТРАТИВЕН РЪКОВОДИТЕЛ-ПРЕДСЕДАТЕЛ**
**ОКРЪЖЕН СЪД ГРАД РАЗГРАД**

# ПРОЦЕДУРА ЗА ОЦЕНКА НА РИСКА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

## 1. ЦЕЛИ

Настоящата процедура има за цел да определи реда и отговорностите в процеса по оценка на въздействието на дадена обработка върху личните данни. Да оцени произлизащите от обработката рискове за организацията, и правата и свободите на субектите на данни. Да осигури адекватна защита на конфиденциалността, целостта и наличността на личните данни, администрирани от организацията.

## 2. ОБХВАТ

Процедурата обхваща процесите по оценка на риска за ЛД, администрирани от организацията, попадащи в обхвата на Общия регламент за защита на данните /ОРЗД/GDPR/.

## 3. ОТГОВОРНОСТИ

Настоящата процедура се прилага от съдебния администратор и служителя изпълняващ длъжностно лице по защита на личните данни /DPO/.

Пряка отговорност за прилагане и спазване на настоящата процедура носят лицата от организацията, както следва:

• Председател за непрекъснат контрол на процесите и осигуряване на необходимите ресурси;

• Длъжностно лице по защита на ЛД за оказване на контрол и методическа помощ в съда и пряко управление на процесите в неговите правомощия и функционални задължения;

## 4. ТЕРМИНОЛОГИЯ И СЪКРАЩЕНИЯ

•Организацията – Окръжен съд Разград

•ДЛЗЛД - Длъжностно лице по защита на личните данни

• ЛД – Лични данни

•GDPR – General Data Protection Regulation /Общ регламент за защита на данните/

## 5.2.ОПРЕДЕЛЕНИЕ ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ,

Оценка на въздействието върху защитата на данните е процес, чиято цел е да опише обработването на ЛД, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на субектите на данни, произтичащи от това обработването, като ги оцени и определи мерки за справяне с тези рискове. Този процес е важен инструмент за отчетност, тъй като помага на организацията да е в съответствие с изискванията на GDPR и да демонстрира, че са предприети подходящи мерки за непрекъснатото гарантиране на това съответствие. Типовете ЛД, обработвани и администрирани от ОС Разград могат да бъдат:

• ***Общи лични данни*** - означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

• ***Чувствителни лични данни*** - разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

**Сигурността на ЛД се характеризира като запазване на:**

• ***Конфиденциалност:*** - ЛД са достъпни само за тези, които са упълномощени да имат достъп до тях;

• ***Цялостност:*** гарантиране на точността и пълнотата на ЛД и на методите за тяхната обработка;

• ***Наличност:*** винаги, когато е необходимо упълномощените потребители имат наличен достъп до ЛД;

• ***Правно съответствие:*** ЛД се обработват в съответствие с изискванията на GDPR. Съгласно GDPR, ако не бъде извършен процеса на оценяване при обработването на ЛД, ако бъде извършена неправилно или ако не бъде проведена консултация с компетентния надзорен орган (КЗЛД), когато това се изисква, това може да доведе до налагане на административна глоба на организацията.

## 5.3.ОБХВАТ НА ПРОЦЕСА ПО ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

При оценяването се въвеждат подходящи мерки, за да се гарантира и докаже спазването на GDPR, като взема предвид рисковете с различна вероятност и тежест за правата и свободите на физическите лица. Извършването на оценяването от съда, следва да се разбира в контекста на

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.

## 5.4.КОГА СЕ ИЗВЪРШВА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Окръжен съд Разград винаги оценява рисковете, които се пораждат от неговите дейности, за да идентифицира кога съществува вероятност определен вид обработване да породи висок риск за правата и свободите на субектите на данни. С влизането в сила на GDPR, за съда възниква задължението на първо място да бъде извършена оценка за всички настоящи процеси по обработване на ЛД. При внедряване на нов процес по обработване на ЛД или промяна на вече съществуващ такъв, следва да бъде извършена първоначална оценка на риска, резултатът от която води до решение, необходимо ли е извършването на пълна оценка за конкретния процес или не.

## 5.5.КОЙ ИЗВЪРШВА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Окръжен съд-Разград в ролята си на администратор на ЛД носи отговорност да гарантира, че се извършва оценяване. Изготвянето на пълна оценка се извършва от длъжностното лице за обработка на ЛД и съдебният администратор. Изготвянето на оценката се извършва съгласно приетата в съда Методология за оценка на риска при обработване на ЛД. Когато е необходимо/целесъобразно може да се потърси становище на независими експерти от различни области (адвокати, ИТ експерти, експерти по сигурността, социолози, експерти по етични стандарти и др.).

