У Т В Ъ Р Д И:
ЛАЗАР МИЧЕВ
АДМИНИСТРАТИВЕН РЪКОВОДИТЕЛ
ПРЕДСЕДАТЕЛ ОКРЪЖЕН СЪД
ГРАД РАЗГРАД
/Заповед №РД-14-157./11.10.2021 г./

ПРОЦЕДУРА

ПО АНАЛИЗ И УПРАВЛЕНИЕ НА РИСКА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Анализът на риска в ОС Разград 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-специано 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 и предприемане на координирани дейности, за постигане на сигурност на личните данни.

I. ПРЕДНАЗНАЧЕНИЕ НА ПРОЦЕДУРАТА

Настоящата процедура има за цел да установи първоначалните стъпки по анализиране на дейностите по обработване на лични данни в Окръжен съд Разград и последващото въвеждане на изискванията на Общия регламент за защита на данните (ОРЗД) в документацията и техническите средства на всеки администратор на лични данни.

II. ЗАДЪЛЖЕНИЯ И ОТГОВОРНОСТИ

Първоначалният вътрешен анализ се прави в Окръжен съд Разград от длъжностното лице по защита на ЛД, който е служител от организацията и който въз основа на длъжностна си характеристика и/или вътрешните правила има задължения в този смисъл.

Съгласно общите принципи на регламента отговорност за предприемане на подходящи мерки за защита на личните данни, респективно доказване, че такива са предприети, носи Администраторът. Санкциите за неизпълнение на задълженията по Общия регламент се налагат от надзорния орган на администратора на лични данни /ИВСС/, който от своя страна би могъл да търси регресна отговорност от лицата, на които е възложил конкретни задачи и съдействие във връзка с ОРЗД.

III. ХОД НА ПРОЦЕДУРАТА

1. Анализ (инвентаризация) и дейностите по обработването на данните в Окръжен съд Разград се провежда чрез:

1.1. Създаване на екип от служители, който има задължение за извършването на първоначалния анализ *(инвентаризация)* на данните, както и за извършването на „картографиране" на потоците от лични данни

(ръководни служители, други ключови служители в организацията – гл.счетоводител, IT, връзки с обществеността и др). В Окръжен съд Разград се създават необходимите условия и отделя необходимия ресурси, така че екипът да се запознае с новите нормативни изисквания в областта на защитата на личните данни.

1.2. Екипът за извършване на първоначален анализ създава въпросници/анкети, в които са зададени първоначалните насоки, свързани с обработването на личните данни и които помагат да се изясни какви лични данни се обработват и какви допълнителни мерки трябва да се предприемат за тяхната защита, в съответствие с ОРЗД. Въпросниците създадени от екипа в Окръжен съд Разград, съдържат следните въпроси:

- Какво са лични данни?;
- Обработва ли организацията лични данни?;
- В кои функционални/административни процеси е включено обработването на лични данни?;
- Какви са основните категории лични данни, които се обработват?;
- Личните данни на какви основни категории субекти (*ФЛ и ЮЛ*) се обработват?;
- За какви конкретни цели се събират, съхраняват и обработват личните данни?;
- На какво основание се обработват отделните категории лични данни?;
- Има ли лични данни, които се обработват без организацията да има необходимост от това?;
- Къде се съхраняват данните?;
- На кого се предоставят или разкриват личните данни извън организацията?;
- други въпроси свързани с анализ на обработването на лични данни в Окръжен съд Разград.

1.3. На основата на създадените въпросници/анкети, екипът по първоначален анализ извлича следните данни за обработваните от организацията лични данни:

- функционалните/административни процеси при които се използват лични данни;
- описание на категориите лични данни и елементите във всяка категория;
- описание на категориите субекти, чиито лични данни се обработват;
- целите, за които се събират, съхраняват и обработват личните данни;
- правното основание за обработването на всяка категория лични данни;
- източниците на лични данни;
- получателите или категориите получатели на личните данни;
- получателите или категориите получатели на личните данни извън ЕС;
- лични данни или категории лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и унищожаване на различните категории лични данни;
- основните системи *(приложения, технологии)* и места за съхранение;
- брой на субектите на данни, чиито данни се обработват.

