РАЙОНЕН СЪД – ГР. ЛУКОВИТ

5770, ул. „Раковски” №6

тел: 0697/ 5 24 04 , факс: 0697/ 5 24 04

УТВЪРДИЛ:

ВИОЛЕТА ФИДЕНКОВА
ПРЕДСЕДАТЕЛ НА
РАЙОНЕН СЪД
ГР.ЛУКОВИТ

ИНСТРУКЦИЯ

за мерките за защита на личните данни в Районен съд - Луковит, вписан в „Регистър на администраторите на лични дани и на водените от тях регистри” с идентификационен № 49630 и Удостоверение за администратор на лични дани с № 49630/11.01.2013 година

I. Общи положения

Чл. 1. (1) Настоящата Инструкция се издава на основание чл. 23, ал. 4 от Закона за защита на личните данни (ЗЗЛД) и Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

(2) Инструкцията урежда условията и реда за водене на регистри по ЗЗЛД, както и организацията и реда за упражняване на контрол при обработването на лични данни в Районен съд-Луковит.

Чл. 2. (1) Инструкцията се приема с цел да регламентира:

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. Видовете регистри, които се водят в Районен съд-Луковит.
3. Оценката на въздействието и нивото на защита за всеки от водените регистри с лични данни.
4. 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.
5. Правата и задълженията на длъжностните лица, обработващи лични данни и лицата, които имат достъп до лични данни, както и тяхната отговорност при изпълнението на тези задължения.
6. Процедурите по докладване, управление и реагиране при инциденти.
7. Правила за предоставяне на лични данни на трети лица.
8. Сроковете за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.

9. Срокове за съхранение на личните данни и реда за тяхното унищожаване след изтичането им.

(2) Инструкцията се утвърждава, допълва, изменя и отменя от Председателя на Районен съд-Луковит.

II. Администратор, обработващ лични данни и регистри с лични данни

Чл. 3. Администратор на лични данни е Районен съд-Луковит, със седалище и адрес на управление: гр. Луковит, ул.»Раковски» № 6.

Чл. 4. (1) Обработващ личните данни е всяко физическо или юридическо лице, което обработва лични данни от името на администратора на лични данни.

(2) Отношенията между администратора и обработващия лични данни се уреждат с писмен акт на администратора, в който се определя обемът на правата и задълженията във връзка с обработването на лични данни.

(3) Администраторът може да определи едно или повече лица, които да отговарят за координиране и прилагане на мерките за защита.

(4) 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, като за целта лицата подписват декларация за неразгласяване на лични данни на основание чл.7, ал.5 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните дани, до които са получили достъп при и по повод изпълнение на задълженията си.

(5) Всички лица, отговарят за спазването на ограниченията за достъп до личните данни, и са персонално отговорни пред Председателя на Районен съд Луковит за нарушаването на принципите за поверителност, цялостност и наличност на личните данни, освен в случаите на форсмажорни обстоятелства.

(6) Всяко физическо лице, чийто 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. получателите или категориите получатели, на които могат да бъдат разкрити данните;
5. информация за правото на достъп и правото на коригиране на събраните данни.

Алинея 6 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 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 по ал. 1;
4. е налице изрична забрана за това в закон.

Чл. 5. В Районен съд Луковит се обработват лични данни в следните регистри:

1. Регистър „Деловодство, участници в съдебни производства" .

2. Регистър «Бюро съдимост»

3. Регистър „Персонал".

4. Регистър „Съдебно изпълнение”.
5. Регистър “Контрагенти”.

III.Регистър “Деловодство, участници в съдебни производства”

Чл. 6. Описание на поддържания регистър

В регистъра се обработват лични данни на страните по делата, образувани по описа на Районен съд Луковит , с оглед:

Използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани с обработването на делата- изготвяне на всякакви документи в тази връзка (призовки, писма, съобщения до страните и техните представители или пълномощници и др.);

- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция;

Чл. 7. Категории лични данни в регистъра и основание за обработването им

В регистъра се обработват следните категории лични данни:

- за физическа идентичност: имена, ЕГН, адреси, телефони за връзка и др.;
- здравен статус на физически лица
-гражданско състояние на физически лица- семейно положение, данни за наследници.

