

О К Р Ъ Ж Е Н С Ъ Д - Р У С Е

УТВЪРДИЛ:

(А. Гавраилова)

И. Ф. Адм. Ръководител – председател на ОС –
Русе (Решение на СК на ВСС по Протокол №
№13/29.03.2022 г., т.15)



Заповед № 641/14.12.2022 г.

ВЪТРЕШНИ ПРАВИЛА ОТНОСНО МЕХАНИЗМА НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ И ЗАЩИТАТА ИМ ОТ НЕЗАКОННИ ФОРМИ НА ОБРАБОТВАНЕ

I. ПРАВНО ОСНОВАНИЕ/ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите вътрешни правила се издават на основание чл. 25д от Закона за защита на личните данни (ЗЗЛД) и са изготвени в съответствие с изискванията на 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), Регламент (ЕС) 2016/680, Закон за електронните съобщения; Правилник за дейността на Комисията за защита на личните данни и на нейната администрация; Инструкция № 1 от 21 декември 2016 г. за обстоятелствата, при които предприятията, предоставящи електронни съобщителни услуги уведомяват потребителите за нарушения на сигурността на личните данни, формата и начина на уведомяването.

Чл. 2 (1) Окръжен съд – Русе е администратор на лични данни по смисъла на чл. 4 от Общия регламент относно защитата на данните (ЕС) 2016/679, юридическо лице на бюджетна издръжка със седалище в гр. Русе и адрес ул. „Александровска“ № 57, ЕИК 000530739. Като такъв, при обработването на лични данни съдът спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

(2) Обработващ личните данни е всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

(3) За Окръжен съд - Русе обработващ лични данни е службата по трудова медицина „Антеа консулт“ ЕООД гр. Русе и други служби, съгласно сключени договори.

(4) Трета страна е физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора,

обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.

(5) За Окръжен съд – Русе трета страна са, НАП, НОИ, други съдилища и служби.

(6) Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „необходимост да знае” и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора.

(7) Всички лица отговарят за спазването на ограниченията за достъп до личните данни и са персонално отговорни пред Административния ръководител за нарушаване на принципите за поверителност, цялостност и наличност на личните данни, освен в случаите на форсмажорни обстоятелства.

(8) Всяко физическо лице, чиито лични данни ще се обработват от администратора, следва да бъде уведомено за:

1. данните, които идентифицират администратора;
2. целите на обработването на личните данни;
3. категориите лични данни, отнасящи се до съответното физическо лице;
4. информация за правото на достъп и правото на коригиране на събраните данни.

(9) Алинея 6 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните е невъзможно или изисква прекомерни усилия;
2. вписването или разкриването на данни са изрично предвидени в закон;
3. физическото лице, за което се отнасят данните, вече разполага с информацията;
4. е налице изрична забрана за това в закон.

Чл. 3 С настоящите вътрешни правила в Окръжен съд – Русе се уреждат:

1. създаването на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на физическите лица, при неправомерно обработване на свързаните с тях лични данни, в процеса на свободно движение на данните;

2. оценката на въздействие и нивото на защита на личните данни;

3. избор на необходимите технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване, или от случайна загуба, неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване. Мерките имат за цел да гарантират поверителност, цялостност и наличност на личните данни;

4. правата и задълженията на длъжностните лица и лицата, които имат достъп до лични данни, както и тяхната отговорност при изпълнението на тези задължения;

5. процедурите по докладване, управление и реагиране при инциденти;

6. срокове за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им;

7. срокове за съхранение на личните данни и реда за тяхното унищожаване след изтичането им.

II. ЦЕЛИ НА ВЪТРЕШНИТЕ ПРАВИЛА.

Чл. 4. Настоящите вътрешни правила имат за цел да регламентират:

1. механизмите на водене, поддържане и защита на съхраняваните лични данни за персонала на съда, зает по трудови или граждански правоотношения, както и лични данни за участниците в съдебния процес;

2. задълженията на съдебните служители и/или лицата, които имат достъп до лични данни, тяхната отговорност при неизпълнение на тези задължения;

3. необходимите технически и организационни мерки за защита личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

III. ДЕФИНИЦИИ

Чл. 5 За целите на Вътрешните правила, използваните понятия имат следното значение:

- **ЗЗЛД** – Закон за защита на личните данни.
- **КЗЛД** – Комисия за защита на личните данни.
- **ОРЗД** – 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).
- **„Лични данни“** са всяка информация, с която едно физическо лице може да бъде идентифицирано пряко или косвено по един или повече признаци, характерни за личността, като например: име, идентификационен номер/ЕГН, данни за контакт – местонахождение/пощенски адрес, телефонен номер, e-mail адрес, онлайн идентификатор/IP адрес и др. Тези признаци може да са част от физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на физическото лице.
- **„специалните категории лични данни“** са: 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.

- „Обработване на лични данни“ е съвкупността от действия, извършвани с лични данни или набор от лични данни като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;
- „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

IV. СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 6. (1) Окръжният съд събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, доставчик на услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от съда, са групирани според вида на дейностите по обработване, съдържащи правила за обработване на лични данни, отнасящи се до:

- ❖ извън правораздавателната дейност на Окръжен съд – Русе:
 - служители;
 - кандидати за работа;
 - контрагенти;
 - заявители на услуги.
- ❖ правораздавателната дейност на съда по граждански, търговски и наказателни дела:
 - управление на делата;
 - вещи лица, преводачи, съдебни заседатели, тълковници и др.;
 - заявители, свързани с правораздавателната дейност;
 - регистратура по ЗЗКИ.