В процеса на инвентаризация Окръжен съд Разград следва да идентифицира, т.е. да установи къде се съхраняват данните, както и на какъв носител са записани.

Забележка: *В Окръжен съд Разград немалка част от личните данни се съхраняват на хартиен носител или в съответните файлове в системата на администратора Обработват се много и различни видове лични данни, намиращи се в различни системи, вследствие наличието на трансфер и обмен налични данни между отделните структурни звена на организацията, както и извън нея, предвид осъществяваните контакти с оглед предлаганите услуги в правораздаването. Това налага IT специалиста в съда да преценява дали съществуващата система на администратора позволява правилно идентифициране на физическите лица-субекти на данни.*

1.4. На основата на направения анализ на функционалните/административни процеси Окръжен съд Разград установява работните потоци с данни и ги картографира

(Описание в схематичен вид пътя на категориите лични данни от момента на получаване, през обработването им вътре в организацията на администратора на лични данни, до получаването им от трети страни - обработващи, контрагенти, публични органи и др.).

При извършване на картографирането на работните потоци съдът решава следните въпроси:

- Под каква форма трябва да бъдат картографирани данните?;
- Може ли автоматизацията да бъде приложена към процеса самостоятелно или в комбинация с

ръчна работа?;

- Има ли средство за сканиране на данни в организацията, което може да бъде използвано?;
- Как ще се поддържа опис на данните и кой ще управлява и поддържа този опис?;
- Прави се преценка за наличието на излишни или неактуални лични данни, с цел тяхното премахване, което е мярка за свеждане до минимум на обработването на лични данни.

Целта на анализа е да се разкрие жизнения цикъл на личните данни в организацията, след което *(при необходимост)* да се създадат по-задълбочени въпросници, както и последващи интервюта с ключови служители на Окръжен съд Разград.

2. Окръжен съд Разград установява съществуващите към момента технически и организационни мерки за защита на личните данни, дали и доколко същите покриват изискванията на ОРЗД. За тази цел се използва помощта на IT експерта на администратора /съда/, който следва да преценява общото техническо състояние и съответствието на защитата на личните данни с Общия регламент по защита на данните.

3. Екипът изготвя препоръки относно това, какви документи /правила, политики/ от правна страна трябва да бъдат изготвени, в съответствието с новите изисквания на Общия регламент.

Определят се необходимите допълнителни технически и организационни мерки, които следва да бъдат взети и как те да бъдат въведени технологично в системите за сигурност на Окръжен съд Разград, така че да се осигури пълна защита на ползваните лични данни на субектите.

Забележка: *Важна част от предварителния анализ е предотвратяването на загубата на данни (DLP), която е обща техническа мярка, помагаща на администратора да инвентаризира личните данни. Това е технология, която помага на администратора да разбере как се обработват данните, независимо къде се намират - в локалната мрежа, външната мрежа и други; Когато данните се съхраняват в местни файлове, могат да се използват работни станции под различни операционни системи, електронни пощенски кутии, бази данни или споделени файлове, прикачени към мрежата хранилища, синхронизиране на файлове от трети страни и споделяне или съхранение при доставчици на облачна услуга или системи за обмен на имейли в облак и за сътрудничество.*

4. Окръжен съд Разград прави преценка дали е необходимо задължение да се назначи или определи служител за Длъжностно лице по защита на данните (ДЛЗД).

5. Екипът за първоначален анализ в Окръжен съд Разград, след като е изготвен списъкът с препоръки, прави анализ и преминава към изготвяне на следните документи:

- анекси към трудовите/гражданските договори;
- корекции в длъжностни характеристики на служители на администратора;
- изготвяне на формуляри за съгласие;
- декларации за поверителност:
- вътрешни правила, процедури и др. документи, които са необходими за осигуряване на максимално ниво на защита на личните данни в съответствие с ОРЗД.