Чл. 8. Технологично описание на регистъра

1. Носители на данни в регистър «Деловодство, участници в съдебни производства»

Данните в регистъра се обработват на хартиен и технически носител.

В деловодството на съда на хартиен носител се водят следните книги и регистри.

- Описни книги
- Срочни книги
- Азбучници
- Входящ регистър
- Изходящ регистър
- Книга за получении и върнати призовки и съдебни книжа
- Регистър на издадените изпълнителни листи
- Регистър на заявленията за достъп до обществена информация.

В Районен съд Луковит регистъра за дстъп до обществена информация се води от административния секретар, който със заповед на административния ръководител е оправомощен да извършва тази дейност.

2. Технология на обработване

Данните в регистъра се предоставят от физическите и юридически лица при входиране на документа във входящия регистър. Данните се въвеждат директно в деловодната програма САС »Съдебно деловодство», с която работи Районен съд Луковит.

3. Срок за съхранение

Данните в регистърите се съхраняват за сроковете, определени в ПАС.

- наказателните дела- 5 години/след архивиране/
- гражданските дела- 5 години/след архивиране/
- описни книги, азбучници и регистри – 100 години
- базата данни от деловодната програма след изтичане на 10 години се архивира в два еднакви носителя, които се съхраняват при специални условия 50 години.

4. Предоставени услуги

Администраторът на лични данни да предоставя достъп- справки, извлечения, да издава документи и други услуги от съответния регистър с лични данни.

Чл. 9. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

1. Данните от регистъра се обработват от съдиите, съдебните деловодители и съдебните секретари в Районен съд Луковит и при спазване на принципа „Необходимост да се знае”.

2. Право на достъп до регистъра имат само упълномощени по длъжност или с изрична заповед лица.

3.Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл. 10. Оценка на въздействието и определяне съответното ниво на защита на регистъра

Оценка на нивото на въздействие на регистър „Деловодство,участници в съдебни производства”

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Регистър «Деловодство,участници в съдебни производства»	средно	средно	средно	средно

1.За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивата на въздействие върху конкретно физическо лице или група физически лица се взема в предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност”, „цялостност” и „наличност”. Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

2.При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – страни по дела, чийто брой надхвърля 2.

3. В зависимост от определеното ниско ниво на въздействие нивото на защита на регистър „Деловодство, участници в съдебни производства” е средно.

Чл. 11. Технически и организационни мерки за защита

1. Физическа защита

Личните данни от регистъра се обработват в стаите на упълномощените по чл. 9 лица. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в помещенията, в които работят упълномощените лица.

Помещенията, в които се обработват лични данни от регистъра са защитени чрез заключване на вратите, сигнално- охранителна система и пожарогасителни средства в коридора на сградата.

Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

Външни лица нямат достъп до помещенията, в които се обработват лични данни от регистъра, с изключение на служба Деловодство, където има обособен вход за граждани и участници в съдебните производства и само в присъствието на упълномощени служители.

2. Персонална защита

Лицата, обработващи лични данни се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните дани и настоящата Инструкция.

Лицата, обработващи лични данни, задължително подписват декларация на основание чл.7, ал.5 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните дани,, 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 политиките за информационна сигурност.

3. Документална защита

Личните данни в Регистър „Деловодство, участници в съдебни производства“ се поддържа на хартиен и технически носител. Обработването се извършва само по време на редовното работно време на съда. Достъп до регистъра имат лицата посочени в чл. 9 по-горе от настоящата Инструкция. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Достъпът до регистъра е ограничен само за упълномощени лица в съответствие с принципа „Необходимост да се знае”.

Сроковете за съхранение на документи от регистър „Деловодство, участници в съдебни производства“, които са на хартиен носител са определени в ПАС.

Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебните им задължения или ако са изискани по надлежния ред от упълномощени лица.

Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер). След изтичане на срока за съхранение, тези документи се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на председателя комисия. Унищожаването се извършва след изрично писмено разрешение от Председателя.

