



РЕПУБЛИКА БЪЛГАРИЯ РАЙОНЕН СЪД – ЛЕВСКИ

АНАЛИЗ НА РИСКА **ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ** **В РАЙОНЕН СЪД ЛЕВСКИ**

Анализът на риска в Районен съд – Левски покрива всички процеси в организацията, свързани с обработването на лични данни. Създаването на подходящо ниво на сигурност на личните данни ги защитава срещу неразрешено или незаконосъобразно обработване, срещу случайна загуба, унищожаване или повреда.

Мерките са съобразени с рисковете, пораждащи се при обработването в контекста на правораздавателната дейност на съда и при спазване изискванията на чл.32, §2 от Регламент (ЕС) 2016/679, респективно – чл.66 от ЗЗЛД. Основна цел на разпоредбите е при анализ на подходящото ниво на сигурност да се вземат предвид по-специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин данни.

Анализът на риска е задължителен елемент от управлението на риска за защита на личните данни и се прилага по отношение на всички операции по обработване, извършвани под контрола на администратора, с цел предприемане на координирани дейности за постигане на сигурност на личните данни.

Оценяване на риска; **действия, които се предприемат с оглед нивото на риск**

➤ много нисък риск

Рисковете с оценка „много ниски“ предполагат изключително ниска вероятност от възникване на неблагоприятно събитие и не изискват предприемане на действия от страна на администратора.

➤ нисък риск

Рисковете с оценка „ниски“ се считат за приемливи. Те подлежат на мониторинг с цел да не се повиши тяхната оценка и при възможност да се избегне вероятността от възникването и въздействието им.

➤ среден риск

Рисковете с оценка „средни“ се считат за потенциално опасни. Върху тях се прилагат мерки с цел понижаване на стойностите им до степен „ниска“, когато е възможно и ефективно.

➤ висок риск

Рисковете с оценка „високи“ се считат за критични. Мерките за защита се ориентират приоритетно към тях.

Идентифициране на рисковите фактори
за защита на личните данни в контекста на Регламент (ЕС) 2016/679
и Закона за защита на личните данни

В изпълнение на чл.32, §2 от Регламент (ЕС) 2016/679 се вземат предвид рисковете, които са свързани с обработването, по-специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни. При анализа и оценката на риска се отчитат обективни критерии, като:

- **естеството на обработваните лични данни.** От значение е дали обработваните данни са „обикновени“ или специални категории. Обработването на специални категории лични данни се подчинява на специална защита, тъй като рисковете за правата на физическите лица могат да бъдат значителни. Неправомерното им обработване може да накърни конституционно признати и гарантирани права, като например принципа за равенството, свободата на убежденията, неприкосновеността на личността и личния живот. Обработването и на някои категории „обикновени“ данни може да бъде съпроводено със специфични рискове за физическите лица, например ако нерегламентираният достъп до тях може да доведе до кражба на самоличност, морални или материални вреди.

- **обхват на обработването.** Този критерий се свързва с мащаба на обработваните данни. Обработването на значителен обем лични данни на регионално, национално и наднационално равнище, може да засегне голям брой субекти на данни и те да бъдат възпрепятствани да упражняват своите права. Отчита се динамичният характер на този критерий, доколкото с течение на времето обхватът на обработването може да варира.

- **контекст на обработването.** Контекстът на обработването и по-специално дали обработването се извършва в трудовия контекст, за изпълнение на задачи в обществен интерес, за статистически цели или научни изследвания, или в една или повече от една държава членка на ЕС, или предполага трансфер извън ЕС, има отношение към специфични рискове, които съпътстват правата на физическите лица при обработване на личните им данни.

- **целта на обработването.** При анализа на риска трябва да се имат предвид не само целите, за които първоначално се събират личните данни, но и последващите съвместими цели, за които данните могат да бъдат използвани, например за научни или статистически цели.

- **последствията за субектите на данни от загуба на наличност, цялостност и поверителност на личните данни.** Преценката им е в изпълнение на чл.32, §2 от Регламент (ЕС) 2016/679, да се отчитат по-специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

Предприети мерки за защита на личните данни:

➤ Мерки за физическа защита:

- личните данни от регистрите се обработват в кабинетите на обработващите ги. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в шкафове в помещения с ограничен достъп;
- елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещения с ограничен достъп;
- помещенията, в които се обработват лични данни, са оборудвани с надлежни заключващи механизми на вратите, с пожароизвестителна система и с пожарогасителни средства;
- физически достъп до зоните, в които се обработват лични данни, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чиито служебни задължения включват обработване на лични данни от регистъра, лицата, които почистват работните помещения, и на външни лица при посочените по-долу условия;
- външни лица имат достъп до помещенията, в които се обработват лични данни от регистрите, при кумулативно наличие на следните условия: в присъствието на упълномощени служители; след разпореждане на административния ръководител; при законово основание за разрешаване на достъпа;
- в зоната с контролиран достъп (втори етаж) са разположени помещенията, в които се обработват част от регистрите за лични данни. Контролираният достъп се осъществява чрез заключващо устройство на коридорната врата;
- достъпът до регистрите, които се обработват на първия етаж, се контролира от съдебните служители и от служителите на ОЗ „Охрана“ - Плевен, чрез пряк контрол.