(2) Относно лицата, заети по трудови правоотношения в съда и на кандидатите за работа, се събират следните лични данни:

а) Идентификация: име; ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни;

б) Образование и професионална квалификация: данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;

в) Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;

г) Други данни: свидетелство за съдимост, когато се изисква представянето му съгласно нормативен акт, както и други данни, чието обработване е

необходимо за изпълнение на правата и задълженията на Окръжния съд като работодател.

Цели за които се обработват:

Индивидуализиране на трудовите правоотношения, управление на човешките ресурси, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на Окръжен съд – Русе, в качеството му на работодател, съгласно нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за съдебната власт, Закона за счетоводството, Закона за държавния архив, Правилника за администрацията в съдилищата, Наредбата за структурата и организацията на работната заплата и др.;

Събраните данни за съответните лица се използват за служебни цели:

- за всички свързани дейности, съществуване, изменение и прекратяване на трудовите правоотношения;
- за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);
- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови договори;
- за водене на счетоводна отчетност, относно възнагражденията на посочените по-горе лица по трудови договори.

Съдът обработва чувствителни данни, само доколкото това е необходимо за изпълнение на специфичните му права и задължения в областта на трудовото и осигурително законодателство.

(3) Относно физически лица, контрагенти на съда и заявители на услуги, се събират лични данни, които са необходими за изпълнението на законовите задължения на съда, като доставчик; лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на съда от външни доставчици на услуги, както следва:

- име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни; електронна поща.

(4) Относно физически лица страни и участници в съдебни производства по граждански и търговски дела, набира и съхранява лични данни на участниците в съдебния процес в съда по време на процеса с оглед индивидуализиране на страните и участниците в него, изпълнение на нормативните изисквания на Граждански процесуален кодекс, Правилника за администрацията в съдилища и др.;

Събраните данни за съответните лица се използват за служебни цели, както следва:

- за всички дейности, свързани със съществуване, изменение и прекратяване на участието им в гражданския процес – за изготвяне на

всякакви документи на лицата в тази връзка (служебни бележки, справки, удостоверения и др. подобни);

- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му като страна/участник в гражданския процес;
- за водене на счетоводна отчетност относно дължимите плащания от и на посочените по-горе лица за държавни такси и разноски по делата;

(5) Относно физически лица **страни и участници в съдебни производства по наказателни дела**, набира и съхранява лични данни на страните и участниците в съдебния процес в съда по време на наказателния процес с оглед индивидуализиране на страните и участниците в процеса, изпълнение на нормативните изисквания на Наказателно-процесуалния кодекс, Правилника за администрацията в съдилищата и др.

Събраните данни за съответните лица се използват за служебни цели, както следва:

- за всички дейности, свързани със съществуване, изменение и прекратяване на участието им в наказателния процес – за изготвяне на всякакви документи на лицата в тази връзка (служебни бележки, справки, удостоверения и др. подобни);
- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му като страна/участник в наказателния процес;
- за водене на счетоводна отчетност относно дължимите плащания от и на посочените по-горе лица за държавни такси и разноски по делата;

(6) Относно физически лица – **вещи лица, преводачи, тълковници, съдебни заседатели и др.**, набира и съхранява лични данни на същите, участващи в съдебния процес в съда с оглед индивидуализиране на посочените лица в процеса, изпълнение на нормативните изисквания на Граждански процесуален кодекс, Наказателно-процесуалния кодекс, Закон за съдебната власт, Закон за счетоводството, Наредба № 2 от 29.06.2015 г. за вписването, квалификацията и възнагражденията на вещите лица, Наредба № 7 от 28.09.2017 г. за съдебните заседатели, Наредба № Н-1 от 16.05.2014 г. за съдебните преводачи и др.

Събраните данни за съответните лица се използват за служебни цели, както следва:

- за всички дейности, свързани с участието им в съдебния процес (служебни бележки, справки, удостоверения и др. подобни);
- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му като вещо лице;
- за водене на счетоводна отчетност относно дължимите възнаграждения на вещите лица, съдебни заседатели, преводачи, тълковници и др. участвали в гражданския/наказателен процес;

(7) Относно физически лица, **заявители свързани с правораздавателната дейност**, набира и съхранява лични данни на същите, участващи в съдебния

процес в съда с оглед индивидуализиране на посочените лица в процеса, изпълнение на нормативните изисквания на Граждански процесуален кодекс, Наказателно-процесуалния кодекс, Закон за съдебната власт, Закон за счетоводството и др.;

Събраните данни за съответните лица се използват за служебни цели, както следва:

- за всички дейности, свързани с участието им в съдебния процес (служебни бележки, справки, удостоверения и др. подобни);
- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до качеството на заявителя в производството.
- за водене на счетоводна отчетност относно дължими възнаграждения.