4. Защита на автоматизирани информационни системи и мрежи

При работа с данните от регистъра се използват софтуерен продукт за обработване, деловодна програма САС «Съдебно деловодство», разработен от «Информационно обслужване» АД. Данните се въвеждат в база данни и се съхраняват на сървър. Прави се архив на друг твърд диск на същия сървър , като архивите са защитени с парола. Всеки упълномощен служител 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.

Администраторът 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.

Съдебните служители- съдебни деловодители и съдебни секретари са отговорни за управлението на регистъра. Само лицата посочени в чл. 9 по-горе имат достъп до регистъра.

За всички компютърни конфигурации, 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 и сигнално-охранителна система.

Организационни мерки за гарантиране нивото на сигурност:

- Охрана на сградата със сигнално-охранителна техника.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено от служебни лица.
- 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.

Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

Сроковете за съхранение на данни от регистъра са описани в чл. 8, т. 3 от настоящата Инструкция.

Актовете /решения и определения/ на Районен съд Луковит се публикуват ежедневно на интернет страницата на съда и в ЦУБИПСА, при спазване на Закона за защита на личните данни и Закона за защита на класифицираната информация. Публикуването се извършва след обезличаване на личните данни на физическите лица, по начин, който не позволява идентифицирането на физическите лица, упоменати в тези актове.

Чл. 12. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.)

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

Чл. 13. Предоставяне на лични данни на трети лица

Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (МВР,Прокуратура, следствени органи и т.н.) и при спазване разпоредбите на чл.2, ал.2 от Закона за защита на личните данни..

IV. Регистър “Бюро съдимост”.

Чл. 14. Работата на Бюрата за съдимост е нормативно регламентирана в Наредба № 8 от 26.02.2008г./ДВ,бр.24 от 04.03.2008г/, в сила от 15.02.2013г.. за функциите и организацията на дейността на Бюрата за съдимост/БС/.

В Районен съд-Луковит не е налице утвърден щат за осъществяване дейността на Бюро съдимост, а същата се осъществява от деловодител-наказателно деловодство, а при отсъствие от деловодител-гражданско деловодство, на които дейността е вменена със заповед на Административния ръководител и длъжностната характеристика.

Използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани с движението и обработването на делата-изготвяне на справки за съдимост при подадени искания от компетентните органи или при пдаване заявление лично от лицето или чрез пълномощник.

В регистъра подлежат на обработка лични данни на участници в съдебни процеси, както и на техни възходящи- родители.

Чл. 15. Категории лични данни в регистъра и основание за обработването им

В регистъра се обработват следните категории лични данни:

- за физическа идентичност: имена, ЕГН, адрес, лични данни за възходящи лица-родители.

Чл. 16. Технологично описание на регистъра

1. Носители на данни

Данните в регистъра се обработват на хартиен и технически носител, посредством внедрен и поддържан софтуерен продукт АИС «Бюро съдимост».

2. Технология на обработване

Данните в регистъра се предоставят от физическите лица, направили искане за издаване на свидетелство за съдимост или от съответните компетентни органи, подали искането за издаване са справката. Данните се въвеждат директно в АИС «Бюро съдимост», посредством която се осъществява и издава справката.

От 2013г. свидетелства за съдимост могат да бъдат издавани и чрез квалифициран електронен подпис на физическо лице чрез интернет-страницата на Министерство на правосъдието.Електронно свидетелство за съдимост се издава само за лица, за които не са съставяни бюлетини за съдимост, включително и по чл.78а НК /Чл.35а от Наредба № 8 БС/.

3. Срок за съхранение

Данните в регистъра се съхраняват за сроковете, определени в Наредба № 8 от 26.02.2008г. за функциите и организацията на дейността на бюрата за съдимост.

- бюлетините за наложени административни наказания по чл.78а НК- 15 години от влизане в сила на съдебния акт

- бюлетините за съдимост се съхраняват 100 години от датата на раждане на лицата и се унищожават, след като бъдат микрофилмирани. /Чл.24, ал.1 от Наредба № 8 БС/

- базата данни от деловодната програма след изтичане на 10 години се архивира в два еднакви носителя, които се съхраняват при специални условия 50 години.

4. Предоставени услуги

Администраторът на лични данни да предоставя достъп, справки, издаване на документи /бюлетини/,справки и свидетелства за съдимост от съответния регистър с лични данни.