Екипът за първоначален анализ в съда прави основен преглед на използваните до момента алтернативни правни основания за обработване на лични данни:

- съгласие;
- законово задължение за администратора;
- защита на жизненоважни интереси на субекта на данните или на друго физическо лице;
- изпълнение на задача от обществен интерес или упражняването на официални правомощия, предоставени на администратора;
- легитимни интереси на администратора или на трета страна, когато същите имат преимущество над интересите или основните права и свободи на субекта на данните.

IV. РЕГИСТЪР НА ИЗДАНИЯТА /РЕВИЗИИТЕ/

Дата на изготвяне/промяна	Издание	Промени, основание	Изготвил	Подпис
Дд/мм/година	първо	GDPR	Име,фамилия	

6. След като се инвентаризират личните данни, организацията трябва да проведе анализ на риска и да приведе в действие програма за управление на риска, която да покрие всички лични данни и свързаните с тях процеси от техническа и организационна гледна точка.

7. Анализът на риска се провежда, като се използват практиките и приложимите международни стандарти, като се намерят подходящите методики и контроли за информационна сигурност. Организацията проверява какви мерки за управление на риска са въведени към момента, какви рискове съществуват и с какви контроли те могат да бъдат елиминирани или минимизирани до приемливо ниво. Анализът на риска покрива всички процеси в организацията, свързани с обработването на лични данни, включително организационни, управленски, технически и административни. На базата на идентифицираните рискове се подготвя и последващата класификация и програма. Зоните, които се покриват, включват:

- организация на информационната сигурност;
- сигурност, свързана с човешките ресурси;
- управление на информационните активи и данни – отговорности, класификация, среда;
- контрол на достъпа; -
- криптография;
- физическа и периметър на сигурност;
- оперативна сигурност на информационните системи;
- мрежова сигурност;
- трансфер на информация и данни;
- придобиване, разработване и поддръжка на софтуер;
- рискове, свързани с доставчици и други.

8.Доклад за рисковете и програма за тяхното управление

След като се направи анализът, се подготвя доклад с класификация на рисковете и програма за управление на риска, в която се приоритизират по значимост рисковете и се разписват контроли за тях с цел елиминиране, избягване или минимизиране.

9. Програма за управление на риска

В програмата за управление на риска се разписват мерките, които могат да са:

- модифициращи – *прилагане на контроли за намаляване на щетата;*
- мерки с цел избягване на риска – *предприемане на действия, които го правят риска, или мерки, чрез които рискът се споделя или трансферира /пример: чрез застраховане/*;

Специфичните контроли могат да се изберат с помощта на посочените по-горе стандарти. Примери за контроли са:

- ограничаване на дистанционния достъп,
- регистрация/дерегистрация на достъпа,
- политика за пароли,
- криптография,
- защитни стени,
- антивирусни и антиспам защити,
- сигурни зони,
- логове,
- мрежова сегрегация,
- сигурен периметър и други.

В договарянето на отношенията администратора обработващ ЛД обръща изрично внимание на сигурната и защитена обработка на личните данни, което да гарантира конфиденциалност, интегритет и достъпност съобразно целите на обработка и регламента за защита на личните данни.

V.АНАЛИЗ НА РИСКА НА РЕГИСТРИТЕ С ЛИЧНИ ДАННА В ОС РАЗГРАД

За целите на дейността в Окръжен съд Разград се поддържат регистри с лични данни, които са както следва:

- Регистър „Човешки ресурси"
- Регистри „Финансово-счетоводна дейност": - „СЕБРА", „Каса", „Движение по набирателна с/ка", „Постъпления по транзитна с/ка", Разчети", „Годишни инвентаризации", „Заплати", Щатно разписание" и др.
- Регистър Решения по „Граждански дела"
- Регистър „Съдебни книги-описни, срочни, азбучници, книга за изпълнение на влезлите в сила присъди и определения"
- Регистър "Софтуерни продукти"
- Регистър „Съдебни заседатели"
- Регистър „Конкурси - съдебни служители и др."
- Регистър „Служебна кореспонденция от/до, регистър - входящ/ изходящ;
- Регистър "Лични данни на лица, подали молби, жалби, предложения, сигнали и искания";
- Регистър „съдебните заседатели и преводачи";
- Регистър „Библиотеката на съда";
- Регистър „Вещи лица"
- Регистър „Стажант-юристи";
- Регистър "Инициативи на ВСС.