(8) Относно физически лица, участници в засекретени производства, набира и съхранява лични данни на същите, участващи в съдебния процес в съда с оглед индивидуализиране на посочените лица в процеса, изпълнение на нормативните изисквания на ЗЗКИ;

Събраните данни за съответните лица се използват за служебни цели, както следва:

- за всички дейности, свързани с участието им в съдебния процес (служебни бележки, справки, удостоверения и др. подобни);
- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция.

V. ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 7. Личните данни се обработват законосъобразно, добросъвестно и прозрачно при спазване на следните принципи:

(1) Субектът на данните се информира предварително за обработването на неговите лични данни;

(2) Личните данни се събират за конкретни, точно определени и законни цели и не се обработват допълнително по начин, несъвместим с тези цели;

(3) Личните данни съответстват на целите, за които се събират;

(4) Личните данни трябва да са точни и при необходимост да се актуализират;

(5) Личните данни се заличават или коригират, когато се установи, че са неточни или не съответстват на целите, за които се обработват;

(6) Личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период, не по-дълъг от необходимия, за целите, за които тези данни се обработват.

Чл. 8. За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:

(1) Субектът на данните е информиран за необходимостта от предоставяне на същите при осъществяване на законовите функции на съда.

(2) Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

(3) Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

(4) Обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;

(5) Обработването е необходимо за изпълнение на задача от обществен интерес;

(6) Обработването е необходимо за целите на легитимните интереси на съда освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. Целите, за които се обработват лични данни на това основание, трябва да са описани в приложимите известия по защита на данните.

VI. СЪГЛАСИЕТО, КАТО ОСНОВАНИЕ ЗА ОБРАБОТКА

Чл. 9. (1) Когато не са налице хипотезите на чл. 7, пар. 1, б. „б“ - „е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от съда, подписват декларация за съгласие по образец (*Образец № 1*).

Елементи на валидно съгласие:

- Свободно дадено;
- Дадено за определена цел на обработката;
- Информирано;
- Недвусмислено.

(2) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.

(3) Декларациите за съгласие се съхраняват от съда, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност.

VII. ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Процедура за обработване на личните данни, отнасящи се до лицата, заети по трудови правоотношения в съда, както и на кандидатите за работа.

Чл. 10. (1) Личните данни, отнасящи се до лицата, заети по трудови правоотношения в съда, както и на кандидатите за работа, се събират при и по повод набирането на персонал. Данните на всеки служител на съда се съхраняват в лични досиета, като някои данни могат да се съхраняват или обработват и на технически носител. Данните от проведени конкурси и интервюта се съхраняват на технически и/или хартиен носител, в зависимост от нуждата.

(2) Личните досиета се подреждат и заключват в каса, намираща се в кабинета на административния секретар. Данните на кандидатите за работа,

които се съхраняват на хартиен носител, се съхраняват в нарочни шкафове в кабинета на административния секретар. Достъпът до кабинета се предоставя само на лицата, оправомощени да обработват личните данни, заместващи административния секретар. Данните за лица, проучени за работа с класифицирана информация се съхраняват в нарочни за целта папки в регистратура за работа с класифицирана информация, по реда на ЗЗКИ и ППЗЗКИ.

(3) Лицата, оправомощени да обработват лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните досиета и класъорите с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.

(4) Досиета на работниците и служителите, както и данните на кандидатите за работа, не се изнасят извън сградата на съда.

Процедура за обработване на лични данни, отнасящи се до контрагентите на съда.

Чл. 11. (1) Личните данни, отнасящи се до клиенти, се събират при подаване на заявка за предоставяне на услуга или сключване на договор с клиент на съда.

(2) Личните данни, отнасящи се до доставчици на услуги, се събират при сключване на договор с доставчик на услуги, като обичайно личните данни се съдържат в текста на самите договори.

(3) Личните данни се съхраняват на електронен и хартиен носител (подписани копия на сключените договори), които се класират в отделни досиета. Досиетата се съхраняват в шкафове, които се заключват, в кабинета на главния счетоводител.

(4) Електронните данни се съхраняват в бази данни.

Процедура за обработване на лични данни, отнасящи се до физически лица, страни по делата.

Чл. 12. (1) Личните данни, отнасящи се до физически лица, страни по съдебни производства (граждански, търговски и наказателни) се събират при подаване на иски молби, заявления, молби, жалби, по които се образуват различни видове дела според предмета на иска.

(2) Личните данни, отнасящи се до лица, страни по дела, се събират при подаване на иски молби, заявления, молби, жалби, като обичайно личните данни се съдържат в текста на самите тях и се вписват в отделни деловодни регистри, съгласно изискванията на ПАС.

(3) Личните данни се съхраняват на електронен и хартиен носител (сканирани в деловодната система на съда, в регистри, съгласно ПАС на електронен и хартиен носител, папка с приложени документи по образуване на делото), които се съхраняват в отделни шкафове в деловодството и в архива на съда, като достъпът на други лица, освен съдебните деловодители е ограничен. При класифицирани дела (томове от дела) личните данни се съхраняват в самите папки в регистратура за работа с класифицирана информация, по реда на ЗЗКИ и ППЗЗКИ.

(4) Електронните данни се съхраняват в бази данни.

VIII. ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл. 13. (1) Съдът документира дейностите по обработване на лични данни при спазване на принципа на отчетност.

(2) Документацията трябва да е достатъчна, за да докаже спазването на принципите за законосъобразно обработване на личните данни.