Чл. 17. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

1. Данните от регистъра се обработват от съдиите, съдебните деловодители-наказателни и граждански дела и съдебните секретари в Районен съд Луковит и при спазване на принципа „Необходимост да се знае”.

2. Право на достъп до регистъра имат само упълномощени лица.

Чл.18. Защита на автоматизирани информационни системи и мрежи

-при работа с данните от регистъра се използва софтуерен продукт за обработка-АИС «Бюро съдимост» разработен и поддържан от Консорциум «Индекс-Бъргария-Лирекс БГ» ООД. Районен съд гр.Луковит има договор за следгаранционно обслужване, поддръжка и актуализация на АИС с консорциума.

Данните се въвеждат в база данни и се съхраняват на сървър. Прави се архив на друг твърд диск на същия сървър , като архивите са защитени с парола. Всеки упълномощен служител 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.

Администраторът 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, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма.

Съдебните служители- съдебни деловодители , съдебни секретари и системен администратор са отговорни за управлението на регистъра. Само лицата посочени в чл. 17 по-горе имат достъп до регистъра.

За всички компютърни конфигурации, 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 и сигнално-охранителна система.

Организационни мерки за гарантиране нивото на сигурност:

- Охрана на сградата със сигнално-охранителна техника.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- 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.

Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

Сроковете за съхранение на данни от регистъра са описани в чл. 16, т. 3 от настоящата Инструкция.

Чл. 19. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.)

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

Чл. 20. Предоставяне на лични данни на трети лица

Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Прокуратура,Следствие, МВР и т.н.), както и на физически лица при спазване разпоредбите на чл.35, ал.2 и ал.3 от Наредба № 8 БС.

V. Регистър „Персонал”.

Чл. 21. Описание на поддържания регистър

В регистърът се обработват лични данни на магистрати и съдебни служители, работещи в Районен съд Луковит по правоотношение възникнали по силата на ЗСВ /магистрати/ и по трудови правоотношения /съдебни служители/, с оглед:

1. индивидуализиране на правоотношения по Закона за съдебната власт /магистрати/ и трудовите правоотношение по Кодекса на труда /съдебни служители/;

2. изпълнение на нормативните изисквания на Закона за съдебната власт, Кодекса на труд, Закона за държавния архив.

3. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите правоотношения и на правоотношенията на магистратите по силата на ЗСВ;

- за изготвяне на всякакви документи на лицата в тази връзка (договори, заповеди, 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 правоотношения /съдебните служители/ и правоотношенията по ЗСВ/магистрати/.

Чл.22. Категории лични данни в регистъра и основание за обработването им

В регистърът се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

4. гражданско-правен статус на лицата, необходими за длъжностите, свързани с материална отговорност (напр. свидетелства за съдимост);

5. лични данни, които се отнасят до здравето: данните се съдържат в медицинско свидетелство за започване на работа, експертни лекарски решения и др.

Чл. 23. Технологично описание на регистъра

1. Носители на данни

Данните в регистъра се обработват на хартиен и технически носител.

Автоматизираната обработка на данните в Районен съд Луковит се осъществява посредством счетоводна програма «Конто» и ТРЗ «Аладин».

2. Технология на обработване

Данните в регистъра се предоставят от физическите лица при назначаване в Районен съд Луковит. Данните се въвеждат директно в трудови договори на съдебните служители, заповеди за магистратите, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

3. Срок за съхранение

Данните в регистъра се съхраняват за срок от 50 години във връзка с нормативно установени срокове.

4. Предоставени услуги

Администраторът на лични данни да предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

Чл. 24. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

1.Данните от регистъра се обработват от главния счетоводител и административния секретар на съда, в чийто длъжностни характеристики е вменено задължение за обработване на данните на магистратите и служителите и при спазване на принципа „Необходимост да се знае".

2. Право на достъп до регистъра има само управомощените лица.

3.Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл. 25. Оценка на въздействието и определяне съответното ниво на защита на регистъра

Оценка на нивото на въздействие на регистър „Персонал"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Регистър"Персонал"	средно	средно	средно	средно

1. За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица се взима в предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност", „цялостност" и „наличност". Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

2. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата, социалната, семейната идентичност на група физически лица – магистрати и съдебни служители, чийто брой надхвърля 2.