➤ Мерки за персонална защита:

- лицата, обработващи лични данни, са запознати със ЗЗЛД, Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година и вътрешните правила в Районен съд – Левски;
- при всяка промяна в нормативната уредба или в политиката за защита на личните данни се провежда обучение на всички обработващи лични данни;
- лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител;
- споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от съображения за информационна сигурност.

➤ Мерки за документална защита и защита на автоматизирани информационни системи и мрежи:

- всички регистри се поддържат и на хартиен носител. Работещите в РС Левски имат достъп до регистри на принципа „необходимост да се знае“. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания. Данните се класифицират в съответствие с тяхното предназначение и характер, и се съхраняват в шкафове в зоните с ограничен достъп. За част от регистри са осигурени заключващи се шкафове;

- административният ръководител и длъжностното лице по защита на данните са отговори за контрола на достъпа до регистри;

- спазването на сроковете за съхранение на личните данни от регистри, които са на хартиен носител, се съблюдава системно;

- преди унищожаването на документите, съдържащи лични данни, се извършват процедурите по реда на ЗНАФ, ПАС и Номенклатурата на делата със срокове за съхраняването им в РС Левски.

- регистри или части от тях, съдържащи лични данни, могат да бъдат размножавани след подаване на писмено заявление, единствено при наличие на законово основание или ако са изискани по надлежния ред от субекти, чиито лични данни се съхраняват;

- данните се унищожават по процедурите, предвидени във Вътрешните правила за организация и дейността на учредения архив в РС Левски, в ПАС и ЗНАФ. Документите се описват в акт за унищожаване на неценни документи с изтекъл срок на съхранение, който се изпраща за съгласуване с Отдел „Държавен архив“ Плевен. Физическото унищожаване се извършва от фирма, регистрирана в КЗЛД като администратор на лични данни, при гарантиране неразпространяването на информация;

- при работа с данните от регистри се използват софтуерни продукти за обработването им. Данните се въвеждат в база и се съхраняват на сървър. Всеки, работещ с деловодните системи, има личен профил (потребителско име и парола) с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър;

- системният администратор създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва седмична профилактика на софтуера и системните файлове;

- административният ръководител и длъжностното лице по защита на данните са отговорни за управлението на регистри, съдържащи лични данни в електронен формат;

- за всички сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS);

- в помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа и сигнално-охранителна система (за част от помещенията).

Предприети организационни мерки
за гарантиране нивото на сигурност на личните данни:

- охрана на сградата със сигнално-охранителна техника, пропускателен режим в сградата, контролиран достъп, видеонаблюдение и обходи от служители на ОЗ “Охрана“ Плевен;

- работните компютърни конфигурации, както и цялата ИТ инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;

- разрешава се осъществяването на отдалечен достъп до данни от регистрите, само след разрешение на административния ръководител, при спазване на нормативните изисквания за защита на личните данни.

Оценка на риска по отношение на регистрите с лични данни,
водени в Районен съд – Левски, базирана на идентифицираните
рискови фактори и предприетите мерки за защита:

	Регистри с лични данни	Идентифициране на потенциалния риск	Степен на влияние при възникване на евентуални нарушения	Предприети мерки за сигурност	Идентифициран остатъчен риск
1	Персонал (магистрати, съдии по вписванията, ДСИ, съдебни служители)	Риск от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин данни.	висока	Физическа защита, персонална защита, документална защита – регламентирани във Вътрешните правила за защита на личните данни в РС Левски	нисък
2	Участници в конкурси	Риск от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин данни.	висока	Физическа защита, персонална защита, документална защита – регламентирани във Вътрешните правила за защита на личните данни в РС Левски	нисък
3	Съдебни дела (физически лица, страни или участници в граждански, наказателни, изпълнителни производства)	Риск от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин данни.	висока	Физическа защита, персонална защита, документална защита – регламентирани във Вътрешните правила за защита на личните данни в РС Левски	нисък

4	Вещи лица и преводачи	Риск от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин данни.	висока	Физическа защита, персонална защита, документална защита – регламентирани във Вътрешните правила за защита на личните данни в РС Левски	нисък
5	Съдебни заседатели	Риск от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин данни.	висока	Физическа защита, персонална защита, документална защита – регламентирани във Вътрешните правила за защита на личните данни в РС Левски	нисък
6	Бюро „Съдимост“	Риск от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин данни.	висока	Физическа защита, персонална защита, документална защита – регламентирани във Вътрешните правила за защита на личните данни в РС Левски	нисък

Заключение

Предвид идентифицираните рискове, предприетите организационни мерки от страна на администратора за ограничаване на риска и предвидените процедури в случай на установяване на нарушения на сигурността на обработваните лични данни, **обобщената оценка на риска в Районен съд – Левски е „нисък“.**

Оценката на риска, а в зависимост от нея и мерките за защита, се преразглеждат периодично най-малко веднъж на две години или при промяна в някой от критериите, при които е определена оценката, или при промени в естеството, обхвата, контекста и целта на обработването, както и в използваната технология за обработване.

28.11.2025 г.

ИЗГОТВИЛ:

Янка Борисова, длъжностно лице по защита на данните