(3) Обработването на данни, свързано с предаване на данни на обработващи, установени в страната или чужбина; съхранение на данни на сървъри, собственост на трети лица; архивиране или изтриване на данни; въвеждане на псевдонимизация, както и всяка друга обработка, чиито параметри са различни от описаните в тези правила, се документира чрез създаване на протоколи, които съдържат следната информация:

(а) целите на обработването;

(б) категориите лични данни и категориите субекти на данни;

(в) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави;

(г) предаването на лични данни на трета държава;

(д) когато е възможно, предвидените срокове за изтриване на различните категории данни;

(е) общо описание на техническите и организационни мерки за сигурност.

IX. ФОРМИ НА ОРГАНИЗАЦИЯ И СЪХРАНЯВАНЕ НА ЛИЧНИТЕ ДАННИ

1. На хартиен носител (писмена форма)

Чл. 14. (1) Формата на организация и съхраняване на личните данни е писмена (документална) и се съхранява в папки-досиета за всеки съдия, служител, както и за всички участници в съдебния процес и се подрежда в специални картотечни шкафове в канцеларии със заключване.

(2) Местонахождението на картотечните шкафове е в помещения, предназначени за самостоятелна работа на оператора на лични данни или в общо помещение за работа с изпълняващи други дейности.

Чл. 15. (1) Носителят (формата) за предоставяне на данните от физическите лица – личните данни за всяко лице от посочения по-горе кръг от лица се набират в изпълнение на нормативно задължение – разпоредбите на Кодекс на труда и подзаконовите нормативни актове за прилагането му, Кодекс за социално осигуряване, Граждански процесуален кодекс, Наказателно-процесуален кодекс, Административно-процесуален кодекс, Закон за съдебната власт, Правилник за администрацията в съдилищата, Закон за счетоводството, Наредба № 2 от 29.06.2015 г. за вписването, квалификацията и възнагражденията на вещите лица, Наредба № 7 от 28.09.2017 г. за съдебните заседатели, Наредба № Н-1 от 16.05.2014 г. за съдебните преводачи и други чрез: устно интервю с лицето (при постъпване или в процеса на работа), хартиен носител – писмени документи – молби, заявления за постъпване/извършване на работа по трудово

или гражданско правоотношение, за изменение или прекратяване на тези отношения, по текущи въпроси в процеса на работа, подадени от лицето, подобни документи, подадени от участниците в гражданския и наказателен процес, както и от външни източници (от съдебни, финансови, осигурителни, данъчни и други институции в изпълнение на нормативни изисквания).

(2) Личните данни от лицата се подават на администратора на лични данни и съдебните служители, обработващи лични данни, на основание нормативно задължение във всички случаи, когато е необходимо;

Чл. 16. (1) Достъп до личните данни имат само оправомощените, а именно: съдиите и съдебните служители, които оперират с данни или имат достъп до тях.

(2) Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично регламентирана в ЗЗЛД.

Чл. 17. Когато информацията, която се обработва е класифицирана по смисъла на ЗЗКИ, информационните носители се съхраняват в каси или заключващи се шкафове, в регистратура за КИ, които отговарят на нормативните изисквания на ЗЗКИ и ППЗЗКИ.

2. На технически носител (електронна форма)

Чл. 18. (1) Личните данни се въвеждат на твърдия диск на компютъра. Компютърът е свързан в локална мрежа, но със защитен достъп до личните данни, който е непосредствен само от страна на обработващите лични данни.

(2) При работа с данните се използват съответните софтуерни продукти по обработка на данните относно възнагражденията на персонала, в това число основни и допълнителни възнаграждения, данъчни и други задължения (вноски по заеми, запори и пр.), трудов стаж, присъствени и неприсъствени дни, по обработка на съответния вид съдебно дело и други подобни. Софтуерните продукти са адаптирани към специфичните нужди на администратора на лични данни;

(3) Компютърът е инсталиран в изолирано помещение за самостоятелна работа на опериращия с лични данни, а когато не е налице организационно-техническа възможност за това, компютърът може да бъде поставен в общо помещение за работа на опериращия с лични данни с изпълняващи други дейности.

Х. ГРУПИ ДАННИ, ПОДЛЕЖАЩИ НА ОБРАБОТВАНЕ

Чл. 19. (1) Относно **физическата идентичност на лицата** – имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.).

(2) Относно **социална идентичност** на лицата могат да бъдат:

- **социално положение** – данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години – данните са необходими при установяване правата на лицата за получаване на семейни добавки за деца до 18 години, за начисляване на съответни удържки от трудовото възнаграждение на дадено лице на основание присъдена издръжка, като критерий при подбор на служителите и др. под.);

- данни относно социалната принадлежност на физическото лице според притежаваното образование;
- данни относно образованието на физическото лице (вид на образованието, място, номер и дата на издаване на дипломата) – данните са необходими с оглед спазване нормативни или установени с щатното разписание на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата, както и за назначаване на съответните вещи лица. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;
- допълнителна квалификация – данните са необходими с оглед спазване нормативни или установени с щатното разписание на длъжностите изисквания за заемане, респ. за освобождаване на длъжности от лицата. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;
- трудова дейност – професионална биография – данните са от значение при избора на подходящо за съответната длъжност лице. Предоставят се на основание нормативно задължение във всички случаи, когато е необходимо.