3. В зависимост от определеното средно ниво на въздействие нивото на защита на регистър „Персонал" е средно.

Чл. 26. Технически и организационни мерки за защита

1. Физическа защита

Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 28 лица. Всички документи на хартиен носител /кадрови досиета/, съдържащи лични данни, се съхраняват в шкаф в кабинета на Административния секретар с ограничен достъп само за упълномощени лица.

Помещенията, в които се обработват лични данни от регистъра са оборудвани с заключване на вратата , пожарогасителни средства в коридора и охрана СОТ.

Физически достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители.

2. Персонална защита

Лицата, обработващи лични данни се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните дани и настоящата Инструкция

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 политиките за информационна сигурност.

3. Документална защита

Регистър „Персонал“ се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативните уредби на Р България, както и на вътрешните нужди за периодична оценка на служителите). Обработването се извършва само по време на редовното работно време на съда. Достъп до регистъра имат лицата посочени в чл. 24 по-горе. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в шкаф в стаята на Административния секретар и Главния счетоводител. Достъпът до регистъра е ограничен само за упълномощени лица в съответствие с принципа „Необходимост да се знае”. Председателят и Административния секретар и Главния счетоводител са отговорни за контрол на достъп до регистъра.

Сроковете за съхранение на документи от регистър „Персонал“, които са на хартиен носител, са определени в чл. 23, т. 3 от настоящата Инструкция по-горе. Документите се съхраняват в сградата на Районен съд Луковит на II етаж /стаята на Административен секретар и Главен счетоводител/.

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 упълномощени лица.

Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер). След изтичане на срока за съхранение, тези документи се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Председателя комисия. Унищожаването се извършва след изрично писмено разрешение от Председателя на съда.

4. Защита на автоматизирани информационни системи и мрежи.

При работа с данните от регистъра се използват софтуерен продукт за обработване. Данните се въвеждат в база данни и се съхраняват на работния компютър, където се обработват личните данни. Упълномощеният служител има личен профил (потребителско име и парола). Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

Администраторът 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 и мрежови устройства. За защита на данните е инсталирана антивирусна програма. Ежемесечно информацията се архивира и се съхранява на твърдия диск.

Административния секретар и Главния счетоводител са отговорни за управлението на регистъра. Само лицата посочени в чл. 24 по-горе имат достъп до регистъра.

За всички компютърни конфигурации, 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 и сигнално-охранителна система.

Организационни мерки за гарантиране нивото на сигурност:

- Охрана на сградата със сигнално-охранителна техника.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- 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.

Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

Сроковете за съхранение на данни от регистъра са описани в чл. 23, т. 3.

Чл. 31. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.)

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

Чл. 32. Предоставяне на лични данни на трети лица

Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

В качеството си на работодател, Районен съд Луковит предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на магистрати и съдебни служители, както и по молба от работещите в Районен съд гр.Луковит във връзка с отпускането на кредити на служителите. Личните данни, които се предоставят са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането, както и размер на трудовото възнаграждение на лицето за определен период от време,в полза на което

се извършва кредитирането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови операции.

Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица съдът посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

V. Регистър «Съдебно изпълнение»

Чл. 33. Описание на поддържания регистър

В регистърът се обработват лични данни на физически и юридически лица, нормативно регламентирани във връзка пряко с извършването на дейността, както и по извънтрудови правоотношения /вещи лица/ с оглед:

1.Индивидуализиране във връзка с пряката дейност на службата

2. индивидуализиране на правоотношения по граждански договори;

3. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани със осъществяване на основната дейност по съдебното изпълнение и по възникналите граждански правоотношения;
- за изготвяне на всякакви документи на лицата, в тази връзка (служебни бележки, справки, удостоверения и др.);
- за установяване на връзка с лицата по телефон, по електронен път за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията им по изпълнителни дела;

Чл. 34. Категории лични данни в регистъра и основание за обработването им

В регистърът се обработват следните категории лични данни:

- физическа идентичност: имена, ЕГН, номер, дата и място на издаване на документи за самоличност, постоянен и настоящ адрес и др.;
- трудова дейност: месторабота и размер на трудовото възнаграждение.
- социално-икономическа идентичност: имотно и финансово състояние, участие в сдружения и /или притежаване на дялове или ценни книжа на дружества и др.