## 5.6.СТАНОВИЩЕ НА СУБЕКТИТЕ НА ДАННИ

Когато е целесъобразно, ОС Разград следва да се обръща към субектите на данни или техни представители за становище относно планираното обработване на ЛД. Тези становища могат да бъдат потърсени по различни начини в зависимост от контекста (напр. чрез общо проучване, въпросници, анкети сред клиенти, запитване към представителите на персонала и т.н.). В случай, че съдът е събрал становища от субектите на данни, но въпреки това окончателното му решение се различава от тях, то причините за това решение следва да бъдат подходящо обосновани и документирани. ОС Разград, също така следва да документира своята обосновка да не потърси становищата на субектите на данни, ако реши, че това не е целесъобразно, например ако би изложило на риск поверителна информация или би било непропорционално или непрактично. Преценката дали е целесъобразно да бъде потърсено становището на субектите на данни се извършва от Административния ръководител на съда след обсъждане с длъжностното лице ЛД.

## 5.7.КРИТЕРИИ

• Оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

• Оценка на рисковете за правата и свободите на субектите на данни;

• Мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на ЛД.

## 5.8.ОТЧЕТНОСТ НА ПРОЦЕСА ПО ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Резултатите от оценката на риска за ЛД служат при определяне:

• заплахите вътрешни и външни вектори;

• вероятността тези заплахи да се случат;

• въздействието върху съда.

След извършване на оценката на риска, ОС Разград избира подходящата стратегия и тактически приоритети при третиране на риска. Подходящите мерки за третиране на риска зависят от конкретния контекст и рисковете във връзка с операциите по обработване. **Такива биха могли да са, но не единствено:** *псевдонимизиране и криптиране на ЛД*, свеждане на данните до минимум, прилагане на механизми за мониторинг и др. Длъжностното лице по защита на ЛД заедно със съдебния администратор изготвя подробен доклад относно извършената оценка на въздействието върху защитата на данните. **Минимално необходимите реквизити, които доклада трябва да съдържа са следните:**

• Описание на обработката на ЛД в разглеждания процес;

• Описание на обхвата на извършваната оценка;

• Списък на приложимото законодателство;

• Идентификацията и оценката на заплахите, уязвимите места и вероятността за тяхната реализация;

• Списък на контролите за третиране на риска;

• Обосновка за потвърждаване на направената оценка;

• План за действие и мерките, които трябва да бъдат предприети за третиране на идентифицираните рискове.

• Длъжностното лице по защита на ЛД следи за правилното документиране на процеса:

- *по оценка на въздействието върху защитата на данните, изготвянето и прилагането на плана за третиране на рисковете, документиране и обосновка на взетите решения относно извършването на оценка на въздействието върху защитата на данните;*
- *по защита на ЛД следи за правилното документиране на процеса след постигане на целите на обработване на личните данни в съответствие с изискванията на ОРЗД и ЗЗЛД, като личните данни се съхраняват за минимално необходимото време:*

✓ *нужно по закон;*

✓ *нужно да се изпълни договор (в т.ч. поръчка) и отговорността по него;*

✓ *нужно да се изпълни целта, за която данните са събрани и обработени;*

на този процес е да се подпомогне изграждането на доверие в извършваните от ОС Разград операции по обработване на ЛД и да се демонстрира отчетност и прозрачност. Решението за публикуване на резюме или заключения от извършената оценка на въздействието върху защитата на данните се взима от Председателя на ОС Разград.

**5.10. КОНСУЛТАЦИЯ С НАДЗОРНИЯ ОРГАН ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ** се изисква, когато съществува вероятност обработването да породи висок риск за правата и свободите на субекта на данни. В такъв случай Окръжен съд Разград носи отговорност да оцени рисковете и да определи мерки за намаляване на тези рискове до приемливо равнище, за да демонстрира спазването на GDPR. Ако въпреки предприетите от съда мерки, нивото на остатъчния риск продължава да бъде високо трябва да се извърши консултация с надзорния орган (КЗЛД). 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 др.). Консултация с надзорния орган (КЗЛД) се извършва всеки път, когато РОС не може да установи достатъчни мерки за намаляване на рисковете до приемливо равнище (т.е. остатъчните рискове продължават да бъдат високи). ***Надзорният орган (КЗЛД) в срок до осем седмици след получаване на искането за консултация дава писмено становище. Този срок може да бъде удължен с още шест седмици предвид сложността на планираното обработване.*** Надзорният орган информира ОС Разград за такова удължаване в срок от един месец от получаване на искането за консултация, включително за причините за забавянето. Тези срокове може да спрат да текат, докато надзорният орган получи всяка евентуално поискана от него информация за целите на консултацията. При консултиране, ОС Разград предоставя на надзорния орган (КЗЛД) следната информация:

- целите на планираното обработване и средствата за него;
- предвидените мерки и гаранции за защита на правата и свободите на субектите на данни;
- координатите за връзка на длъжностното лице по защита на данните;
- пълния доклад от извършената оценка на въздействието върху защитата на данните;
- всякаква друга информация, поискана от надзорния орган.

## 6. СПРАВОЧНА ДОКУМЕНТАЦИЯ

- Общия регламент за защита на данните /ОРЗД/GDPR/.

Настоящата Процедура за оценка на риска при обработване на лични данни е в сила от деня на Утвърждаване от административния ръководител председател на Окръжен съд Разград 21.06. 2021 г.