(3) **Медицински данни** относно физиологичното, психическо и психологическо състояние на лицето – данните са от значение при заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи особено висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, в това число от рискови групи. Предоставят се на основание нормативно задължение във всички случаи, когато е необходимо.

(4) Данни относно **икономическа идентичност**, като данни относно имотното и финансово състояние на физическото лице, участието и/или притежаването на дялове или ценни книжа на дружества и др. В масовите случаи тези данни се предоставят от физическото лице на администратора с оглед изпълнение на съответните задължения към данъчни и осигурителни органи, покриване на изисквания при заемане на изборни постове и др. под., както при искане за освобождаване от държавни такси, при което основанието за обработване на тези данни е посочено в нормативен акт.

(5) Други данни, като лични данни относно **гражданско-правния статус** на лицата, необходими за длъжностите, свързани с материална отговорност, като свидетелство за съдимост. Предоставят се на основание нормативно задължение.

XI. МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Физическата защита в съда се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградата и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 20. (1) Всички помещения, в които се съхраняват и обработват лични данни в съда са с контрол на достъпа, както следва:

- охрана на помещенията – денонощно и чрез видеонаблюдение от ГД „Охрана” към МП;

- заключващи механизми;
- допускане на външни лица до помещенията на съда само с придружител от персонала на съда.

(2) Помещенията на съда са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.

Мерки за документална защита

Чл. 21. (1) Съдът установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани в тези правила.

(2) Размножаването и разпространението на документи или файлове, съдържащи лични данни се извършва само при възникнала необходимост.

Персонални мерки на защита

Чл. 22. (1) Преди заемане на съответната длъжност лицата, обработващи личните данни:

- поемат задължение за неразпространение на личните данни, до които имат достъп;
- се запознават с нормативната база, вътрешните правила и политики на съда, относно защитата на личните данни;
- преминават обучение за реакция при събития, застрашаващи сигурността на данните;
- са инструктирани за опасностите за личните данни, които се обработват от съда;
- се задължават да не споделят критична информация помежду си и с външни лица, освен по установения в тези вътрешни правила ред.

(2) При постъпване на работа всички служители преминават обучение за реакция при събития, застрашаващи сигурността на данните и обучение относно задълженията на съда, свързани с обработката на лични данни и мерките за защита на данните, които следва да предприемат в процеса на работа. Последващи обучения и тренировки на персонала се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им. Следва да се обработват данните само по указания на администратора, да не се посещават съмнителни или нелегални сайтове.

Мерки за защита на автоматизирани информационни системи и криптографска защита

Чл. 23. (1) Достъп до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.

(2) Електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично, защитни стени (firewalls) и др.

(3) Архивиране на личните данни на технически носител се извършва периодично с оглед съхранение на информацията. Не следва да се използват лични флашки, да се осъществява достъп до данните чрез публични WI-FI мрежи, да се прехвърлят данни на персонални компютри (лаптопи).

Чл. 24. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия и др., се осигурява посредством:

- въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни и файловете, които съдържат лични данни;
- антивирусни програми, проверки за нелегално инсталиран софтуер;
- периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;
- периодично архивиране на данните на технически носители, поддържане на информацията на хартиен носител (архивни копия).

ХП. БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 25. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) Окръжен съд – Русе прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола и др.), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни, правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(5) Системите, обработващи и/или съхраняващи лични данни, включват система за контрол, регистрираща следните действия в журнал (log) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (например влизане в нетипично време, неизключване на работна станция след изтичане на работното време и др. п.), системният администратор незабавно уведомява Председателя на съда за извършване на проверка по случая.

Чл. 26. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране в разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 27. (1) В Окръжен съд – Русе се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от системния администратор на съда. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 28. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

XIII. НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 29. (1) Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на съдебния и системния администратор на съда, като му предоставят цялата налична информация.

(2) Съдебният и системният администратор извършват незабавно проверка по подадения сигнал, като се опитват да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(3) Съдебният и системният администратор докладват незабавно на Председателя на съда наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които считат, че трябва да се предприемат.

(4) След съгласуване с Председателя на съда, съдебният администратор съвместно със системният администратор, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с председателя би забавило реакцията и би нанесло големи щети, съдебният и/или системният администратор, може по своя преценка да предприеме мерки за предотвратяване

или намаляване последиците от нарушението на сигурността. В този случай той, уведомява незабавно председателя за предприетите мерки и съобразява последващи действия с получените инструкции.

(6) Съгласно чл.33, пар.5 от Регламент (ЕС) 2016/679, респ. чл.67, ал.5 от ЗЗЛД всяко отделно нарушение на сигурността на личните данни се документира в Регистър на нарушенията на сигурността на личните данни в Окръжен съд – Русе.

Чл. 30. (1) В случай, че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от председателя на съда, съдебният администратор организира уведомяването на Инспектората на ВСС.

(2) Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до Инспектората на ВСС съдържа следната информация:

(а) 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;

(б) името и координатите за връзка на съдебния и системния администратор;

(в) описание на евентуалните последици от нарушението на сигурността;

(г) описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

(4) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, съдебният администратор и/или системният администратор без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

XIV. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 31. (1) 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, извършвана от съда. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при всяко въвеждане на ключова система или смяна на програма, която е свързана с обработване на лични данни, включително:

- първоначалното въвеждане на нови технологии или прехода към нови технологии;
- автоматизирано обработване, включително профилиране или автоматизирано вземане на решения;
- обработване на чувствителни лични данни в голям мащаб;

- мащабно, систематично наблюдение на публично обществена зона.