Чл. 35. Технологично описание на регистъра

1. Носители на данни

Данните в регистъра се обработват на хартиен и технически носител.

В регистър «Съдебно изпълнение» се водят следните книги и регистри.

- Описна книга
- Азбучници
- Входящ регистър
- Изходящ регистър
- Книга за получении и върнати призовки и съдебни книжа

2. Технология на обработване

В масовите случаи данните в регистъра се предоставят от самия администратор на лични данни след издаване на изпълнителен лист и или от съответните лица , с оглед изпълнение на нормативно регламентираните задължения на администратора и при изпълнение задълженията към взискатели/данъчни, контролни и осигурителни органи/, при покриване на критерии и изисквания при заемане на изборни постове или при участие в обществени поръчки, както и при искане за освобождаване от държавни такси, при което основанието за обработване на тези данни е посочено в нормативен акт.

Данните се въвеждат директно в деловодната програма, в документи, удостоверяващи определени обстоятелства пред компетентни нормативно-регламентирани органи, в служебни бележки, в справки, в удостоверения и друга кореспонденция.

3. Срок за съхранение на информацията:

- азбучни регистри и книги- 100 години;

-изпълнителни дела по частни и държавни вземания на физически и юридически лица - 5 години/след архивиране/

-изпълнителни листове по премирани/просрочени/ дела- 25 години/ след архивиране/.

- базата данни от деловодната програма след изтичане на 10 години се архивира в два еднакви носителя, които се съхраняват при специални условия 50 години

4. Предоставени услуги

Администраторът на лични данни да предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

Чл. 36. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

1. Данните от регистъра се обработват от Държавния съдебен изпълнител, съдебен секретар при СИС и съдебен деловодител при СИС в чиято длъжностна характеристика е определено задължение за обработване на данните на взискатели и длъжници, вещи лица и при спазване на принципа „Необходимост да се знае".

2. Право на достъп до регистъра имат само упълномощените лица.

3. Длъжностното лице няма право да разпространява информация за личните данни, станали му известни при изпълнение на служебните му задължения.

Чл. 37. Оценка на въздействието и определяне съответното ниво на защита на регистъра

Оценка на нивото на въздействие на регистър „Съдебно изпълнение"

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Регистър"Съдебно изпълнение"	средно	средно	средно	средно

1. За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица се взима в предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност", „цялостност" и „наличност". Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

2. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – взискатели, длъжници и вещи лица, чийто брой надхвърля 2.

3. В зависимост от определеното средно ниво на въздействие нивото на защита на регистър „Съдебно изпълнение" е средно.

Чл. 38. Технически и организационни мерки за защита

1. Физическа защита

Личните данни от регистъра се обработват в стаята на упълномощените по чл. 36 лица. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в стаята на лицата, упълномощени по чл.36, находяща се на първия етаж на сградата на Районен съд Луковит.

Помещението, в което се обработват лични данни от регистъра е защитено от посегателства чрез заключване на вратата и поставяне на метални решетки от външната страна на прозорците, свързано е със сигнално-охранителна система и пожарогасителни средства в коридора на съда.

Достъп се предоставя само на служителите, чиито служебни задължения включват обработване на лични данни от регистъра.

Външни лица имат достъп до помещението, в което се обработват лични данни от регистъра, само в присъствието на упълномощените служители.

2. Персонална защита

Лицата, обработващи лични данни се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните дани и настоящата Инструкция.

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 кадровите досиета на служителите.

Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

3. Документална защита

Регистър „Съдебно изпълнение“ се поддържа на хартиен носител (папки, чието съдържание съответства на нормативните уредби на Р България, както и на вътрешните нужди за периодична оценка на служителите). Обработването се извършва само по време на редовното работно време на съда. Достъп до регистъра имат лицата, посочени в чл. 36 по-горе. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Достъпът до регистъра е ограничен само за упълномощени лица в съответствие с принципа „Необходимост да се знае”.