Във всички регистри се съдържат и обработват различни категории и видове лични данни: обикновени/общи лични данни и специални чувствителни данни, на които се прави анализ и оценка на риска. Анализа и оценката на риска на ЛД в съда се извършва на основата на: - *естеството, обхвата, контекста и целите на обработването; - възможните рискове за правата и свободите на ФЛ и тяхната вероятност и тежест; последиците за правата и свободите на ФЛ.*

Анализа се извършва на три етапа:

1.Идентифициране на релевантните */приложими/* рискове, при което се прави ясно описание на произхода на риска и естеството на последиците, които той може да има с точното представяне кой и какво би било негативно засегнато, при какви обстоятелства и по какъв начин;

2.Определяне на вероятността от настъпване и степента на вредите.

3.Описание на алтернативните начини за ограничаване на идентифицираните рискове.

Резултатите от оценката на риска се степенуват като нисък, среден и висок риск за съхранението на данните.

Оценка на въздействието се извършва, когато това се изисква, съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни. Оценка на въздействието се извършва за високорискови дейности по обработване. Ако извършената оценка на въздействието покаже, че обработването ще породи висок риск и ако администраторът **не предприеме** мерки за ограничаване на риска, следва да се извърши консултация с ИВСС или КЗЛД преди планираното обработване.

Администраторът на лични данни прилага мерки за защита на личните данни съда, които осигуряват:

1.Физическата защита на личните данни се осъществява при спазване на следните мерки:

- определяне на зони с контролиран достъп на външни лица;
- личните данни се обработват в кабинетите на лицата, на които е вменено задължението за обработване на данни от съответните регистри;
- всички документи на хартиен носител, съдържащи лични данни, се съхраняват в помещения с подходящи мерки за контрол на достъпа до тях само за оправомощени лица;
- помещенията, в които се обработват лични данни, са оборудвани със заключващи се врати;
- сградата на Съдебната палата е оборудвана с пожарогасителни средства;
- елементите на комуникационно-информационните системи, използвани за обработване на ЛД, се намират в помещение с ограничен достъп;
- външни лица имат достъп до помещенията в които се обработват лични данни, само в присъствието на упълномощени служители.

2. Персоналната защита на личните данни се осъществява при спазване на следните мерки:

- Лицата, обработващи ЛД, се запознават с нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане (*Общия регламент за защита на данните, Закона за защита на личните данни, настоящите Вътрешни правила*), както и с други нормативни актове, относими към съответната дейност по обработване.

- Достъп до лични данни се предоставя само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае";

- Всички лица, обработващи лични данни, са длъжни да спазват ограниченията за достъп до личните данни и са персонално отговорни пред АЛД за нарушаването на принципите за „Поверителност",„Цялостност" и „Наличност" на личните данни;

- Оторизираните с право на достъп лица подписват Декларация за конфиденциалност на личните данни, до които получават достъп при и по повод изпълнение на служебните си задължения, която се прилага към трудовото досие;

- Подписването на декларация не се изисква, ако съответното задължение е включено в длъжностната характеристика на лицето;

- Забранено е споделянето между служителите на критична информация като идентификатори, пароли за достъп и др.;

3. Документалната защита на личните данни се осъществява при спазване на следните мерки:

- Регистрите с лични данни обработвани от Окръжен съд Разград, се поддържат на хартиен или на електронен носител;

- Обработването на личните данни се извършва в рамките на работното време на съда, по изключение в извънработно време, когато е свързано с дейности по правораздаване;