XV. УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 32. (1) Унищожаване на личните данни се извършва от съда или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването и при спазване на разпоредбите на относимите нормативни актове.

(2) Информацията в регистрите се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.

(3) Унищожаването на данни на хартиен носител се извършва по ред и в сроковете, съгласно нормативните разпоредби чрез нарязване с шредер машина. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

XVI. ОСИГУРЯВАНЕ НА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Чл. 33. (1) Заетите по трудови правоотношения, както и другите лица, обект на останалите регистри, имат право на достъп до личните си данни в свободно избрана от тях форма, очертана в Закона за защита на личните данни, за който подават писмено заявление до обработващия лични данни и/или лицето, действащо под негово или на администратора ръководство при обработването, в това число и по електронен път по реда на Закона за електронния документ и електронния подпис, лично или чрез упълномощено по нотариален ред лице. Подаването на заявление е безплатно.

(2) При упражняване на правото си на достъп заинтересованото лице има право по всяко време да поиска от администратора:

- потвърждение за това, дали отнасящите се до него данни се обработват; информация за целите на това обработване; за категориите данни и за получателите или категориите получатели, на които данните се разкриват;
- съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник;

Чл. 34. Когато при осъществяване достъпа до лични данни по искане на едно лице, е възможно да се разкрият лични данни за друго лице, администраторът е длъжен да предостави достъп само до частта от тях, отнасяща се до заинтересованото лице.

Чл. 35. (1) Освен на достъп до лични данни, заетите по трудови правоотношения, както и останалите лица, обект на регистрите, имат право по всяко време да поискат от администратора да:

- заличи, коригира или блокира негови лични данни, обработването на които не отговаря на изискванията на Закона за защита на личните данни;
- уведоми третите лица, на които са разкрити личните му данни, за всяко заличаване, коригиране или блокиране, извършено в съответствие с горното, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

(2) Заявлението съдържа име на лицето и други данни, които го идентифицират – ЕГН, длъжност/качество в процеса, месторабота, описание на искането, предпочитана форма за предоставяне на достъп до личните данни, подпис, дата на подаване и адрес за кореспонденция, нотариално заверено пълномощно, когато заявлението се подава от упълномощено лице. Заявлението се завежда в общия входящ регистър на администратора;

Чл. 36. Достъп до данните на заинтересованото лице се осигурява под формата на:

- устна справка;
- писмена справка;
- преглед на данните от самото лице или от изрично упълномощеното от него такова;
- предоставяне на копие от исканата информация;
- предоставяне на копие от исканата информация на предпочитан носител, освен в случаите, когато законът забранява това.

Чл. 37. (1) Срокът за разглеждане на заявлението и произнасяне по него е един месец от деня на подаване на искането, съответно – три месеца, когато обективно се изисква по-дълъг срок за събиране на всички искани данни на лицето и това сериозно затруднява дейността на администратора, съобразно чл. 12, пар. 3 от регламент (ЕС) 2016/679.

(2) В посочените срокове, по заявлението на лицето, администраторът на лични данни взема решение за предоставяне на пълна или частична информация или мотивирано отказва предоставянето ѝ.

Чл. 38. (1) При искане за заличаване, блокиране на лични данни, поради неправомерно обработване, несъответстващо на Закона за защита на личните данни, администраторът взема решение и извършва съответното действие в едномесечен срок от подаване на заявлението или мотивирано отказва извършването им.

(2) При искане за уведомяване на трети лица, на които са разкрити личните данни за извършеното заличаване, коригиране, блокиране, администраторът на лични данни взема решение в едномесечен срок и незабавно уведомява третите лица или мотивирано отказва да извърши уведомяването.

(3) Администраторът на лични данни уведомява писмено заявителя за решението или отказа си в съответния срок лично срещу подпис или по пощата с обратна разписка. Липсата на уведомление се смята за отказ.

(4) Когато данните не съществуват или предоставянето им е забранено със закон, на заявителя се отказва достъп до тях с мотивирано решение.

Чл. 39. (1) Администраторът отказва пълно или частично предоставяне на данни на лицето, за което те се отнасят, когато от това би възникнала опасност за отбраната или националната сигурност или за защита на класифицираната информация и това е предвидено в специален закон.

(2) Отказът за предоставяне достъп може се обжалва от лицето пред посочения в писмото орган и срок.

Чл. 40. Достъп до личните данни на лицата, съдържащи се на технически носител, има само обработващият лични данни и/или лицето, действащо под

негово или на администратора ръководство, а в негово отсъствие и когато тези данни се отнасят до възнагражденията на лицата, достъп до тях има лице, определено със заповед на административния ръководител – председател на съда, комуто е известна паролата за достъп до файловете.

XVII. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл. 41. (1) Адм.ръководител на ОС Русе, като администратор на лични данни, определя със заповед длъжностно лице по защита на данни, обработването на които се извършва за дейности, извън изпълнението на съдебните функции.

(2) Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, експертните му познания в областта на законодателството и практиките в областта на защитата на данните, познанията за дейността и структурата на администратора.