Сроковете за съхранение на документи от регистър „Съдебно изпълнение“, които са на хартиен носител, са определени в чл.35, т. 3 по-горе. Документите се съхраняват в архива на съда.

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 упълномощени лица.

Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер). След изтичане на срока за съхранение, тези документи се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на председателя комисия. Унищожаването се извършва след изрично писмено разрешение от Председателя на съда.

4. Защита на автоматизирани информационни системи и мрежи.

При работа с данните от регистъра се използват софтуерен продукт за обработване “ДСИ-JES”, разработен и поддържан от ЕТ”Темида-2000-Еди Чакъров” . Данните се въвеждат в база данни и се съхраняват на работния компютър, където се

обработват.Упълномощените служители има личен профил (потребителско име и парола). Дефинирани са и уникално потребителско име и парола за стартиране на операционната система на компютъра.

Администраторът 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.

Лицата, упълномощени по чл.36 са отговорни за управлението на регистъра. Само те има достъп до данните от регистъра.

За всички компютърни конфигурации, 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 и сигнално-охранителна система.

Организационни мерки за гарантиране нивото на сигурност:

- Охрана на сградата със сигнално-охранителна техника.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- 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.

Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

Сроковете за съхранение на данни от регистъра са описани в чл. 35, т. 3.

Чл. 39. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.)

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

Чл. 40. Предоставяне на лични данни на трети лица

Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

Във връзка с използването на куриерски услуги – приемане, пренасяне, доставка и адресиране на пратките до физически лица съдът посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

VI. Регистър “Контрагенти”.

Чл. 41. Описание на поддържания регистър

В регистъра се обработват лични данни на физически и юридически лица, нормативно регламентирани във връзка с извършването на дейностти, както пряко свързани с основната дейност на регистратора, така и във връзка с допълнителни

дейности- възлагане на обществени поръчки, изпълнение на текущи и авариини ремонти и др.

1. индивидуализиране на данни, свързани със сключване на договори;

2. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани с осъществяване на основната дейност-правораздаване ;

- по възникване на служебни правоотношения в останалите случаи-изготвяне на документи на лицата (служебни бележки, справки, удостоверения и др.);

- за установяване на връзка с лицата по телефон, по електронен път за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията им по сключени договори или поети ангажименти;

Чл. 42. Категории лични данни в регистъра и основание за обработването им

В регистъра се обработват следните категории лични данни:

- физическа идентичност: имена, ЕГН, номер, дата и място на издаване на документи за самоличност, постоянен и настоящ адрес и др.;
- трудова дейност: месторабота и заемана длъжност, професионален опит.
- социално-икономическа идентичност: текущо финансово състояние, участие в сдружения .

Чл. 43. Технологично описание на регистъра

1. Носители на данни

Данните в регистъра се обработват на хартиен и технически носител.

2. Технология на обработване

Личните данни на вещите лица, лицата с юридическа правоспособност-служебни защитници и особени представители и свидетелите по делата се въвеждат в програмен продукт ПП»Аладин».В масовите случаи данните в регистъра се предоставят от съответните лица , с оглед изпълнение на нормативно регламентираните задължения, възложени от администратора , при покриване на критерии и изисквания за участие в обществени поръчки, при които основанието за обработване е посочено в нормативен акт.

3. Срок за съхранение на информацията:

- договори и приемо-предавателни протоколи за изпълнение на обществени поръчки- постоянен/ съхраняват се в съда/

- служебни бележки и удостоверения за изплатени възнаграждения -10г. след одитиране /финансова ревизия/

- договори за отдаване под наем- 5 години след приключване

- лични данни на свидетели , вещи лица и лица с юридическа правоспособност изпълнителни дела по частни и държавни вземания на физически и юридически лица - 5 години/след архивиране/

4. Предоставени услуги

Администраторът на лични данни да предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

Чл. 44. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

1. Данните от регистъра се обработват от Административния секретар и Главния счетоводител, в чиито длъжностни характеристика е определено задължение за обработване на данните на външни лица- вещи лица, свидетели, лица с юридическа правоспособност и представители на фирми, извършващи външни услуги и при спазване на принципа „Необходимост да се знае”.

2. Право на достъп до регистъра имат само упълномощените лица.