- Достъп до регистрите с лични данни имат служителите, на които е възложено обработване на данните, при спазване на принципа „Необходимост да се знае";

- Личните данни се събират само за конкретни цели, в съответствие с нормативните изисквания на ОС Разград;

- Сроковете за съхранение на личните данни от различните регистри е определен в утвърдената Номенклатура на делата със срокове за съхранение за съда;

- Документите, съдържащи лични данни, се съхраняват само в помещения с ограничен достъп;

- Архивирането на лични данни на хартиен носител се осъществява в съответствие с Вътрешните правила за архивиране на делата в ОС Разград;

- Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица;

- Временните документи, копия от документи и работни материали от регистрите, които са на хартиен носител и съдържат лични данни, се унищожава, чрез машини за унищожаване на документи (шредер);

- След изтичане срока за съхранение на документите от регистрите, документите се унищожават по начин, непозволяващ тяхното възстановяване от оторизирана фирма с предмет конфиденциално унищожаване на документи.

4. Защитата на автоматизираните информационни системи и мрежи (АИС/М) се осъществява при спазване на следните мерки:

- Електронната обработка се реализира с помощта на специализирани приложни софтуерни продукти и чрез стандартни средства за текстообработка, електронни таблици и др. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен потребител на АИС/М има личен профил с определени нива на достъп, съобразно неговите задължения и принципа „Необходимост да се знае". В автоматизираните информационни системи за обработка на съдебни дела се поддържа системен журнал за извършените от потребителя действия.

- Администраторът на АИС/М създава и поддържа базови конфигурации за защита на операционната система, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове;

- За компютърните конфигурации, сървъри и комуникационни средства 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;

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

- Заличаването на личните данните в електронен вид се осъществява чрез стандартните средства на операционната система или със средствата на специализираните софтуерни продукти;

- При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата на които се съхраняват лични данни.

VI. ПРОЦЕДУРА ПО ДОКЛАДВАНЕ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

При регистриране на неправомерен достъп/нарушение на сигурността до информационните масиви за лични данни, или при друго нарушение на сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на длъжностното лице по защита на данните. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му.

Длъжностното лице по защита на данните писмено уведомява за инцидента администратора, като му предоставя наличната информация относно характера на инцидента, времето на установяване, вида на щетите, предприетите мерки за ограничаване на щетите. След уведомяването Администраторът предприема необходимите мерки за предотвратяване или намаляване на последиците от неправомерния достъп/нарушението на сигурността както и възможните мерки за възстановяване на данните.

В случай, че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, администраторът, чрез длъжностното лице по защита на данните, уведомява ИВСС без ненужно забавяне и когато това е осъществимо не по-късно от 72 часа след първоначалното узнаване на нарушението.

Уведомлението до ИВСС съдържа следната информация:

1. Описание на нарушението на сигурността, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни.

2. Името и координатите за връзка с администратора.

3. Описание на евентуалните последици от нарушението на сигурността.

4. Описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица администраторът без ненужно забавяне, уведомява засегнатите физически лица.Администраторът трябва да документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него.

VII.СПРАВОЧНА ДОКУМЕНТАЦИЯ

- Общият регламент за защита на данните /ОРЗД/GDPR/]
- Закона за защита на личните данни;
- Закона за съдебната власт;
- Правилника за администрацията в съдилищата;
- Акт за резултати от извършена планова проверка по ЗЗЛД, изх. № ПЛД-21-10/28.09.2021 г. от органи на ИВСС;

Настоящата Процедура за анализ и управление на риска при обработване на лични данни е неразделна част от Вътрешните правила за мерките за защита на личните данни в Окръжен съд Разград и Процедурата за оценка на риска при обработване на лични данни утвърдени със заповед № РД-14-103/21.06.2021 г. на председателя на Окръжен съд Разград и влизат в сила със заповед от деня на утвърждаването им от административния ръководител председател на Окръжен съд Разград, 11.10.2021 г.