(3) Администраторът на лични данни публикува данните за контакт с длъжностното лице по защита на данните и ги съобщава на надзорния орган.

(4) Длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни.

(5) Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на администратора.

(6) Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно регламент (ЕС) 2016/679.

(7) Длъжностното лице по защита на данните е длъжно да спазва секретността или поверителността на изпълняваните от него задачи.

(8) Длъжностното лице по защита на данните може да изпълнява и други задачи и задължения. Администраторът прави необходимото тези задачи и задължения да не водят до конфликт на интереси.

Чл.42. (1) Длъжностното лице по защита на данните изпълнява следните задачи:

1. да информира и съветва администратора на лични данни и обучава служителите, които извършват обработване, за техните задължения по силата на регламент (ЕС) 2016/679 и на други разпоредби за защитата на данни;

2. да наблюдава спазването на регламента и на други разпоредби за защитата на данни и на политиките на администратора по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване;

3. при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните;
4. да си сътрудничи с надзорния орган;
5. да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването на данни и по целесъобразност да се консултира по всякакви други въпроси;
6. да следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на обработваните лични данни;
7. да определя ред за съхраняване и унищожаване на информационни носители;
8. да спазва конфиденциалността на изпълняваните задачи;

(2) При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

Чл. 43. Служителите на съда са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;
3. да актуализират при необходимост обработваните лични данни;
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

Чл. 44. (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за съда или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

XVIII. КОНТРОЛ И ОПАЗВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 45. С цел опазване на техническите и информационните ресурси при аварии, произшествия и бедствия (пожар, наводнение и др.) се провеждат съответните мероприятия: периодична проверка на изправността на контакти, ел. инсталациите, ел. таблата, забрана за ползване на отоплителни уреди, освен при необходимост, съхраняване на информационните носители в каси или метални шкафове, които се заключват.

Чл. 46. (1) Достъп до операционната система, съдържаща файлове за обработка на лични данни, има само съответният обработващ и/или лицето, действащо под негово или на администратора ръководство чрез парола за

отваряне на тези файлове, известна на него, а в негово отсъствие – на лице, определено със заповед на административния ръководител – председател на съда.

(2) Защитата на електронните данни от неправилен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на CD, както и чрез поддържане на информацията на хартиен носител.

(3) Сървърите, на които се съхранява информация, включваща и лични данни на физически лица, са разположени в отделно помещение, което се заключава с ограничен пропускателен режим.

(4) Достъпът на служителите до компютърната операционна система на всяко работно място е чрез лична парола. В съдебните зали на работното място на съдебния секретар се използват индивидуални пароли за достъп за всеки съдебен секретар.

(5) Когато информацията е класифицирана по смисъла на ЗЗКИ, помещението, в което се съхраняват информационните носители – регистратура за КИ се заключава от служител с регламентиран достъп и се охранява със сигнално-охранителна техника.

Чл. 47. (1) Личните данни от съответните регистри се обработват в рамките на установеното работно време и при спазване на реда за обработване на постъпилите книжа, съгласно Правилника за администрацията в съдилищата и длъжностните характеристики на съдебните служители.

(2) Обработването на лични данни, свързани със съдебното производство, е допустимо и след края на работното време, както и в неработни дни, в случай, че съдебните заседания се провеждат по това време.

Чл. 48. (1) Профилактиката на компютърната техника, антивирусната защита на операционната система и др. мероприятия с цел защита на данните се осъществяват от упълномощено със заповед на административния ръководител – председател лице.

(2) Регистрите се съхраняват и личните данни в тях се обработват само в определените за целта помещения, по работни места на длъжностните лица, като не се допускат граждани и външни лица до работните места и до компютърната техника.

Чл. 49. При установяване на случаи на умишлено повреждане и нерегламентиран достъп до личните данни, лицата, които имат достъп до лични данни докладват незабавно писмено на административния ръководител – председател на съда времето на установяване на умишленото повреждане, нерегламентиран достъп или друг инцидент, като административният ръководител в зависимост от последствията взема съответните мерки или възлага вземането им на други длъжностни лица.

Чл. 50. (1) За неизпълнение на задълженията, вменени на съответните съдебни служители по тези Вътрешни правила и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда, а когато неизпълнението на съответното задължение е констатирано и установено от

надлежен орган – предвиденото в Закона за защита на личните данни административно наказание – глоба.

(2) Ако в резултат действията на съответния съдебен служител по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. Приложение към настоящите Вътрешни правила са образци на следните документи, съставяни при и по повод обработката на лични данни:

- **Образец № 1** – Декларация-съгласие за обработка на лични данни (която се подписва, когато обработването не се извършва на друго основание, предвидено в чл. 6 от Регламент 2016/679);
- **Образец № 2** – Уведомление за нарушаване сигурността на личните данни до или Инспектората на ВСС;
- **Образец № 3** – Уведомление за нарушаване сигурността на личните данни до заинтересовано лице.

ДЕКЛАРАЦИЯ
съгласие за обработка на лични данни

Подписаният:
(трите имена)

Декларирам,

че доброволно и информирано давам изричното си съгласие на Окръжен съд – Русе да обработва личните ми данни чрез автоматизирани системи и/или на хартия с цел осигуряване на възможност на Окръжен съд – Русе да изпълнява задълженията си по упражняваната от мен дейност/ трудов договор/ граждански договор и др., а именно:

- а) Идентификация: име; ЕГН, дата на раждане, постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни;
- б) Образование и професионална квалификация; данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;
- в) Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;
- г) Други данни: свидетелство за съдимост, както и други данни, чието обработване е необходимо за изпълнение на правата и задълженията на Окръжен съд – Русе като работодател.

Уведомен(а) съм, че категориите лични данни, които ще бъдат обработвани на основата на моето съгласие, са: **физическа идентичност, икономическа идентичност, здравна идентичност, социална идентичност; други.**

- Личните ми данни ще бъдат съхранявани за срок, съгласно утвърдената номенклатура
- След срока на съхранение личните ми данни ще бъдат унищожени по следния ред:
 - данни на хартия – чрез нарязване с шредер машина;
 - електронни данни – чрез изтриване от електронната база данни.

Декларатор:
(подпис)

Имена:

Дата:

УВЕДОМЛЕНИЯ ЗА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

**УВЕДОМЛЕНИЕ ДО ИНСПЕКТОРАТА НА ВСС ЗА НАРУШЕНИЕ НА
СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ**

До

Инспектората на ВСС

София

.....[дата]

Относно: Уведомление за нарушение на сигурността на личните данни

Уважаеми г-н/г-жо Главен инспектор,

Долуподписаният/ите, в качеството си на представляващ/и на Окръжен съд – Русе, с настоящото Ви уведомявам/е за нарушение на сигурността на личните данни в периода [посочете точна дата или период].

Нарушението на сигурността на данните се състои в [посочете максимално подробно описание на нарушението, например нерегламентирано изнасяне на данни от настоящ или бивш служител, хакерска атака и т.н.].

Доколкото ми/ни е известно, засегнати са следните категории данни:
[ако е възможно посочете категориите лични данни, засегнати от нарушението], отнасящи се до
..... [посочете приблизителния брой засегнати субекти на данни].

Останалите лични данни, обработвани от организацията, не са застрашени от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

[Тази част се попълва само в случаи на обработване на лични данни по възлагане от външен обработващ:]
Обработването на [всички]/[част от горепосочените категории данни; посочете категорията/категиите данни] е възложено по силата на договор за обработване на лични данни на [посочете пълното наименование и данни за контакт с обработващия/обработващите].

Възможните последици от допуснатото нарушение на сигурността са:

.....
[посочете максимално подробно описание на рисковете, напр. нерегламентиран достъп до информация за банкови сметки на лицата].

С цел да защитим правата на субектите на данните и да ограничим възможните вредни последици от допуснатото нарушение предприехме/ще предприемем следните мерки:

.....[посочете предприетите или планирани мерки, напр. информирахме или ще информираме субектите на данните за инцидента].

При необходимост от допълнителна информация или пояснения, оставам/е на Ваше разположение.

С уважение,

[Име][Длъжност]

**УВЕДОМЛЕНИЕ ДО СУБЕКТИТЕ НА ДАННИТЕ ЗА НАРУШЕНИЕ НА
СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ**

До

.....

.....

[имена, адрес]

[дата]

Относно: Уведомление за нарушение на сигурността на личните данни

Уважаеми г-не/г-жо,

Долуподписаният/ите, в качеството си на представляващ/и на Окръжен съд – Русе, с настоящото Ви уведомявам/е за нарушение на сигурността на личните данни в периода....., засягащо Ваши лични данни.

Нарушението на сигурността на данните се състои в

.....
[посочете максимално подробно описание на нарушението, например нерегламентирано изнасяне на данни от настоящ или бивш служител, хакерска атака и т.н.].

Доколкото ми/ни е известно, засегнати са следните категории данни:

.....
[ако е възможно, посочете категориите лични данни, засегнати от нарушението].

Други Ваши данни, обработвани от организацията, не са застрашени от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

Възможните последици от допуснатото нарушение на сигурността са:

.....
[посочете максимално подробно описание на рисковете, напр. нерегламентиран достъп до информация за банкови сметки на лицата].

Целта на настоящото уведомление е да Ви позволи да предприемете съответните действия, за да намалите възможните негативни последици от нарушението. Препоръчваме Ви да вземете незабавно превантивни мерки, за да предотвратите всяка възможност за злоупотреба с личните Ви данни. Подобни мерки могат да са:

.....

[посочете конкретни съвети към субектите на данните като смяна на парола на потребителски профил].

Разбираме важноста за защитата на личните данни за Вашите права и свободи, затова предприехме/планираме да предприемем следните мерки:.....
[посочете предприетите или планирани мерки].

Своевременно уведомихме Комисията за защита на личните данни за допуснатото нарушение на сигурността, за да изпълним законовите си задължения и да получим указания за по-нататъшни действия.

Съжаляваме и поднасяме извиненията си за неудобствата, причинени от инцидента. Уверяваме Ви, че ще вземем всички възможни допълнителни технически и организационни мерки за предотвратяване на подобни събития в бъдеще.

При необходимост от допълнителна информация или пояснения оставам/е на Ваше разположение.

[информация за контакт с длъжностното лице по защита на данните, ако е определено такова]/[друга информация за контакт].

С уважение,

[Име][Длъжност]