3. Длъжностното лице няма право да разпространява информация за личните данни, станали му известни при изпълнение на служебните му задължения.

Чл. 45. Оценка на въздействието и определяне съответното ниво на защита на регистъра

Оценка на нивото на въздействие на регистър „Контрагенти”

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Рег.”Контрагенти”	средно	средно	средно	средно

1. За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица се взима в предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност”, „цялостност” и „наличност”. Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

2. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – вещи лица, свидетели и лица с юридическа праводпособност,чийто брой надхвърля 2.

3. В зависимост от определеното средно ниво на въздействие нивото на защита на регистър „Контрагенти” е средно.

Чл. 46. Технически и организационни мерки за защита

1. Физическа защита

Личните данни от регистъра се обработват в стаята на упълномощените по чл. 44 лица. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в стаята на лицата, упълномощени по чл. 44.Помещението, в което се обработват лични данни от регистъра е защитено от посегателства чрез заключване на вратата, свързано е със сигнално-охранителна система и пожарогасителни средства в коридорите на съда.

Достъп се предоставя само на служителите, чиито служебни задължения включват обработване на лични данни от регистъра.

Външни лица имат достъп до помещението, в което се обработват лични данни от регистъра, само в присъствието на упълномощените служители.

2. Персонална защита

Лицата, обработващи лични данни се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните дани и настоящата Инструкция.

Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали му известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровите досиета на служителите.

Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

3. Документална защита

Регистър „Контрагенти“ се поддържа на хартиен и технически носител (съхраняват се в папки, чието съдържание съответства на нормативната уредба на Р България, както и на вътрешните нужди за периодична оценка на служителите). Обработването се извършва само по време на редовното работно време на съда.

Достъп до регистъра имат лицата, посочени в чл. 44 по-горе. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Достъпът до регистъра е ограничен само за упълномощени лица в съответствие с принципа „Необходимост да се знае”. Главния счетоводител, Административния секретар и секретар СИС са отговорни за контрола на достъпа до регистъра.

Сроковете за съхранение на документи от регистър „Контрагенти“, които са на хартиен носител, са определени в чл.43, т. 3 по-горе. Документите се съхраняват в архива на съда.

Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебните им задължения или ако са изискани по надлежния ред от упълномощени лица.

Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер). След изтичане на срока за съхранение, тези документи се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на председателя комисия. Унищожаването се извършва след изрично писмено разрешение от Председателя на съда.

4. Защита на автоматизирани информационни системи и мрежи.

При работа с данните от регистъра се използват софтуерен продукт за обработване ПП»АЛАДИН».Данните се въвеждат в база данни и се съхраняват на работния компютър, където се обработват личните данни. Упълномощените служители имат лични профили (потребителско име и парола). Дефинирани са и уникално потребителско име и парола за стартиране на операционната система на компютъра.

Администраторът 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.

Лицата, упълномощени по чл.44 са отговорни за управлението на регистъра. Само те има достъп до данните от регистъра.

За всички компютърни конфигурации, 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 и сигнално-охранителна система.

Организационни мерки за гарантиране нивото на сигурност:

- Охрана на сградата със сигнално-охранителна техника.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- 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.

Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

Сроковете за съхранение на данни от регистъра са описани в чл. 43, т. 3.

Чл. 47. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.)

При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

Чл. 48. Предоставяне на лични данни на трети лица

Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, и т.н.).

Във връзка с използването на куриерски услуги – приемане, пренасяне, доставка и адресиране на пратките съдът посочва следните данни: име на получателя, адрес, област, пощенски код и наименование на населеното място.

Чл. 49. Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им

Съдебните служители следва да извършват ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Чл. 50. Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

След изтичане на срокът за съхранение на данните, комисия определя чрез актови протоколи кои документи подлежат на унищожение и мястото на извършване на процедурата. Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за съда, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса и разтрошаване на носителя на данни.

В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването, като се съставят съответно приемо-предавателни протоколи.

Допълнителни разпоредби

1. Инструкцията влиза в сила от 01.03.2014 г. и е утвърдена със Заповед №……/……...2014 година на Председателя на Районен съд Луковит.

АДМ.СЕКРЕТАР: